SCIENTIFIC EDITOR

Ryszard Szczebiot

INNOVATION TRENDS 2025

Scientific Editor

Ryszard Szczebiot

INNOVATION TRENDS 2025

University of Lomza

Łomża 2025

Scientific Editor Ryszard Szczebiot

Reviewers Ryszard Szczebiot
Ladislav Várkoly
Michal Zábovský
Romuald Kotowski

Łomża 2025

ISBN 978-83-60571-75-0

CONTENT

page

VISUALISED SIMULATION MODELS IN DEEP LEARNING ALGORITHMS AND PROGRAMMING

Veronika STOFFOVÁ

Trnava Universty in Trnava, Faculty of Education, Department of Mathematics and Informatics, Trnava, Slovakia

veronika.stoffova@truni.sk

ABSTRACT

Simulation modelling is a suitable tool for acquiring new knowledge not only in research but also in education. Appropriate visualization can increase the clarity of teaching, and shorten the time needed to understand complex dynamic phenomena. Didactic simulations can involve students in "deep learning" (DL), which support for better understanding. DL means that students learn to apply scientific methods and procedures for getting new knowledge, recognize the individual steps of the model building process and the importance of following them. They understand the relationships and connections between parameters and variables in a model. Students solve data-related tasks apply probability and sampling theory. They investigate how the model can be used to predict outcomes, or how to achieve the desired results. Observe the properties of the system and its reactions to changes in parameters, etc. They learn to reflect and expand their knowledge by actively participating in student-student or teacher-student conversations and discussions that are necessary to conduct simulation experiments. Students are able to transfer the acquired knowledge to solve new problems, situations. They learn to systematize their knowledge by understanding and developing their own thought processes. Build your knowledge system correctly and thus acquire usable knowledge - they learn actively. They see the observed processes and their parts in interaction, i.e. in real operation. Simulations help students understand that scientific knowledge is based on the results of testing hypotheses. Teaching with visualized simulation models significantly increases the quality and efficiency of learning.

Key words: modelling, simulation, deep learning, algorithms, programming

INTRODUCTION

Modeling and simulation in education plays two important roles.As a research method for obtaining new information about the modeled object, it can be the subject of teaching.As a didactic method, to study and investigate dynamic phenomena – to understand how they work, what properties they have, how they can be controlled etc. In the first case, it is about investigating an unknown object, phenomenon, process of the real world on which we have defined the system.First, we must identify the system and create its exact mathematical model, which serves as a basis for implementing a computer model of the system.Such a relevant computer model can serve as a substitute for the object under study for conducting simulation experiments for deeper knowledge of the system, for forecasting, predicting the behavior of the object under study in various situations, under various circumstances, etc., by setting the parameters of the system [1, 2]. The results of simulation experiments that help to make the right decisions for managing production processes, managing the provision of services, distributing goods, etc.

In education, we have a mathematical model of the phenomenon under study at our disposal – that is, we do not have to identify it.It is up to the designer/programmer how to approach the graphic presentation so that the dynamic phenomenon under study is understandable, so that the simulation process is clearly animated and the results can be easily and correctly interpreted[3, 4].In this case, it is not a classic static animation – the projection of static image sequences, but an animation controlled by algorithms and parameters.In other words, these are simulation experiments for educational purposes [5].

In the computer application of M&S a computer is used to build a mathematical model which contains key parameters of the physical model. The mathematical model represents the physical model in virtual form, and conditions are applied that set up the experiment of interest. The simulation starts – i.e., the computer calculates the results of those conditions on the mathematical model – and outputs results in a format that is either machine- or human-readable, depending upon the implementation [1, 6]. Modeling and simulation as a subject of teaching has gradually entered the study programs of universities oriented towards technical, natural, biological, medical, pharmaceutical, social, economic and other sciences. Here we are talking about modeling and simulation as a serious research method and research tool, with which it is possible to obtain new knowledge about the subject of research through simulation experiments and thus refine the picture of the real world. This new knowledge is then used and applied in practice. This universal research procedure can be used in any field of science and almost every scientific discipline. The second role of modeling and simulation is related to the educational process, where they play the role of an effective educational tool for acquiring new knowledge for the learner, mainly based on observing the processes and results of visualized (animated) simulation experiments. For a deeper understanding of the connections between the parameters of the system, their influence on the behavior of the system. The student later plans appropriate experiments himself - he experiments with an interactive simulation computer model to solve various (often crisis) situations, system instability, finding sensitive parameters and optimally setting their values, etc. [5, 6].

1. SIMULATION MODELS

An exact simulation model is a concentration of knowledge about the modeled object.The computer implementation is based on an exact mathematical model, which can be a simple function expressing the functional dependence of the monitored dependent variable(s) on the values of the independent variable(s).In dynamic systems, the independent variable is (usually) time.In simulation experiments, it is necessary to distinguish between real and simulation time.Simulation time usually flows faster than real time, which is actually often the main reason for applying the simulation method, so that we can predict the state of the system "in the future". In order to be able to monitor the development of the system under certain conditions that we do not want to occur, we want to prevent them.Thus, we will use simulation experiments to predict the occurrence of dangerous events, show the effect of measures to mitigate their consequences, etc. Conversely, we are looking for values of system parameters that ensure its optimal functioning and stability.There are many cases where conducting a real experiment is not only time-consuming but also very expensive, so we replace them with simulation.Visualized simulation is an effective tool not only for events that are slow and their monitoring would be time-consuming, but also for fast events where changes cannot be observed with the naked eye. When using models of real objects to better understand their behavior, visualized simulation experiments are usually performed.In this sense, students use simulation techniques to gain new knowledge and experience.

The common procedure for building simulation models is as follows:
Selecting and defining the object of modeling; Defining the goals and purpose of modeling; Identifying the object of modeling as a system; Defining the level of differentiation of modeling, determining subsystems and their parts and the method of their mutual connections; Determining the level of resolution and depth of detail of the model; Identification of the system; Create the mathematical model for replacing the object with its mathematical model; Selecting and adapting the mathematical procedures used;Computer program implementation of mathematical model; Validation and verification of model;Determination of limits and conditions of validity; Designing and conducting simulation experiments; Interpreting and generalizing the simulation results. Thus means, when examining an object (everything that can be the subject of investigation), it is necessary from the point of view of practical activity to single out a system on general objects.The system (as a tool) defines the object and also its elements and the surroundings of the system, the properties of the elements and the relationships between the elements.It is always a relative concept, the specific content of which is given

by the need to define the subject of knowledge from the point of view of the goals of knowledgeinvestigation [7].

2. CREATION AND USE OF DIDACTIC ANIMATION AND SIMULATION MODELS

The procedure for creating didactic animation-simulation models is very similar to creating simulation models for scientific and research purposes.The difference is that they are extended by visualization - a visual representation of dynamic phenomena and processes that we study, learn about and investigate by conducting simulation experiments [5, 6].

Another significant difference is that here the mathematical model of the object under study is already known, and there may be several of them depending on the reasons for which we are interested in the real object, why it is the subject of our investigation.There is no difference in the interpretation of simulation experiments results, but they are usually easier to interpret them because they are given in a clear graphic form.It is also important to set a goal, what we want to find out, what we are investigating.The results obtained are usually already known scientific facts - scientific knowledge, but they are new to the learner.This will also help in planning a simulation experiment so that the results obtained confirm this scientific knowledge.

The procedure shown in Figure 1 is the result of our long-term experience in the field of creating simulation models for didactic purpos.

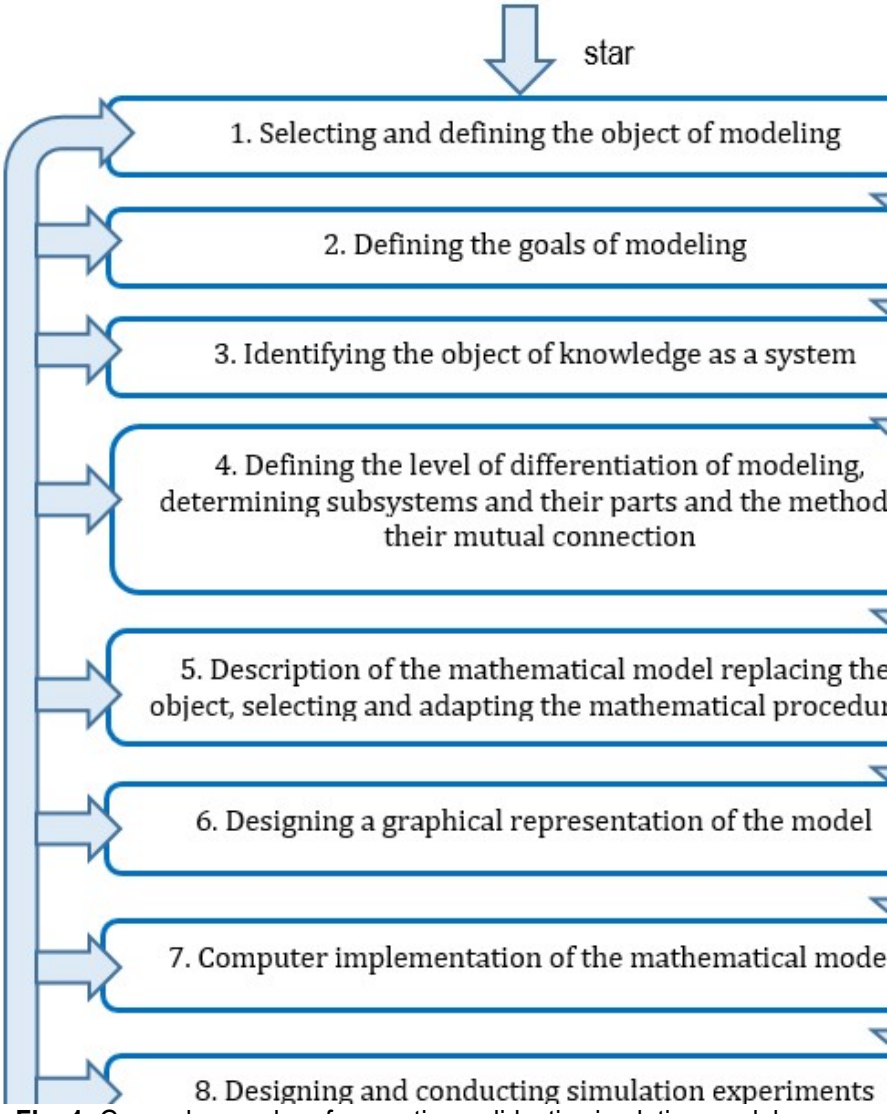


Fig. 1. General procedure for creating a didactic simulation model.

When creating didactic animation simulation models and using them effectively, we should keep in mind that when creating didactic animation simulation models and using them effectively for educational purposes, we should keep in mind that:

- Information is conveyed in various forms in order to involve more senses in the learning process at the same time - that is why multimedia presentation is used.
- Animation should be interactive and should ensure not only the active involvement of the learner but also the active cooperation of the students.
- Mutual feedback must also be ensured - the student responds to the stimuli in the presentation, but the program also responds adequately to the student's interventions and activities.
- Simulation models are used where appropriate and necessary - both for presenting new knowledge and for experimenting with the model in order to gain new knowledge and own experience.

3. VISUALISED SIMULATION MODELS OF SORTING ALGORITHS

Simulation modeling is a suitable tool not only in research but also in education.We will present examples of visualized simulation models that demonstrate how selected sorting algorithms work.The application contains 5 sorting algorithms: SimpleSort, SelectSort, BubbleSort, InserSort and QuickSort and serves to visually present how the selected simulation algorithm works.We have chosen the QuickSort algorithm as an example.We will describe and show how this algorithm works, how the simulation experiment can be controlled.What tasks do students solve using simulation experiments. The application we have chosen was created to demonstrate how selected sorting algorithms work, what properties they have and how these properties can be used in writing a program to solve more complex tasks where sorting algorithms are used.Therefore, the pseudocode of the program is in the form of a procedure [8, 9].

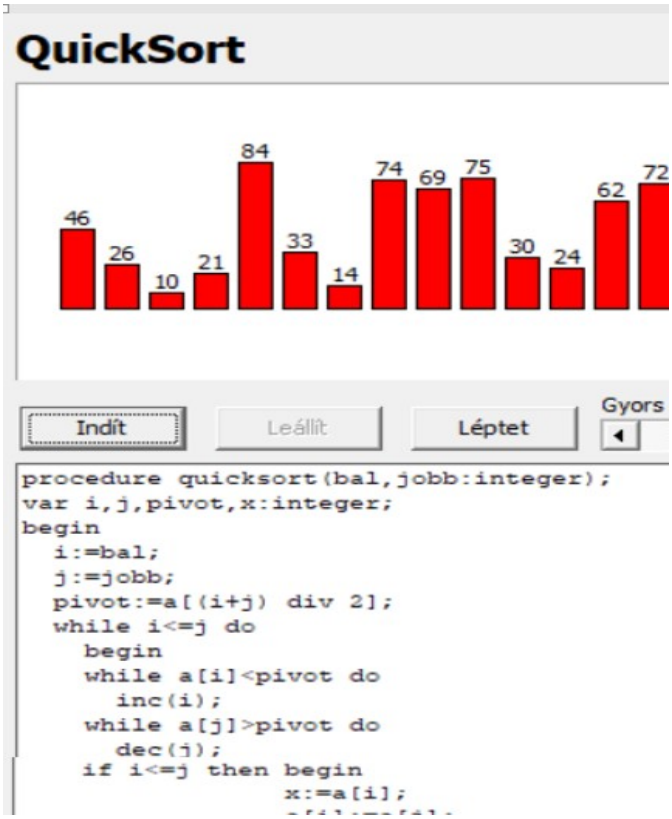


Fig. 2. QuickSort: The start screan of simulation.

The screen for each sorting algorithm has the same structure. In the upper part of the window there is a graphic display of the elements to be sorted, in the form of columns above which there is a number indicating the height of the column. In Figure 2 we see the Home screen of the sorting algorithm "QuickSort", one of the five offered sorting algorithms. After generating 16 random elements (numbers), in the form of red columns, it is necessary to sort from the smallest value to the largest. Below that are the functional buttons for controlling the simulation. The sorting process, and therefore its animation, are easily controllable. It is possible to carry out the process step by step using the "Step-Léptet" button, or using the "Start-Indít" button to start the entire sorting process with the speed set using the last element signed “Gyors – Lassú” in the row of control buttons. The running process can be stopped using the "Stop" button. As soon as the simulation starts, a blue line cursor appears in the program window, showing the execution/interpretation of the program code.During the animation process, only active buttons marked with black letters can be used. The gray heading indicates the buttons that cannot be used at the given moment (the actions they trigger are not active in that situation). The window in the last part of the saved screen contains the pseudocode of the algorithm and the blue line cursor shows which command is currently being executed. The value of the variables **i** and **j** can be read in the animation window they are equal with number of its position. The pivot value is written in the upper left corner of the first window and is also marked with a yellow horizontal line in the rectangle where the sorting is currently taking place.It is clear to the programmer that the sorting is done "in place" and the sorted values are in the data structure of a one-dimensional array of numbers.

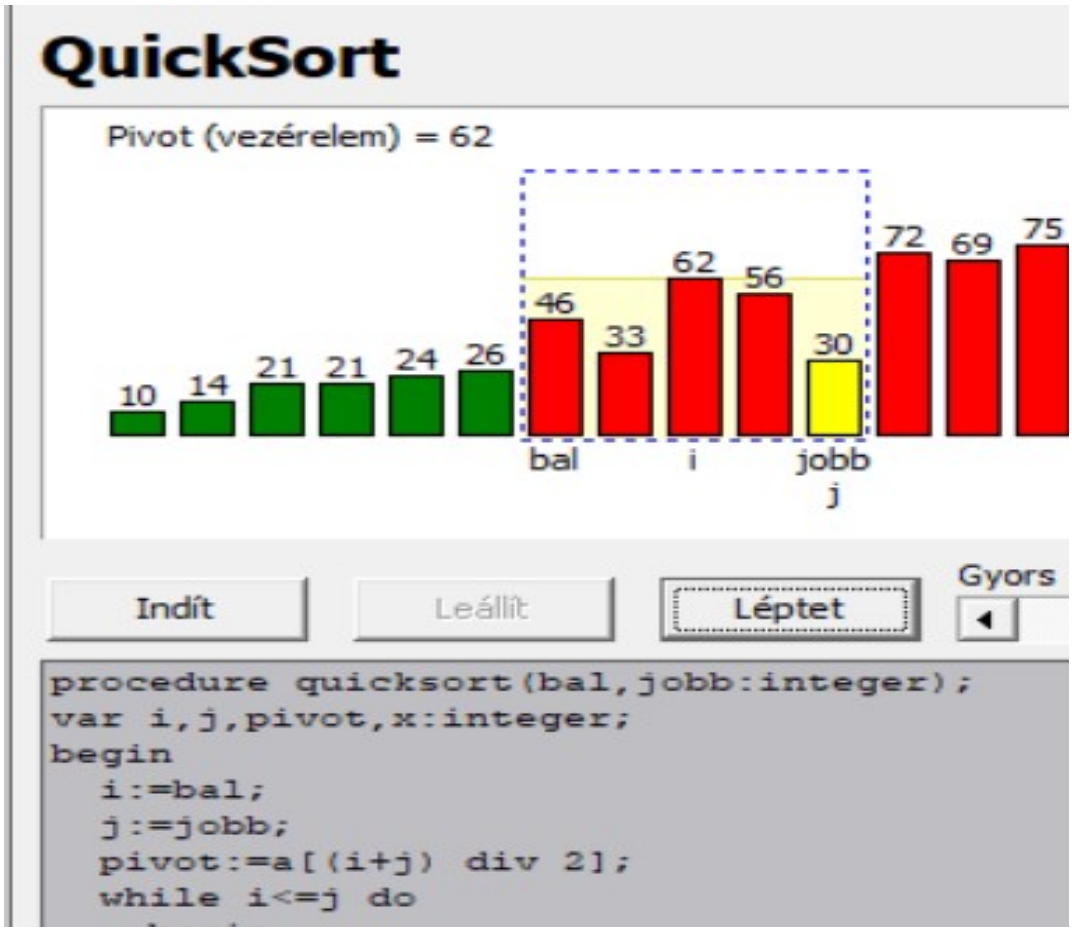


Fig. 3. QuickSort: PrintScrean in the midle of simulation.

The colors of the display of the columns, which gradually change from red to another, also carry certain information. The meaning of the colors during the animation is as follows: Unsorted elements are red.

Yellow indicates the selected elements that will be compared with pivot. A blue rectangular frame made of dashed lines delimits the section that is currently being sorted."jobb" is the right boundary, "bal" is the left boundary of interval.An already sorted element is drawn in green.

3.1. EXPERIMENTING WITH SORTING ALGORITHMS

Students perform simulation experiments and study how the arrangement of elements changes until an ordered sequence is achieved. In the lower window, the blue line cursor shows which command is being executed.

Students solve the assigned tasks and search for answers to the questions posed by observing what is happening on the screen.We will select only some of the results of the students' solutions that we consider interesting.

Task 1:Describe in your own words how the algorithm works.

Algorithm “QuickSort”belongs to the quicksorts algoritms with complexity (n*logn), which work on the principle of dividing the array into smaller parts.At the beginning, it chooses one of the numbers in the array as a “comparison basis” – it is called the pivot.Based on the value of the pivot, the array is divided into two sections.One section consists of elements that are smaller than itself, and those that are larger than itself. The algorithm then traverses the section from the beginning and end of the array towards the center.From the left, it searches for the first number that is greater than or equal to the pivot, and from the right, it searches for the first number that is less than or equal to the pivot.When it finds them, it swaps these two values with each other. It continues in this way until both sides meet or exceed each other.When this happens, the algorithm is guaranteed that all numbers to the left of the encounter are less than or equal to the base, and all numbers to the right are greater than or equal to it. The same procedure is then repeated separately for the left and right parts of the array.This process is repeated until all parts of the array are sorted.The result is a sequentially sorted array from smallest to largest element.

Task 2: Describe how the program works (using variables,control structures (loops, branching…etc.)

While the visualization of the algorithm is running, several columns of different heights are displayed on the screen, representing the values that we want to sort.These columns are initially colored mostly red, indicating that they are not yet sorted. Initially, one of the columns is selected as the comparison basis.This column is highlighted in color (for example, yellow) to make it clear that the other values will be compared according to it.Subsequently, pointers start moving on both sides of this column – one from the left and the other from the right. The pointer from the left looks for the first column that is larger than the comparison basis, while the pointer from the right looks for the first column that is smaller.When two such are found, their values (column heights) are swapped with each other.After the swap, the pointers continue towards the center until they meet. At the moment when the pointers meet or pass each other, the entire field is divided into two parts.Then the algorithm is repeated - first the left part is sorted, then the right.Visually, we can see how the columns gradually turn green - which means that they are already in their correct place.At the end of the whole process, all columns are sorted from lowest to highest and colored green, which signals that the array is completely sorted.

Task 3: Recall the screen approximately in the middle of the simulation experiment and describe the current state of the sorting (using program variables)

The line responsible for selecting the comparison element is as follows: pivot := a[(i + j) div 2]; This command says that the basis for comparison is the value that is exactly in the middle of the currently processed part of the array.It is calculated as the arithmetic average of the positions at the beginning (i) and at the end (j) of the subarray. The task of this line is to select a suitable element according to which

the array is divided into two parts - one will contain values less than or equal to this element, and the other values greater.This dividing element (pivot) is the basis for sorting. This selection is key to the functioning of the QuickSort algorithm, because QuickSort always selects a certain element as a “pivot” and divides the input data according to it.The more suitable the selection of this element, the more efficient the algorithm works - if a good central element is selected, the division of the array is uniform and the number of operations is reduced.In case of poor selection (for example, the largest or smallest element all the time), the performance of the algorithm deteriorates.

Task 4: Properties of the chosen sorting algorithm that you observed/discovered during simulation experiments.Express the properties in the form of statements about the location, length of the ordered and unordered parts (of the numerical sequence)

At the beginning of the animation, all elements are unsorted – in the simulation, they are represented as colored columns of different heights, arranged in random order.All columns are colored mostly red, which indicates that they have not yet been processed. The first phase is the selection of a comparison element (pivot) according to which the other elements will be arranged.This element is visually highlighted to make it clear that the comparison is being made according to it.Then, pointers start moving from both sides, looking for incorrectly placed values – an element larger than the selected base is searched for from the left, and an element smaller than the selected base is searched for from the right.When such two are found, their places are swapped. After the swap, the pointers continue and look for incorrect elements again.This process continues until both sides meet or cross.At that moment, the current section of the array is considered divided – the part with smaller elements is on the left and the part with larger elements is on the right. In the next phase, the same procedure is repeated on both resulting parts separately.This gradually reduces the original range that needed to be sorted.This can be seen in the visualization as more and more columns change color – from red to green or another color, which means that they are now correctly positioned.Overall, the animation nicely shows how a large unsorted array breaks down into smaller and smaller parts, each of which is sorted separately, until all values are correctly sorted.

Task 5: Have you discovered any properties that can be used to shorten the algorithm?

From observing the animation of the QuickSort algorithm, we could notice several properties that have a fundamental impact on its speed and efficiency: Choosing a comparison element (pivot): If an element is chosen that is somewhere in the middle of the sorting (e.g., not the smallest or largest), the array is divided into approximately equally sized parts. This leads to faster sorting. If we always chose a very small or very large element, the division would be very unbalanced and the sorting would take longer. Choosing a “pivot” as the median of three values (beginning, middle, end of the array) improves the division. Dividing the array into smaller sections: The speed of the algorithm depends on how efficiently the subarray is divided. The smaller and more uniform these parts are, the fewer comparisons and swaps are needed. If the subarrays are small enough, we can replace QuickSort with a simpler algorithm (e.g., InsertSort), which is faster for small quantities. In-place sorting (without creating an additional array). The algorithm works directly with the original array, without turning it into a copy. This saves memory and increases performance.
Preserving the work in the original array is advantageous, especially for large amounts of data. Although recursion makes the algorithm elegant, it can become memory-intensive for very large inputs.Using an iterative version or limiting the depth of recursion can reduce the risk of memory-intensive operations. In summary: the speed of QuickSort is most affected by the choice of comparator, the efficiency of the array partitioning, and the way it handles small sections.These are the features that can be used to improve it.

Task 6: Have you discovered any shortcomings in the graphical representation that may make it difficult to understand the algorithm, or may lead to a misunderstanding of how the algorithm works?

Based on watching the animation of the QuickSort algorithm in the application, we can identify several shortcomings that relate to both the algorithm itself and its visual implementation in a given program: Flaws of the algorithm as such:

- If an inappropriate comparison element is repeatedly selected (e.g. always very small or very large), an unbalanced division of the array occurs and thus a significant slowdown in sorting.
- Recursive calls on large inputs can be memory-intensive and can cause a stack overflow if the correct constraints are not implemented.
- For very small subarrays, QuickSort is not the most efficient - there are simpler algorithms that would be faster in these cases (e.g. InsertSort). Flaws of the implementation in the RendAlgo application:
- The pivot is not always highlighted enough - it is not clearly distinguished from other elements, which can make it difficult for the observer to understand.
- The pointers (left and right) are not visually marked in any way – for example, with arrows or colors, so it is not immediately obvious which elements are being compared or which are to be swapped.
- The colors do not change intuitively – sometimes the color of the columns does not change immediately after swapping or sorting, which can give the impression that nothing is happening.
- There is no textual commentary or legend – it would be very helpful for the student to be able to read what is happening, for example in the form of a title: “Comparing values…”, “Swapping…”, “Sorting completed” and the like.

For these reasons, we can say that although the QuickSort algorithm itself is very powerful, understanding it through visualization would be more effective if the implementation included more didactic elements and visual aids.

Task 7: Do you have any further comments or suggestions for improvement regarding the application?

Based on the observation of the visualization of the QuickSort algorithm in the “RendAlgo”aplication environment, the implementation could be improved from a didactic point of view in several ways:

- Highlighting the comparison element;
- Marking the comparison positions (left and right sides);
- Text and audio commentary during the animation;
- Improving the color scale;
- Displaying indices or numerical values.

These suggestions would help to increase the clarity of the visualization, especially for pupils or students who are encountering the QuickSort algorithm for the first time.Visual support together with commentary and logical highlighting is the key to a deeper understanding of its functioning.

3.2. VISUALISATION OF SORTING ALGORITHMS

How to properly visualize simulation experiments is in the hands of the application creator - programmer.The environment in which the application is implemented offers certain possibilities for the graphic presentation of the modeled phenomenon.It only depends on the author's imagination and his abilities to implement a graphic model with an appropriate didactic transformation to present the dynamics of the studied phenomenon.It depends on the pedagogical mastery of the teacher/author how he/she adapts the graphic display to the mental level of the learner and how he/she implements the didactic transformation of the presented knowledge [8, 9, 10, 11].

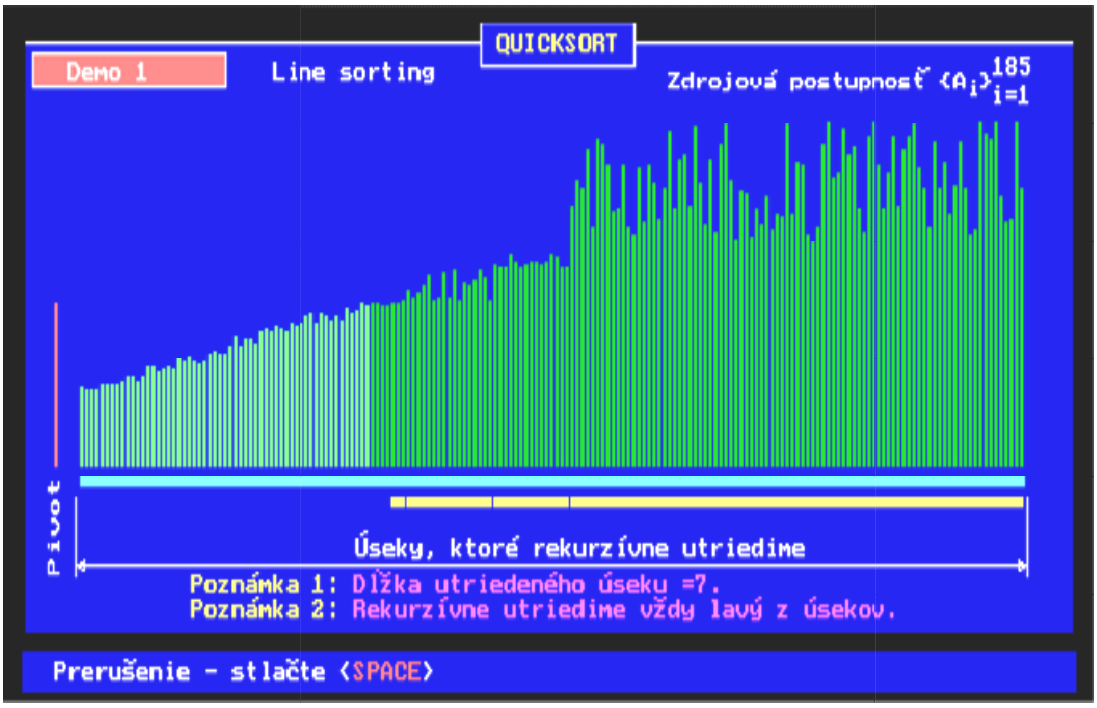


Fig. 4. QuickSort: PrintScrean in the midle of simulation sorting vertical lines.

Figures 4 and 5 present 2 PrintScreen from the simulation of the QuickSort sorting algorithm.The animation was created using the graphics library of the TurboPascal programming language (in 1987 - 1990).Given that this is a didactic application that serves to understand how the sorting algorithm works and to reveal its properties, it can be stated that the presentation of sorted elements in the form of points that are sorted by the vertical coordinate field better reflects the properties that were described in the previous section in the solution to task 5, than the presentation of the sorting procedure using sticks.The number of sorted elements also plays a significant role in the readability of the result and the discovery of properties.Many features may not appear during the animation when the number of sorted elements is small.In this case, 128 elements were used for the QuickSort representation using sticks and 10,000 for the point representation.

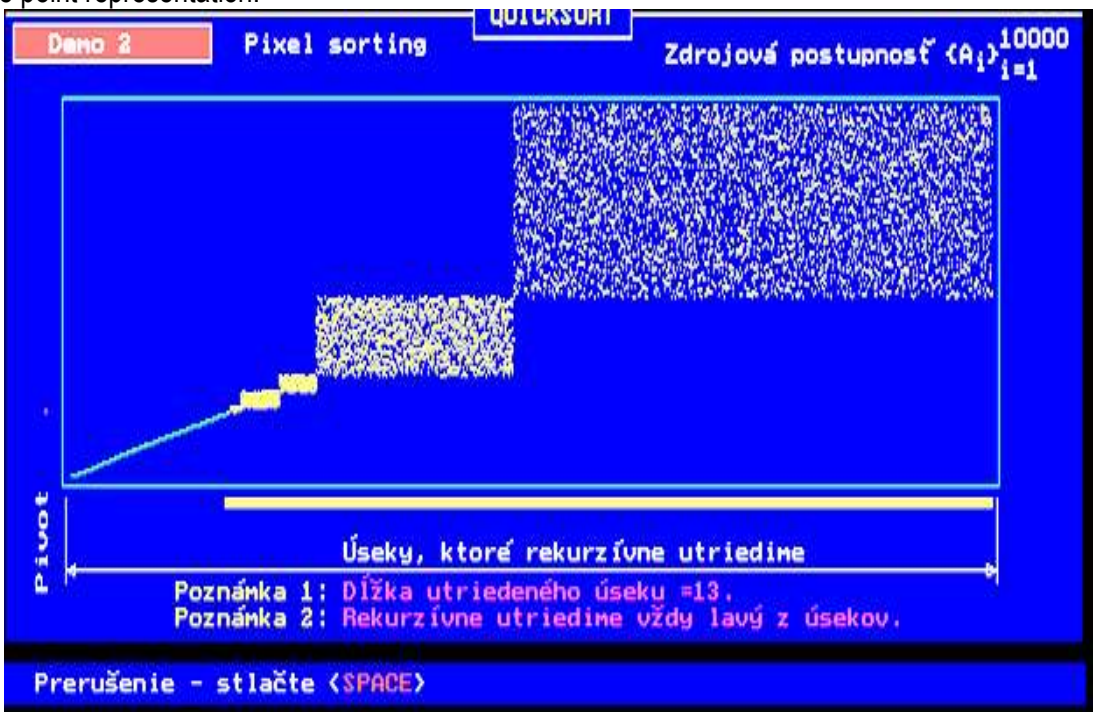


Fig. 5. QuickSort: PrintScrean in the midle of simulation sorting points by horizontal coordinate.

Algorithm simulations generally require that the program code be available during the animation.Usually, in a separate window, it is possible to monitor in parallel which commands are currently being executed.In most applications, especially those that are intended to support programming education, this requirement is met.Animation also helps to read the program and interpret its meaning.This makes it easier for the programmer to use the source code to solve new problems and correctly integrate it into the application being developed. We would also like to note that the application "RendAlgo" with 5 simulation sorting algorithms, implemented in the Delphi programming environment, takes up 445 kB of memory, equivalent programs, for example, in Flash, HTML5, and the like, have ten times higher memory requirements.

CONCLUSION

Visualized simulation models (VSM) play a significant role in teaching thematic units that require understanding the basic principles of the functioning of the dynamic phenomena and processes under study and the relationships between them.They help to understand how the "world" around us works.Simulation experiments can be very effective tools for active learning using constructivism.The effectiveness of teaching by depends on the active participation of students in problem solving, discussion, and evaluation of the results of simulation experiments. Using selected interactive visualized simulation applications, we will demonstrate how to create didactic simulation models, how to use them in teaching and learning and how to design simulation experiments.The presented examples of visualized simulation models primarily focuses on the deep learning of algorithms and programming.

ACKNOWLEDGEMENTS

The paper was supported by project KEGA 014 TTU-4/2024 "Intelligent animation-simulation models, resources and environments for deep learning".

REFERENCES

[1] I. Paholok(2008). *Simulácia ako vedecká metóda.* [online] (Simulation as a scientific method). 2008,fromhttps://e-logos.vse.cz/pdfs/elg/2008/01/10.pdf

[2] K. Czakóová, R. Horváth andV. Stoffová,(2023),*Modelovanie, simulácia a animácia v edukácii (Modelling, simulation and animation in education.* Trnavská univerzita v Trnave. Pedagogická fakulta. [online]. 2023,fromhttps://pdfweb.truni.sk/doi?978-80-568-0624-1-2023

[3] V. Stoffová, How to Create and How to Use Didactic Educational Software. *Proceeding of the 14th International Conference eLearning and Software for Education (eLSE),* 2018, pp. 487–494.

[4] D. Goldsman, (1998),*Comparisons with a Standard in Simulation Experiments* [online]. ResearcgGate [cit.2024-11-19]. from https://www.researchgate.net/profile/David-Goldsman/publication/2449438_Comparisons_with_a_Standard_in_Simulation_Experiments/links/567982c308ae40c0e27dc89b/Comparisons-with-a-Standard-in-Simulation-Experiments.pdf

[5] S. M. Sanchez and H Wan(2018),*Work smarter, not harder: a tutorial on designing and conducting simulation experiments* [online]. Simulation.su [cit.2024-11-19]. from http://simulation.su/uploads/files/default/2018-sanchez-sanchez-wan.pdf

[6] K. Czakóová, (2023). Virtual programming environments and simulations in favor of active learning of programming. *International Journal of Advanced Natural Sciences and Engineering Researches*, *7*(5), 105–109. https://doi.org/10.59287/ijanser.910

[7] . Šafařík, - V. Štofová, - P Cvik, (1984): *Modelovanie a simulácia.* 2. vyd. Bratislava : Slovenská vysoká škola technická. Fakulta elektrotechnická, 1984. 132 s.

[8] V. Stoffová, What programming tool to choose for teaching programming [electronic], 2023. In *EDULEARN23.* Palma : IATED, 2022. ISBN 978-84-09-52151-7. ISSN 2340-1117. S. 4232–4239 [online, CD-ROM, USB key]. Web of Science Core Collection.

[9] V. Gabaľová, V.: Detské programovacie jazyky a ich využitiev pedagogickej praxi, Pedagogická fakulta Trnavská univerzita, Trnava 2022, ISBN 978-80-568-0510-7, 73 s.
[10] K. Czakóová, J. Udvaros, “Applications and games for the development of algorithmic thinking in favor of experiential learning,“ in EDULEARN21: Proceedings of the 13th International Conferenceon Education and New Learning Technologies, 2021. Valencia: IATED Academy, 2021. pp. 6873-6879.
[11] K. Czakóová, “Game-based programming in primary school informatics,“ in INTED2021: Proceedings of the 15th International Technology, Education and Development Conference, 2021. Valencia: IATED Academy, 2021. pp. 5627-5632.

Veronika, Stoffová: https://orcid.org/0000-0001-8067-6876

AN INNOVATION OF A POWERTRAIN SYSTEM OF A MULTIPLE-UNIT TRAIN

Ján DIŽO[1], Alyona LOVSKA[1], Miroslav BLATNICKÝ[1], Martin BUČKO[1]

Department of Transport and Handling Machines, Faculty of Mechanical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovak Republic[1]

jan.dizo@fstroj.uniza.sk, alyona.lovska@fstroj.uniza.sk, miroslav.blatnicky@fstroj.uniza.sk, martin.bučko@fstroj.uniza.sk[1]

ABSTRACT: Railway transport is very important part of the transportation system. It ensures the movement of goods and passengers from shorter to very long distances. Regarding to passenger railway transport, there are several kinds of passenger rail vehicles used in urban and rural areas. Despite of efforts for electrification, there are still some locations in a country, where electrification is not possible or there are some other difficulties. Therefore, rail vehicles with an independent traction system are operated in such regions. These rail vehicles with an independent traction system are usually powered by a diesel engine. However, stricter and stricter emission limits and requirements for saving fossil fuels force to invite and to apply innovative and non-convetional sources of energy. Currently, hydrogen is suppose one of the future sources of energy. The main goal of the presented research is a presentation of an idea of an innovation of a multiple-unit powertrain system. It is proposed that the original diesel powertrain system of a multiple-unit train would be replaced by an innovative hydrogen fuel cells powertrain system. This system would be built to an existing passenger multiple-unit train. As such an innovation of a multiple-unit train requires a different distribution of the needed components of the hydrogen powertrain together with expected change of parameters of the vehicle, the presented study includes a comparison of conceptual design of a vehicle and a comparison of the selected parameters of the original and innovative powertrain system.

Key words: rail vehicle, multiple-unit train, hydrogen powertrain, hydrogen fual cells, emissions

INTRODUCTION

Energy is necessery to drive rail vehicles. Energy is obtained either from the thermal conversion of fuel in combustion engines or in a form of electric energy as a direct source. Although the first variant is still dominant in current transportation system, there are strong efforts to find new, innovative and environmentaly friendly sources of energy as a source of power for rail vehicles [1]. The energy, which is contained in fuels with the carbon petroleum base, is converted into the mechanical work. It happens during combustion process in a combustion engine. Subsequently, as a direct consequence, carbon dioxide is released into the air. Therefore, there is the necessity of the continuous development of vehicles in order to reduce the proportion of pollutants released into the air, not only during their real operation, but also regarding to production, distribution, as well as the storage of fuels.

Currently, there are being introduced alternative types of fuels and propulsion systems in large quantities in transport means in a form of electromobility, hydrogen fuel cells, and other ways.

In terms of the use of electric energy, railway transport is the dominant sector, where electric energy is applied and spend as a source of energy to power rail vehicles. On one hand, electrification of railway tracks seems to be as very even the most effective way of reducing harmful exhaust emissions production. On the other hand, there are still railway tracks, where the full electrification is not possible. Moreover, it is necessary to take into account, that additional electrification of tracks would be too financially demanding and it can be even unprofitable [2, 3]. Therefore, there are understandable efforts to find innovative suitable technical solutions and sources of energy for rail vehicles with an independent traction system [4]. It is desirable to find other suitable technological solutions or sources of a propulsion. One of the possible option is a conversion of diesel powertrain systems of current rail

vehicles to powertrain systems based on hydrogen fuel-cells [5-7].Currently, rail vehicles equipped with a hydrogen powertrain include hydrogen fuel-cells technology. It means, that electric energy is produced from hydrogen. The main benefit of this technical solution is almost zero exhaust emissions released into the air during rail vehicles operation [8-10]. However, heat loss needed for cooling are the main disadvantage of this system [11, 12].

1. MATERIALS AND METHODS

The multiple-unit train Alstom Coradia iLint was the first rail vehicle powered by hydrogen fuel-cells. This hydrogen rail vehicle was presented at the International railway exhibition Innotrans in 2016. After that, running tests were performed in 2017 and finally, this multiple-unit train was commissioned in 2018 by the ERA for passenger railway transprot in Germany. The original powertrain equipped with three diesel engines and a mechanical transmission system was replaced by hydrogen fuel-cells in a combination with a traction motor. Moreover, other important manufacturers of rail vehicles consider about an innovation of powertrains based on a concept of hydrogen fuel-cells as a primary source of energy and power, such as Stadler and its model Flirt H2, Alstom with Eversholt Rail with the model Project Breeze and Siemens within the project Mireo Plus H [13].

The presented innovation of the powertrain is aimed at the multiple-unit train manufactured in the Slovak Republic and which is marked as the 861 class. This multiple-unit train is depicted in Fig. 1.

Fig. 1. A multiple-unit train for implementation of an innovative hydrogen powertrain.

It is necessary to considermany aspects, such as maximal operating range, traction characteristics, available infrastructure, storage of hydrogen, maintenance requirements and others in case of a modification of a multiple-unit train from the original diesel-powered concept to the innovative hydrogen fuel-cells powered concept [14].

Tab.1. Technical parameters of the diesel multiple-unit train.

Parameter	Unit	Value
Track gauge	mm	1435
Max. speed	km/h	140
Max. capacity (number of passengers)	No.	177
Length between buffers	mm	58,880
Curb weight	kg	120,000
Max. weight	kg	142,000
Min. curve radius	m	150
Power of diesel combustion engines	kW	2 × 588

In this case, the modified multiple-unit train is a partially low-floor multiple-unit train originally powered by a MAN diesel engine. It is intended to be operated for railway transport of passengers on regional railway tracks without electrification. It is the three-article multipe-unit train with four bogies, at which, two bogies under head wagons are drive bogieswith traction motors and two bogies are so-called Jacobs bogies. These Jacobs bogies carry two opposing articles of the multiple-unit train. The powertrain system is located in head wagons. The selected main technical parameters of the diesel multiple-unit train are listed in Tab. 1.

The total power of the entire set is an important parameter from the pointof view of its assessemnt and its possible modification. The multiple-unit train with the hydrogen powertrain should reach the same (or at least approx. the same) parameters regarding to operational properties as the current diesel powertrain, which is currently installed in the train. It allows to achieve the comparable running dynamics, i.e. the traction charactersitics. From the running characteristics point of view, the definition of the following input parameters of the multiple-unit train is essential. There are as follows:

- The traction characteristics;
- Braking characteristics;
- Running resistances.

Moreover, there is necessary to define additional technical parameters, such as geometrical dimensions, maximal braking force, the input power of auxiliary devices and similar. In case of railway tracks, on which the multiple-unit train is supposed to be operated, information about their curve radii and slopes are crucial. As it is assumed, that the multipe-unit train will operate on various types of railway tracks, curve resistance, tunnel resistance and slope resistance should be considered as well [14].

2. THE ORIGINAL POWERTRAIN SYSTEM OF THE MULTIPLE-UNIT TRAIN

The original powertrain system of the multiple-unit train includes two diesel-hydraulic units called as RailPack. These RailPacks are located under the vehicle floor. The power is transmitted by means of cardan shafts to the traction bogies (located in head articles of the train). The RailPack is composed of a MAN diesel combustion engine, a cooling system, a hydrodynamic gearbox with a retarder and a generator for auxiliary devices. The torque is transmitted from the diesel engine crankshaft to the individual wheelsets gearboxes by means of viscous-elastic clutch. A schematic distribution of components in the original diesel multiple-unit train is shown in Fig. 2.

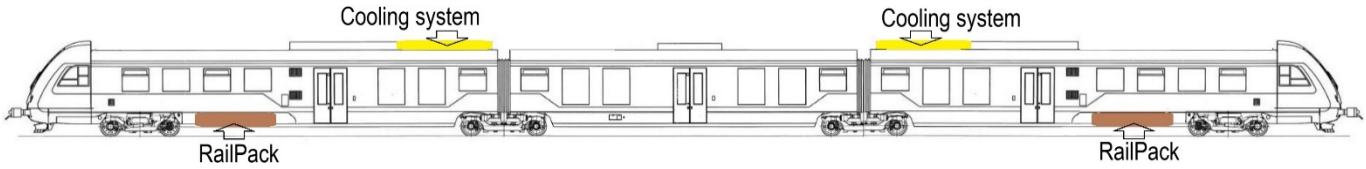


Fig. 2. A scheme of a components distribution in the original multiple-unit train with the diesel combustion engine.

There is necessary to know the energy consumption of the original vehicle for the suggested modification, which is as follows: during the summer period 113.4 kW, during the winter period 101.7 kW. The basic concept of vehicle modification comes from the main requirements:

- Elimination of the original diesel powertrain as a main source air pollution;
- Preserving the original cardan shafts;
- Installation of the hydrogen powertrain;
- Ensuring the needed power for auxiliary devices.

3. THE HYDROGEN POWERTAIN OF THE MULTIPLE-UNIT TRAIN

The vehicle with the original powertrain uses a hot-liquid heating system from the waste heat of the combustion engine. The heating of the vehicle with the hydrogen powertrain will be heated by electric energy. The hydrogen vehicle will be equipped with new traction motors. It is necessary to ensure their cooling by a fan and a corresponding air distribution. A proposal of a distribution of the traction aggregate is shown in Fig. 3.

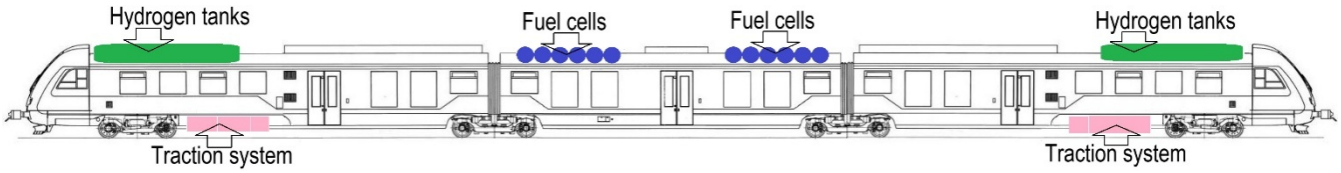


Fig. 3. A scheme of a components distribution in the modified multiple-unit train with the hydrogen powertrain system.

A selection of the main components of the hydrogen powertrain comes from the assumption that it has to be achieved at least the same parameters as for the original diesel multiple-unit train. There were chosen the fuel cells called as Accelera Cummins of the 4th generation (marked as G4+). These fuel cells have two layers. Further, they include a reservoir, a cover, components for the air, components for the hydrogen and control elements. The air input to the cells is ensured by means of variable pressure. A technology of the air moistening is used to improve the average efficiency, and it allows to decrease operational temperature for a better cells distribution. An air intake system includes a filter with a dry cartridge, a chemical cleaning cartridge and connecting tubes. Coolers with fans and a balancing tank are placed on the vehicle roof to ensure proper functionality of the hydrogen fuel cells. As water steam is a side product of the chemical reaction in the cells, it is necessary to exhaust it. This product will be used in hygienic rooms of the vehicle (washing hands, toilets). Hydrogen will be brought to the cells from the tank placed on the vehicle roof. A proper operation is secured by means of safety valves and reductors. Further, a control unit controls not only the functions of individual cells, but also heat management and DC/DC converters. DC/DC converters are located between hydrogen cells and a DC traction intermediate circuit. It serves as the modification of voltage from hydrogen cells to the voltage level of the DC circuit. The main function of the DC circuit is to interconnect hydrogen cells, a traction battery and converters through securing and control elements [15, 16]. A scheme of the power part of the hydrogen fuel cells in the multiple-unit train is depicted in Fig.4 [17]. Fig. 5 shows a scheme, how it is proposed to distribute individual components of the hydrogen fuel cells powertrain in the multiple-unit train.

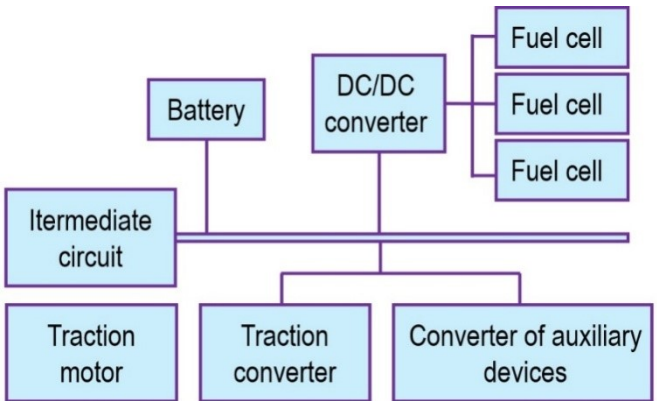


Fig. 4. A scheme of the power part of the hydrogen fuel cells in the multiple-unit train.

A traction converter serves as a converter of electrical energy of the DC traction intermediate circuit of the vehicle for connection of traction asynchronous motors. Three-phase variable voltage with a

variable frequency is the output from the traction converter. Convention of electric energy is controlled by a vehicle control system according to actual requirements for the needed traction power of the vehicle.

It is proposed that the hydrogen tanks will be placed on a raised roof of the vehicle. This raised part of the roof is located from the air-conditioner of a driver up to a location near to the entrance door for passengers. It is necessary to use the maximum of the available free space on the driven articles of the multiple-unit train. Shortened tanks are located behind the driver's air conditioner. The tanks with the standard length are placed on the sides. It will be necessary to modify the placement of the static fans of the air conditioner and air conditioner canals. There is proposed to install cylindrical tanks. The tanks will be different to each other as follows: four tanks with the volume of 400 l., two tanks with the volume of 175 l and additional 7 tanks with the volume of 400 l. The operational pressure of 35 MPa is in all tanks. A distribution of components of the hydrogen powertrain in the multiple-unit train is depicted in Fig. 5.

The modification of the powertrain of the multiple-unit train also requires changing the traction bogies drivetrain. The retention of connected drivetrains of axles through axle gearboxes as well as the main drivetrain by means of a cardan shaft seems to be the most advantageous. The power hydrodynamic gearbox will be replaced by an asynchronous traction motor. An additional reduction mechanical gearbox should be placed between them. Braking system includes a recuperation system, with allows to recuperate energy to increase the batteries voltage. Batteries also required to be cooled [18].

A three-phase asynchronous motor with individual ventilation will be used. The motor has the forced ventilation, Itmeans, that the traction motor should be cooled by an individual ventilation system. Newly mounted traction motors should be also cooled during their operation. Anair-cooling system will be applied, when cooling fan brings the required amount of air to the traction motor.

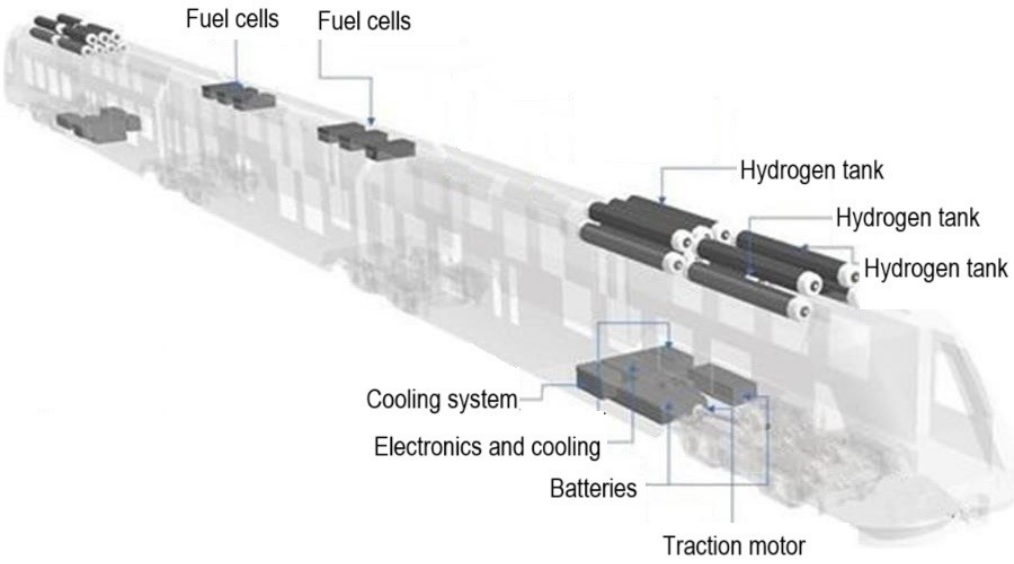


Fig. 5. A scheme of a components distribution in the multiple-unit train.

3.1. ASSESSMENT OF THE LOAD OF THE MULTIPLE-UNIT TRAIN

Based on the chosen concept of the powertrain, there is necessary to perform analyses. On one hand, it is necessary to make a weight balance of the removed and newly added components of the powertrain and subsequently to analyse their influence on the mass distribution to wheelsets and individual wheels. On the other hand, there is an analysis of a dimension layout. It means, that the possibility of placing and layout of new devices and components within the given vehicle contours should be evaluated [17].

Regarding to a design and verifying the wheel and the axle load, there is necessary to considerthe maximal permissible wheelset load of the used bogies, which are applied on the solved multiple-unit train and which should not be exceeded. As it was already described above, the multiple-unit train uses two types of bogies, driving bogies and driven bogies (Jacobs's bogies). Both bogie types allow the maximal axleload of 18.5 t.

In case of an innovation of the powertrain of the solved vehicle, the most important issue is not only the total mass of the traction system, but also evenness of the mass distribution regarding to individual wheelsets (i.e. axleload). The permissible axleloadof the wheelset marked as No. 1, 2, 7 and 8 (counting in a running direction) are a critical point. There is possible the weight increasing only by 100 kg per an axle in comparison with the original diesel multiple-unit train. As it can be seen in a scheme in Fig. 6, the components of the hydrogen powertrain lead to slightly higher position of the centre of gravity.

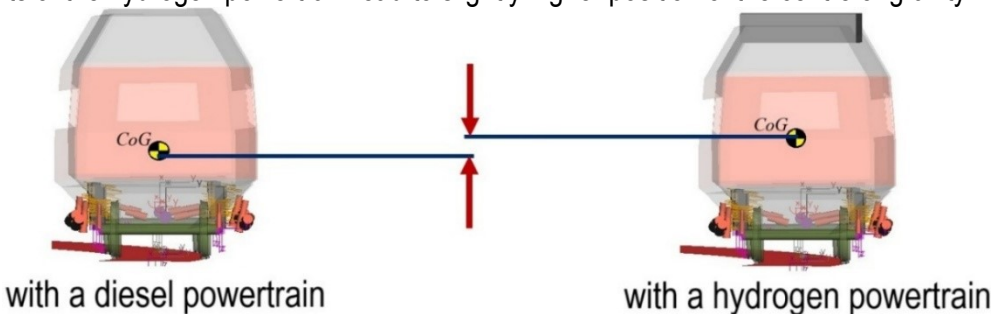


Fig. 6. A comparison of a position of a center of gravity (CoG) of the multiple-unit train with a diesel powertrain (left) and with a hydrogen powertrain (left).

As the results of the simulation analyses have shown [19], the distribution of the components of the hydrogen powertrain is not proper in the primary design. There was found oud, that the maximal axleload was exceededby 1100 kg, what is by almost 6 %. [17]. It is not acceptable, because the used bogies are not dimensioned for such the axleload. As a possible solution, a re-distribution of individual components of the hydrogen powertrain can lead to more favourable even acceptable alxeload. On the other hand, a different distribution of components from the primary proposal requires more significant modification of the rough structure of the vehicle.

CONCLUSION

The current state of the knoweledges about the development of powertrain systems, which use hydrogen as a source of power in the railway transport sector allowed to design a concept of an innovative powertrain syetem of a commercially produced multiple-unit train including hydrogen fuel cells. A proposal design of the vehicle was created based on the availabe data about the selected mutliple-unit train. A distribution of the needed components together with the required modifications of the existing design of the vehicle was processed. Another step was performing a weight evaluation of the vehicle and its comparison with the original vehicle. A distribution of the components needed for the hydrogen powertrain seems, that there are still a space for a modification. The current state showed, that a cricial issue is the exceeded permissible axleload of the vehilce together with the total weight of the vehicle.

The presented research is quite complicated on one hand from a point of view of the needed modifications of the vehicle and on the other hand from a point of view of specificaition of parameters and factors appearing in a real operation of the solved multiple-unit train. The research leads to a conclusion, that the hydrogen powertrain is one of a possible alternative of energy sources in order to sustain mobility and to protect the environment. However, significantly different components of the hydrogen powertrain as well as its specifics require more significant modification of the existing vehicle, which can be one of the limiting factors in a process of changing to alternative non-fossil fuels in passengers rail transport.

ACKNOWLEDGEMENT

This publication was realized with support of Operational Program Integrated Infrastructure 2014 - 2020 of the project: Concept, safety and related industrial research for the replacement of diesel traction by hydrogen fuel cell traction in the railway vehicles series 861 (code ITMS2014+: 313011BVC2), co-financed by the European Regional Development Fund.

This publication was supported by the Cultural and Educational Grant Agency of the Ministry of Education of the Slovak Republic in the project KEGA 031ŽU-4/2023: Development of key competencies of the graduate of the study program Vehicles and Engines.

„Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I03-03-V01-00131."

REFERENCES

[1] S. Fischer and S. Kocsis Szürke, (2023), "Detection process of energy loss in electric railway vehicles," Facta Universitatis, Series: Mechanical Engineering, vol. 21, DOI 10.22190/FUME221104046F, no. 1, pp. 81–99.

[2] A. Malek, R. Taccani, D. Kasparek and J. Hunicz, (2021), "Optimization of energy management in a city bus powered by the hydrogen fuel cells," Communications - Scientific Letters of the University of Žilina, vol. 23, DOI 10.26552/com.C.2021.4.E56-E67, no. 4, pp. E56–E67.

[3] L. Meilus, L. Maskeliūnaitė and H. Sivilevičius, (2025), "Economical comparison of passenger rail traction rolling stock alternatives," Lecture Notes in Intelligent Transportation and Infrastructure, vol. Part F230, DOI 10.1007/978-3-031-85390-6_39, pp. 423-435.

[4] G. Fabri, A. Ometto, H. Li and G. D'Ovidio, (2024), "Redesign of a non-electrified urban railway line with hydrogen-fuelled trains," Lecture Notes in Civil Engineering, vol. 526 LNCE, DOI 1007/978-981-97-4355-1_62, pp. 640-648.

[5] T. Fischer, S. Reinold, M. Lichteberg and M.-A. Sahba, (2024), „Farewell diesel: On the way to climate neutrality using alternative drives and fuels in rail passenger service and rail transport," Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, vol. 238, DOI 10.1177/09544097231174487, no. 3, pp. 284-291.

[6] V. H. S. de Abreu, D. L. Da Ros Hollanda, L. F. C. Proença, L. Bahiense and A. S. Santos, (2024), "A systematic review on renewable hydrogen application in the land transportation sector," Energy, Environment, and Sustainability, vol. Part F2419, DOI 10.1007/978-981-97-0515-3_2, pp. 9-31.

[7] S. Rahim Marjani, S. Motaman, H. Varasteh, Z. Yang and J. Clementson, (2025), "Assessing hydrogen as an alternative fuel for rail transport – a case study," Scientific Reports, vol. 15, DOI 10.1038/s41598-025-90887-3, no. 1, 6449.

[8] T. J. Wallington, M. Woody, G. M. Lewis, G. A. Keoleian, E. J. Adler, J. R. R. A. Martins and M. D. Collette, (2025), "Hydrogen as a sustainable transportation fuel," Renewable and Sustainable Energy Reviews, vol. 217, DOI 10.1016/j.rser.2025.115725, 115725.

[9] S. Wieser, L. Brünner, M. Böhm, M. Soto and E. J. Rodríguez, (2025), „Development, application and optimization of hydrogen refueling processes for railway vehicles," International Journal of Hydrogen Energy, vol. 124, DOI 10.1016/j.ijhydene.2025.04.040, pp. 331–344.

[10] A. Emran, S. Garg, S. Mertes, A. Gautam, M. Schmidt, M. Wick, M. Walters, S. Wagh and V. Sharma, (2024), „Fuel cell electric metro train concept - zero emission rail transport solution for Indian cities," SAE Technical Papers, DOI 10.4271/2024-26-0179, 197403.

[11] A. Nqodi, T. C. Mosetlhe and A. A. Yusuf, (2023), "Advances in hydrogen-powered trains: a brief report," Energies, vol. 16, DOI 10.3390/en16186715, no. 18, 6715.

[12] Z. Xu, N. Zhao, Y. Yan, S. Gao and S. Hillmansen, (2025), "Electric-thermal collaborative system and control for hydrogen-fuel cell passenger trains in the UK's winter," Energy Conversion and Management, vol. 328, DOI 10.1016/j.enconman.2025.119629, 119629.

[13] A. Jakubowski, L. Lipiński, D. Kwiatkowski, D. Karkosiński and N. Karkosińska-Brzozowska, (2024), "Hydrogen fuel cell power supply for hybrid electric multiple unit train," Archives of Electrical Engineering, vol. 73, DOI 10.24425/aee.2024.150894, no. 3, pp. 763-777.
[14] L. Čajkovič, J. Harušinec, M. Pácha and B. Rácek, (2023), "Simulation analysis of traction/braking work and usability of traction characteristics with knowledge of the traction energy parameters of a railway vehicle (in Slovak)," Technológ, vol. 15, no. 4, pp. 51-59.
[15] E. Fedele, D. De Simone, L. Piegari, P. Tricoli and R. Rizzo, (2024), "Multiport traction converter with partial-power-processing DC-DC stage for hydrogen rail vehicles," in 2024 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, SPEEDAM 2024, vol. 2024, DOI 10.1109/SPEEDAM61530.2024.10609044, pp. 363-368.
[16] P. Radziszewski, M. Cierniewski and D. Stachowiak, (2025), "Analysis of energy flow in a rail vehicle powered by a hydrogen fuel cell," PrzegladElektrotechniczny, DOI 10.15199/48.2025.01.60, no. 1, pp. 281 – 285.
[17] J. Krško, (2023), "Concept and structural design of the main drive units when replacing a diesel drivetrain by an electric one with hydrogen fuel cells for DMU r. 861 (in Slovak)," Technológ, vol. 15, no. 4, pp. 22-29.
[18] S. Kocsis Szürke, G. Kovács, M. Sysyn, J. Liu and S. Fischer, (2023), "numerical optimization of battery heat management of electric vehicles," Journal of Applied and Computational Mechanics, vol. 9, DOI 10.22055/jacm.2023.43703.4119, no. 4, pp. 1076–1092.
[19] A. Lovska, V. Ichshuk, J. Dižo and M. Blatnický, (2025), "Analysis of running properties of a rail multiple-unit with a diesel and a hydrogen powertrain," Lecture Notes in Intelligent Transportation and Infrastructure, vol. Part F230, DOI 10.1007/978-3-031-85390-6_49, pp. 527-536.

Ján Dižo: https://orcid.org/0000-0001-9433-392X
Alynoa Lovska: https://orcid.org/0000-0002-8604-1764
Miroslav Blatnický: https://orcid.org/0000-0003-3936-7507
Martin Bučko: https://orcid.org/0009-0006-0566-4430

SYNTHETIC DATA FOR SMART TRAFFIC ANALYTICS

Michal ZABOVSKY[1], Martin MAZUCH[2]

Lead Researcher, Syntelia, s.r.o., Data Analytics and AI, Zilina, Slovak Republic[1]

Researcher, University of Zilina, Faculty of Management Science and Informatics, Dept. of Informatics, Zilina, Slovak Republic[2]

michal.zabovsky@syntelia.tech[1], martin.mazuch@uniza.sk[2]

ABSTRACT: Article investigates the use of computer-generated or synthetic data to enhance AI models used in transportation systems. Difficulties in obtaining sufficient real-world transportation data, particularly for unusual or challenging scenarios, and propose that synthetic data can expand training datasets for AI models to improve their accuracy, reliability, and safety, especially in addressing less common occurrences are discussed. Authors present an application concept using the Unreal Engine 5 physical engine to create realistic 3D virtual environments and are testing the effectiveness of YOLOv8 object detection models on these synthetic scenes, demonstrating promising results for identifying objects even under difficult conditions. The paper proposes use of synthetic data for training to fundamentally improve the resilience and adaptability of transport systems to anomalous situations.

Key words: synthetic data,smart transportation, data analytics, artificial intelligence models, objects recognition

INTRODUCTION

Current transport-related issues in the form of new procedures and methods used to solve traditional optimization and management tasks and new challenges of intelligent mobility require the existence of a sufficient data base for the creation and verification of applied research solutions. Despite the existence of multiple data sources and data storage systems, the availability of original, unaggregated data is problematic due to its time-limited existence, overall size, and the possibility of unambiguous linking with other data sources.

Synthetic data or computer-generated examples (situations/observations) enable the expansion or replacement of real data to accelerate the training process of artificial intelligence models with the aim of improving the model or its selected parameters overall.

Obtaining real data in transport systems is generally expensive, time-consuming, and, in the case of new models, usually impossible. In contrast to this situation, the use of synthetic data is suitable for capturing specific situations in data used to train artificial intelligence models with the aim of increasing the accuracy and reliability of predictions and ensuring the overall resilience and safety of the models created. Another important reason for using artificially generated data is the restrictions imposed by legislation on personal data protection and copyright.

Synthetic data in the field of transport is created regarding specific needs or descriptions of certain model situations that may not be found in the original, real data. This can be useful when creating any predictive model, as such data can be used to simulate situations that are not captured in real data but are known to occur. It is also useful to use such data if we want to eliminate certain results of predictive models, especially when using specific artificial intelligence methods.

In this article, we present an application-based concept for improving predictive and interpretative models based on existing data using generated synthetic data and its use for assessing and designing new transport modes and solutions. Structure of the paper is following- Introduction presents motivation for research based on real-life needs, Related work section shortly summarize current research related to the discussed topic, while Problem definition section defines problem area together with references to the research papers. Proposed solution shows outputs from our environment implemented in 3D

physical engine Unreal Engine 5 as the input data for AI models training. Finally, Conclusion and Future work sections conclude the article and presents next research steps.

RELATED WORK

The boom in synthetic data-based solutions followed the widespread acceptance of AI models for solving complex problems in the last 4 years. This is mainly due to an improvement in the overall interpretability of models based on so-called black-box methods in the field of deep machine learning. Models themselves, focusing on interpretation instead of overall predictive power, are preferred precisely in the field of transport and understanding of complex systems.

Based on the overview of existing synthetic data companies, one can see a relatively small number of existing companies that provide synthetic data and prepare it as a service [1]. These are in the order of dozens of companies, with a substantial increase in creation dating back to 2019 and 2020. Overall, these companies can be divided into a) structured synthetic data providers (e.g. Generatrix, Mostly AI, Ydata), b) unstructured synthetic data providers (Anyverse, Datagen, Deep Vision Data, OneView, Zumo Labs), and c) providers of structured synthetic privacy-oriented synthetic data (Betterdata, Mostly AI, Statice) [1] [2]. Specifically, a large group of these providers focus on the areas of healthcare, testing data creation, and partly on academia. The field of transport is not represented in a specific way, one of the options is to use the services of companies operating in the field of physical gaming environments, such as Unity or Unreal Engine [3, 4].

In the field of academic research, a breakthrough is the work and tutorial for generative adversarial networks (GAN) [5], published in 2017 by Ian Goodfellow of OpenAI. [6] The original GAN worked on examples of simple datasets such as MNIST (handwritten digit database) [7]. One of the first truly successful architectures based on these principles was Deep Convolutional GAN (DCGAN) [8]. It used a fully convolutional, maxpooling-free architecture (using incremental convolutions), added batch normalization layers, used the Adam optimizer (which was new at the time), and added a few other improvements to improve results. As a result, DCGAN learned to generate very reasonable interiors on an LSUN dataset (a dataset of color images of 64 × 64 pixels).

PROBLEM DEFINITION

Currently, there are several data sources available in the Slovak Republic under the authority of different data holders related to the issue of modeling of transport systems [8]. Within the existing cooperation and partnerships we were able to obtain data for specific types of tasks, but it is not possible to obtain data for certain types of tasks related to the transport systems due to the absence or aggregation of source data. These include data recorded at different time intervals than is currently common due to the registration of vehicle crossings (hourly intervals), data from accidents, near-miss incidents or data obtained during the occurrence of emergencies.

The solution is to use existing data and supplement them (replace) with data created artificially – synthetic data. To create new samples, either advanced techniques of real data modification (augmentation) or artificial data generation are used, which falls within the field of research on the preparation of synthetic data.

The most promising way to create synthetic data for transport systems appears to be the use of generative modelling techniques. The generative model describes how a set of data is generated in the sense of a probabilistic model. By sampling from this model, we can generate new data. The existing procedures are mainly focused on the area of creating artificial image data, which in the case of transport systems allows the generation of model situations serving as training data for AI models used for traffic recognition situations, automated driving, identification of security incidents, etc. In addition, the use of generated data allows the incorporation of various meteorological and light phenomena occurring in the real environment and thus the verification of models in a wide range of potentially occurring situations, even though their real occurrence has a low probability of occurrence in the real data.

The AI-based procedures currently used to analyze traffic data are based on discriminatory models, where within the model learning takes place to obtain a conditional probability p(y|x), where there is an input data vector x and a target variable y. In the case of the present project, the aim is to create generative models where the aim of learning is to obtain a common distribution p(y,x) or p(x), alternatively, to create samples from the input data set. In principle, the use of generative models is more difficult than the use of discriminatory models, since in the case of generative models to obtain p(y|x) it is enough to calculate p(y,x) for all values y and normalize result, which in the case of classification tasks is a solvable problem. However, the fundamental problem is that there is no clear way to move from p(y|x) to p(y,x) [10].

The issue of generating synthetic data for neural networks solving specific tasks in transport began to be addressed in the early days of adaptation of artificial intelligence models. Simard et al [11]. used distortions to expand the MNIST training file back in 2003, and it is uncertain whether this is the very first use in transport. The MC-DNN network, arguably the first truly successful deep neural network for computer vision, also used similar extensions, although it was a relatively small network trained to recognize relatively small images (road signs) [10].

However, whole proces of preparation requires training data. As most of the datasets dealing with resilience and crisis events are highly unbalanced, we focused on generation of image data with challenging conditions or accidental situations. E.g. Tian et al. present a set of synthetic data ParallelEye [12] for scenes from urban environments. Their approach relies on the previously developed Esri CityEngine framework [13], which provides capabilities for batch generation of 3D urban scenes based on terrain data. In the test app, this data was automatically extracted from the Open-StreetMap2 platform. The 3D scene was then imported into the Unity game engine, which made it possible to add vehicles to the roads, set traffic rules, and add support for different weather and lighting conditions. Tian et al. showed an improvement in object detection quality for state-of-the-art architectures trained on ParallelEye and tested on a real KITTI test set compared to training on a real KITTI training kit [10].

Synthetic datasets with explicit 3D data (with simulated sensors) for the outdoor environment are less common, although it seems that such sensors are easy to include in the hardware of autonomous cars. In the development of architecture SqueezeSeg Wu et al [14]. added LiDAR simulator to the computer game Grand Theft Auto V and collected a synthetic set of data from the game. SynthCity by Griffiths and Boehm [15] is a vast open synthetic data set that is essentially a huge cloud of urban/suburban environments. It simulates the work of a mobile laser scanner (MLS) with the Blender plugin [16] and is specially designed for pre-training deep neural networks [10].

PROPOSED SOLUTION AND EXPERIMENTS

To receive as realistic data as possible, we created series of 3D virtual environment using physical engine Unreal Engine 5.An essential motivating factor is the ability to create inputs for AI models that prevent the models created fromgenerating erroneous decisions that, for example, a human would not commit or recognize that they are wrong.Foundation of data came from camera systems located in the city of Zilina and cameras located in vehicles. We use the database of image data to detect objects in the direction of travel of the vehicle, vehicles in parking lots, pedestrians, and dynamic traffic [17]. We also have part of the data for object identification and segmentation in the form of cloud points from 3D scanning (static, aerial). However, for specific types of objects that do not have a well-defined character (potholes, water on the road, light-affected parts, but also traffic density), we do not have sufficiently large data sets that we can use to better create prediction models.

We prepared synthetic scenes from 3D physical based simulationsprepared in Unreal Engine 5. Image data from scenes can be used as raw scene data or parametrized for challenging conditions (weather, lights, rain, etc.). For the experimental evaluation we used 4 images rendered directly from Unreal Engine 5. Two of them were additionallypostprocessed with AI model Sora. [18]Sora is a text-to-video model developed by OpenAI. The model generates short video clips based on user prompts and can also extend existing short videos (see Fig. 1).

a) b)

c) d)

Fig. 1. Generated scenes for objects recognition – a) T-junction in rainy night, b) T-junction in rainy night improved by AI, c) Road works in sunny day improved by AI, d) Road work in shadows.

Specific special conditions are low visibility, reflections, shadows, obstacles and others like in specific situations in real life. All the images are cuts from simulated video sequence and thus, other specific images could be easily generated if necessary.As seen, all images were generated for challenging conditions. Images have different size dimensions and size (1483x894, 1536x1024, 1536x1024, and 1414x796 pixels, 2.2, 1.5, 3.0, and 1.8 MBytes).

For object recognition purposes we used YOLOv8 model trained on COCO dataset.[19] YOLOv8 (You Only Look Once version 8) is version of the popular real-time object detection model family developed by Ultralytics. It builds upon previous YOLO versions and introduces several improvements in performance, flexibility, and ease of use. The motivation is its overall performance, real-time character and capability for real-time video surveillance, autonomous driving, anddrone vision.

Tab. 1.YOLOv8 models for objects detection.

	Size (pixels)	mAP (50-95)	CPU speed (ms)	Layers	Parameters	GFLOPs
yolov8n.pt(nano)	640	37.3	80.4	168	3 151 904	8.7
yolov8s.pt(small)	640	44.9	128.4	168	11 156 544	28.6
yolov8m.pt (medium)	640	50.2	234.7	218	25 886 080	78.9
yolov8l.pt (large)	640	52.9	375.2	268	43 668 288	165.2
yolov8x.pt (huge)	640	53.9	479.1	268	68 200 608	257.8

We selected group of models prepared for object detection of different robustness (layers and parameters, Tab. 1) with confidence level 0.25.Ultralytic's YOLOv8 version 8.3.40, Python version 3.11.5, and PyTorch library version 2.7.0 were used during the experiments. Experimental results are shown in the Tab. 2 and Tab. 3 respectively, where we are trying to detect 4 cars for scenes a) and b), traffic lights and potential obstacles/barriers for scenes c) and d).

Tab. 2. Experimental results for T-junction synthetic scenes (4 cars).

Scene	Model	Cars detected	Confidence	Inference speed (ms)
A: Rainy night	yolov8n.pt	4	0.94 / 0.61 / 0.64 / 0.33	28.6
	yolov8s.pt	4	0.95 / 0.90 / 0.84 / 0.75	52.1
	yolov8m.pt	4	0.95 / 0.89 / 0.88 / 0.85	107.0
	yolov8l.pt	4	0.95 / 0.61 / 0.82 / 0.84	176.0
	yolov8x.pt	4	0.96 / 0.92 / 0.90 / 0.88	257.9
B: Rainy night (AI)	yolov8n.pt	3	0.95 / 0.93 / 0.59 / -	29.8
	yolov8s.pt	4	0.95 / 0.94 / 0.88 / 0.75	59.6
	yolov8m.pt	4	0.96 / 0.95 / 0.87 / 0.71	124.5
	yolov8l.pt	4	0.97 / 0.91 / 0.88 / 0.82	207.0
	yolov8x.pt	4	0.96 / 0.95 / 0.89 / 0.86	274.3

Tab. 3. Experimental results for road work synthetic scenes (1 light, 7 barriers*).

Scene	Model	Light / barriers detected	Confidence light	Confidence barriers(max / min)	Inference speed (ms)
C: Road work sunny (AI)	yolov8n.pt	1 / 1	0.87	0.36	29.8
	yolov8s.pt	1 / 6	0.84	0.75 / 0.36	60.2
	yolov8m.pt	1 / 3	0.87	0.60 / 0.41	123.2
	yolov8l.pt	1 / 0	0.90	-	201.8
	yolov8x.pt	1 / 0	0.90	-	272.2
D: Road work shadows	yolov8n.pt	2** / 0	0.61	-	25.9
	yolov8s.pt	1 / 2	0.79	0.42 / 0.39	49.5
	yolov8m.pt	1 / 1	0.86	0.60	104.9
	yolov8l.pt	1 / 4	0.91	0.39 / 0.35	173.2
	yolov8x.pt	1 / 5	0.93	0.71 / 0.29	242.3

* Barriers are not exactly presented in the training COCO datasets for objects detection
** Same traffic light was detected twice with low confidence

As can be seen, objects such as cars and traffic lights were identified with high accuracy. Cars in scenes a) and b) were better identified in the scene modified using AI, as were vehicles that were not obscured by other vehicles (camera angle) (Fig. 2). The traffic light indicating road works was reliably identified in the scene without shadow overlap. A more robust model can be used in the case of shadows. An interesting case occurred with traffic barriers, which are not part of the COCO training dataset. Despite this, the TOLOv8 model identified them as other objects, but the detection is not very reliable.

Fig. 2. Results for T-junction sceen improved by AI (scene B) obtained by yolov8s.pt model (168 layers, 11.2 M parameters).

CONCLUSION

Based on the use of generated scenes, it can be said that such data can be used for models that were created using real data to verify their properties in rare situations and difficult conditions. This fact demonstrates the usefulness of our proposed approach of using synthetic data as a substitute for hard-to-obtain real data.The originality of proposedsolution is determined by its application domain in the field of transport, namely increasing the safety and resilience of the transport system by detecting phenomena that cannot be sufficiently captured by the collected real data. The application of the created models and their results contributes in a fundamental way to the better usability of solutions based on them in application practice. While real-world data alone may be sufficient to address typical, easily predictable scenarios, there is still a gap in the protection and resilience of systems in dealing with anomalous situations. Gathering big data through synthetically generated data for a range of scenarios allows target wide range of challenges for the emergence of truly intelligent systems [20].

FUTURE WORK

The correlation of inputs and their redundancy are analyzed by the potential redundancy of phenomena in the transport system. The principle of confrontational interactive training of the generative model will make it possible to eliminate the problem of small training sets in the case of situations related to the resilience and adaptation of the transport system. By practicing GAN confrontation and using a classification network, an improvement in system detection accuracy can be achieved. Subsequently, we will apply random noise and the principle of mixing data to create new training sets.The goal for future work is to create a model for the continuous generation of synthetic data usable for increasing the robustness of transport.

REFERENCES

[1] E. Devaux, “List of synthetic data startups and companies — 2021”, 2021. [Online]. Available: https://elise-deux.medium.com/the-list-of-synthetic-data-companies-2021-5aa246265b42.

[2] E. Devaux,“[New] List of synthetic data vendors— 2022”, 6 10 2022. [Online]. Available: https://elise-deux.medium.com/new-list-of-synthetic-data-vendors-2022-f06dbe91784.

[3] Unity Technologies, “Unity”, 2025. [Online]. Available: https://unity.com/.

[4] Epic Games, “Unreal Engine”, 2025. [Online]. Available: https://www.unrealengine.com/en-US.

[5] I. Goodfellow, (2017),“NIPS 2016 Tutorial: Generative Adversarial Networks”, arXiv, 2017.

[6] OpenAI, “OpenAI”, 2025. [Online]. Available: https://openai.com/.

[7] Wikipedia: The Free Encyclopedia, “MNIST database”, 2024. [Online]. Available: https://en.wikipedia.org/wiki/MNIST_database.

[8] A. Radford, L. Metz, S. Chintala, (2016)“Unsupervised representation learning with deep convolutional generative adversarial networks.”, rev. 4th International Conference on Learning, JCLR 2016, San Juan, Puerto Rico, 2016.

[9] Ministerstvodopravy a výstavbySlovenskejrepubliky / Ministry of Transport of the Slovak Republic, “Metodickápríručka k zostavedopravnýchmodelov a dopravnýchprognóz / Methodological guide to the compilation of transport models and transport forecasts”, 2021.

[10] S. I. Nikolenko, (2021), “Synthetic Data for Deep Learning”, Springer, 2021.

[11] P. Simard, D. Steinkraus, J. Platt, (2003), “Best practices for convolutional neural networks applied to visual document analysis.”, rev. Seventh International Conference on Document, 2003.

[12] Y. Tian, X. Li, K. Wang, F.-Y. Wang, (2018), “Training and testing object detectors with virtual images”, IEEE/CAA Journal of Automatica Sinica, Vol. 5, No. 2, pp. 539-546, 2018.

[13] X. Hu a et al., (2013), “Batch modeling of 3D city based on ESRI cityengine“, rev. IET International Conference on Smart and Sustainable City 2013 (ICSSC 2013), 2013.

[14] B. Wu, A. Wan, X. Yue, K. Keutzer, (2017),“Squeezeseg: Convolutional neural nets with recurrent CRF for real-time road-object segmentation from 3d lidar point cloud.”, CoRR, 2017.

[15] D. Griffiths and J. Boehm, (2019), “SynthCity: A large scale synthetic point cloud.”, arXiv, 2019.

[16] M. Gschwandtner, R. Kwitt, A. Uhl a W. Pree, (2011), “Blensor: Blender sensor simulation toolbox.”,rev. Advances in Visual Computing, Berlin, Springer, 2011, pp. 199-208.

[17] B Bucko, E.Lieskovska, K.Zabovska, M. Zabovsky, (2022), “Computer vision based pothole detection under challenging conditions”, Sensors, 2022.

[18] OpenAI, “Sora”, 2025. [Online]. Available: https://openai.com/sora/

[19] Ultralytics, “Explore Ultralytics YOLO v8”, 2025. [Online]. Available: https://docs.ultralytics.com/models/yolov8/

[20] S. Harris, (2022), “Why Synthetic Data Is Key To Paving the Way for Smart Cities”, 17 11 2022. [Online]. Available: https://www.spiceworks.com/tech/innovation/guest-article/why-synthetic-data-is-key-to-paving-the-way-for-smart-cities/.

Michal Zabovsky: https://orcid.org/0000-0002-3014-6399

CERAMIC MATERIAL WITH NANOPARTICLES INCREASED MAGNETIZATION WITH DIFFERENT CHROMIUM CRYSTALLINE STRUCTURES USING GREEN CHEMISTRY

Pedro VERA-SERNA[1], Luis A. GARCIA-CAMACHO[2]

Universidad Politécnica de Tecámac, División de Ingenierías, Centro de Ingenieria Avanzada, Tecámac, Estado de México, México[1,2]

Author's e-mail[1]: pedrovera.upt@gmail.com, author's e-mail2: armando.camacho101@outlook.com

ABSTRACT

This research is oriented towards the synthesis of materials with possible applications in electronics due to their magnetic response and the observed ceramic phases, as well as the generation of knowledge regarding the modification of properties based on the characterization of advanced materials by using solid state reaction and being considered as green chemistry processes. The process started with a stoichiometric chemical balance of iron and chromium oxides, then they enter a mechanochemical process at different times, in which the material is characterized, identifying the modification in its crystalline structure, the variation of particle size to nanometers, morphology and magnetization increase and the relationship between them, determining a variety of reactions that result in a superior magnetic response compared to previously published information. The techniques used were X Ray Diffraction, Scanning Electronic Microscopy, Analysis of Particle Size Distribution and Vibrating Sample Magnetometry.

Key words: advanced nanomaterials, magnetic materials, synthesis of ceramics, iron (II) chromite, green chemistry

INTRODUCTION

In recent years, the research and development of advanced materials has received significant attention due to their diverse applications in electronics, energy storage, environmental technologies, and others applications[1]. The need to adopt more sustainable practices within the industry has driven this advancement, leading to the integration of green chemistry in synthesis and manufacturing processes [2]. In green chemistry, emphasis has also been placed on developing sustainable solid-phase synthesis methods that use fewer solvents and reduce the use of hazardous materials. These methods allow magnetic materials to be obtained by mixing solidprecursors and sintering them, improving the energy efficiency of the process [3].In this context, various ceramic advanced materials composed mainly of iron and chromium, has been studied for its intrinsic properties and potential to contribute to a future with advanced products and systems [4].One of the most relevant characteristics of chromium ferrite and iron chromite is that they are oxide ceramics that can be processed using methods in solid state which minimize waste generation and pollutant gas release. Through green chemistry implementation, chromium ferrite synthesis processes have become more efficient, using less hazardous solvents and reducing energy consumption [5]. These approaches today also maximize recyclability, making chromium ferrites valuable in the transition to cleaner technologies [2]. Studying these ceramics involves various techniques to evaluate their structural, physical, and chemical properties, which is crucial for understanding their performance in different applications [6].

In materials researchis necessary the characterization techniques to evaluate changes during the process. One such technique is X-Ray Diffraction (XRD), which identifies the crystalline structure of materials. It is especially useful for analyzing materials with crystalline arrangements, such as minerals, metals, ceramics, and some polymers. This tool has confirmed that some ferrites and chromites have a spinel-like structure with an ordered arrangement of cations in the crystal lattice. This arrangement is

related to magnetic moments, which modify the material's response to external magnetization fields [7]. Scanning electron microscopy (SEM) is another widely used technique in the modification and development of advanced materials, traditionalm ceramics and smart materials. It allows one to observe the surface of samples with high resolution. This technique has been used to observe the morphological characteristics, particle size, distribution, and shape of particles. SEM also provides information on the microstructure, which is crucial to understanding the mechanical and thermal properties of these materials [8].Due to the advances in the last decades it has been observed that the Particle Size Distribution Analysis (PSDA) technique helps to correlate the magnetic properties as a function of the nanometric sizes reached, in some cases derived from the change of dimensions of the bloch walls [9]. Finally, another fundamental study is the evaluation of the magnetic response of the material along the process, which allows to observe advances for applications or knowledge generation [10].These techniques allow us to determine the physical and structural properties of chromium ferrites or iron chromites and understand how their composition and microstructure affect magnetic, electrical, and mechanical properties. This knowledge is crucial for their performance in various applications [11] [7].

In recent decades the synthesis methods in advanced materials have evolved to improve material properties and align with green chemistry principles, reducing environmental impact and production costs [1][2]. The most commonly used methods are the Sol-Gel it is a bottom-up process in which a liquid solution (the "sol") is transformed into a gel (a solid network in a liquid phase) through chemical reactions. The gel is then dried and calcined (heated) to obtain the desired solid material, often at the nanometer level. The sol-gel process is popular for synthesizing chromium ferrites due to its ability to produce materials with controlled particle distribution and homogeneous mixtures of reagents. The hydrothermal synthesis method involves reacting precursors under high-pressure and -temperature conditions in the presence of water. This method has proven effective in fabricating chromium ferrites with nanometric structures [12].

Due to its unique properties, chromium ferrite has a wide range of applications that continues to expand. Some of the most prominent applications in recent years respond to magnetic fields in various ways: attraction, repulsion, and generation. Their response depends on the atomic structure and electron spin behavior within the material [4, 6,10], 11, 13]. Chromium ferrites are used in the fabrication of magnetic materials, such as magnets and data storage materials. Thanks to their high thermal and magnetic stability, chromium ferrites have been implemented in electronic devices, including magnetic sensors and memory devices, which require stable, high-quality magnetic properties [6, 11, 13]. They have applications in power electronics because they are highly efficient in converting and transmitting energy. This is fundamental for renewable energy systems and low-power electronics [7,13]. Other applications include use as catalysts and sorbents because their structure facilitates interaction with various chemical compounds. One technological advance is the development of new generations of batteries and supercapacitors. These electrochemical devices store and convert chemical energy into electrical energy through redox reactions.However, chromium ferrites have displaced this technology due to their use in developing new battery materials. These materials offer electrochemical stability, making them suitable for energy storage applications, such as rechargeable batteries and large-scale systems for renewable energy sources [6, 11, 14]. Thus, their applications remain of interest from a technological standpoint.

This work presents the results of evaluating advanced materials obtained by mechanochemical processes within a green chemistry framework. The evaluation is based on precursor materials of Cr_2O_3 and Fe_2O_3, and the magnetization results are analysed in relation to those reported in the literature. The work also presents phase changes in the structure of the obtained material, which are related to particle size variation, and shows images of the obtained morphology.

1. CONCEPTULIZATION

Spinel and orthorhombic structures have been identified in soft magnetic advanced materials. These structures can be obtained through solid-state reactions by alternative methods. The evaluation of magnetic saturation has increased compared to previous publications, in which particle size was related to increased magnetization. In this work, we used Cr_2O_3 and Fe_2O_3 precursor materials to obtain ceramic $FeCr_2O_4$ if is possible. We evaluated the structural changes from the precursor materials and during the milling process for twelve hours. The images of material were taken by a scanning electron microscope (Fig. 1), and the most representative ones are presented. Since there is no previous work on the entire process, these findings contribute to the generation of knowledge.

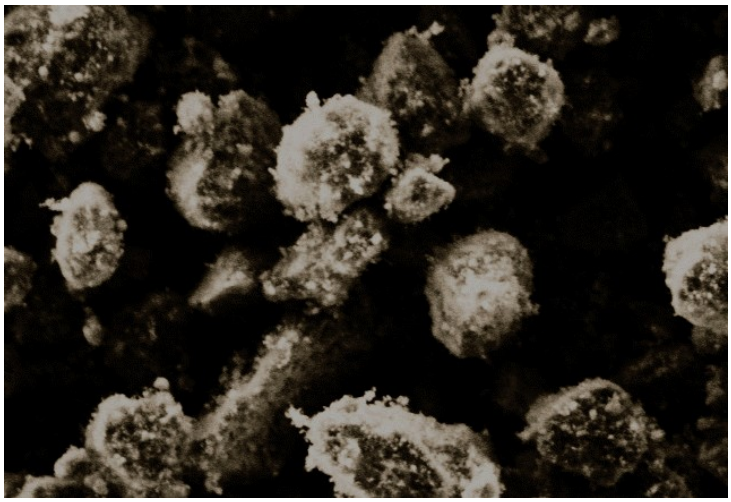


Fig. 1. Powders obtained by milling processusing Fe_2O_3 and Cr_2O_3.

2. MATERIALS AND METHODS

The methodology begins with selecting the precursors materials to be used.Previous literature has shown that $Fe_2O_3$and Cr_2O_3can generate a structural change and improve the magnetization level [11].In addition, modifications in themagnetization were observed. Then, characterization techniques were then selected.

2.1. MATERIALS

Precursor materials from the Sigma-Aldrich brandwith a purity greater than 99%. These materials included Fe_2O_3 and Cr_2O_3. These precursors, together with steel spheres, were used.The hardened steel spheres, measuring 12.7 mm, were placed in stainless steel vials.For the determination of the size distribution,Darvan 7N, a dispersant from Vanderbilt, was used in the measure process while the particles were separated in an ultrasonic bath to have the conditions to evaluate the particle size distribution.This approach is based on previous references in the literature.

2.2. EQUIPMENT

The high-energy mill used in the process was a Spex 8000D mixer/mill. To determine the crystalline phases in the material, a Bruker D8 Advance X-Ray Diffractometer with 1.6 kW and Cu radiation (λ= 0.14051 Å)and a LYNXEYE XE detector was used. The analysis was supported by EVA software and the PDF2 database. The magnetometer used was a Microsense EV7 vibrating sample magnetometer. The particle size analyzer was a Brookhaven Nanobrook 90 Plus. The images or the materials were obtained with Scanning Electronic Microscope JOELmodel JSM- 6000 in high vacuum with 10 kV.

2.3. PROCEDURE

Materials were selected which had managed to interact in previous works with $Fe_2O_3$and Cr_2O_3as presented in the introduction giving rise to different compounds [11], Chromium material was of particular interest due to their applications and that they have managed to replace iron which gives viability to this work, after that a stoichiometric balance was performed to have a certain control.After that, they were inserted in the 60 cm^3 stainless steel vials, the milling was started for several hours, observing that favorable results have been obtained in similar works of other authors after 12 hours, the characterization was carried out with X-Ray Diffraction to determine the crystalline structural changes of the phases, it was also necessary to observe in the scanning electron microscope the morphologies that developed with the milling process An important point was to determine the smallest particle sizes that were reached for which the analysis by particle size distribution was applied, in this procedure the grinding particles were previously entered into an ultrasonic bath with a few drops of dispersant, finally the characterization was performed with the magnetometer as shown in Fig. 2.

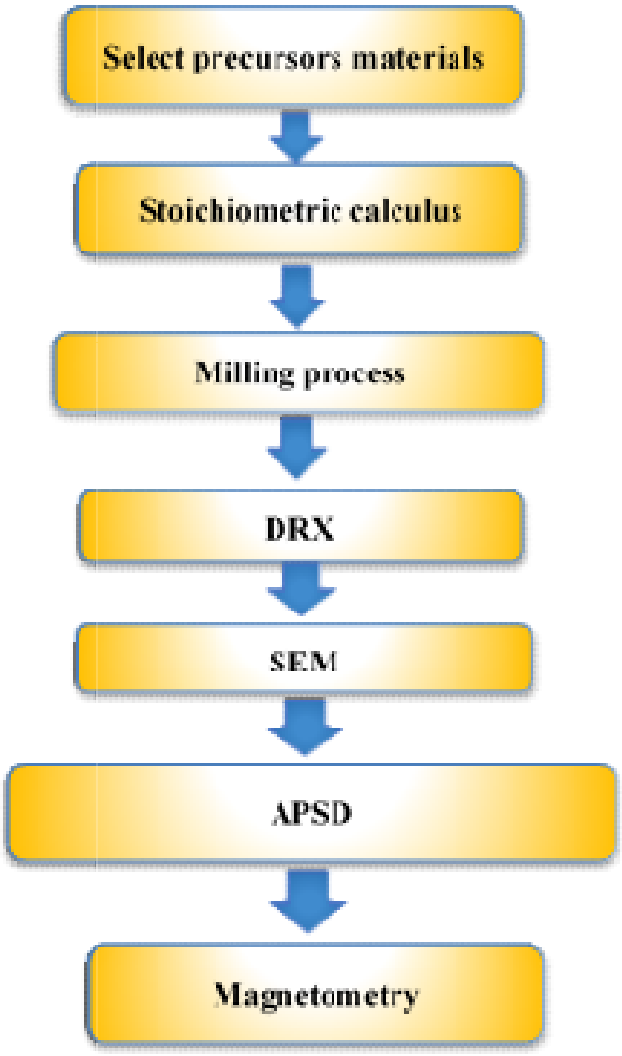


Fig. 2. Experimental process.

3. RESULTS AND DISCUSSION

The results presented are those obtained up to 12 hours of milling. It is possible to observe modifications in the crystalline structure, in morphology, identification of nanometric particle sizes, and magnetization of the obtained material.

3.1. X-RAY DIFFRACTION

The results obtained by XRDdemonstrate variousmodifications on crystalline structure, which is associated with the values obtained from the magnetization analysis. The analysis reveals a concurrence of the peaks with those corresponding to the iron (II) chromite phase are with higher intensity on 12 hours of milling, while over 3 hours of milling the structure was modified.A secondaries phases that is chromium ferrite, chromium iron and precursors oxides were identified with database PDF2+ and EVA software, which $FeCr_2O_4$(PDF 01-075-3312) exhibits an spinel structure, while $(Cr_{0.6}Fe_{0.4})_2O_3$(PDF 00-034-0412) has been reported withrhombohedral structure and $Cr_{0.2}Fe_{0.8}$(PDF 01-071-7535) with cubic system. The preceding discussion indicates that the mechanochemical process was successfully employed to generate ferrite and chromite (Fig. 3).

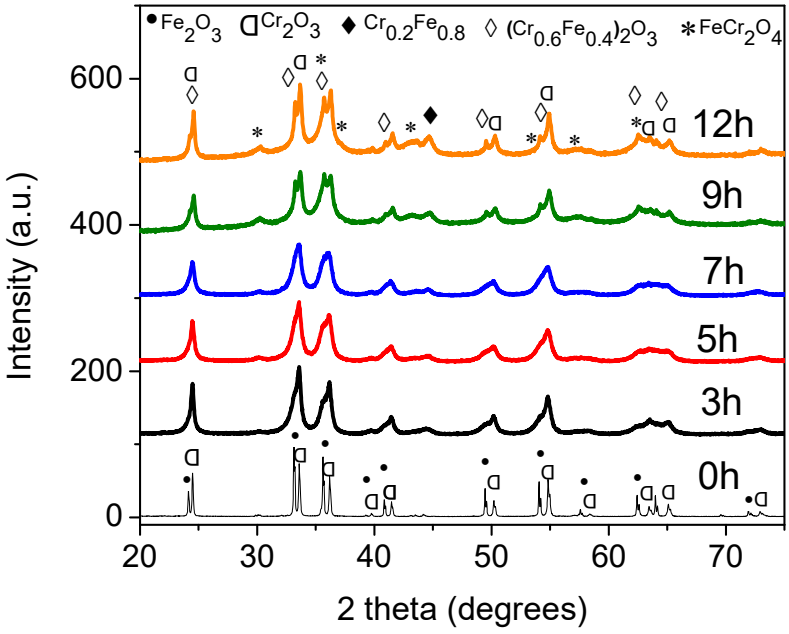


Fig. 3. XRD profiles during the process of green chemistry.

3.2. SCANNING ELECTRON MICROSCOPY

The results of Figure 4,obtained by scanning electron microscopyrevealed the integration of precursors materials, giving rise to irregular particles with a tendency toward compacted arrangement. A certain homogeneity was observed in agglomerates on 5 and 7 hours, the milling generate reactive surfaces in particles, while on 9 and 12 hours increase the agglomerates (in SEM the dispersant was not applied), it can be attribuible to the changes in structure and the milling traditional process, it is a reduction when start the process and welding the flakes with the energy impact on material. The milling process achieved this integration at room temperature and produced a more homogeneous material containing a clear phases of $FeCr_2O_4$ on 12 hours. These elements exhibited variations in magnetic response, which will be discussed later.

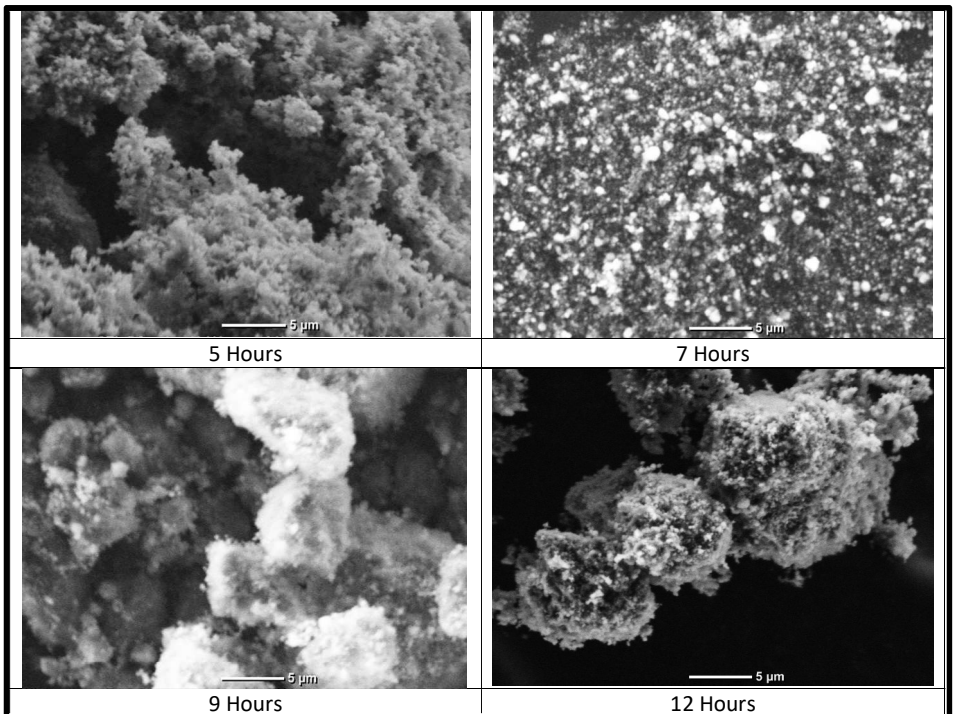


Fig. 4. Morfology of particles and agglomerates on 3400X scale.

3.3. PATICLE SIZE DISTRIBUTION

As shown in Figure 5, the graphic begins with the particle size measured after three hours of milling. These measurements were taken using Brookvaven equipment. The initial distribution shows a significant presence of particles between 30 and over 300 nanometers. The second specimen, which was subjected to milling for a duration of five hours, exhibited an augmentation in its particle size. This observation aligns with the images obtained from the SEM derived from the welding of particles. The utilization of high-energy milling in this process resulted in the observed enhancement in particle size. As shown in Figure 4, the milling process over a period of seven hours leads to a reduction and homogenization of particles. This is consistent with the image of the powders obtained. The results of the nine-hour milling process indicate a decrease in the major distribution, with the majority of the distribution falling below 100 nm. This facilitates the agglomerates, as illustrated in Figure 4, and generates new reactive surfaces on the particles. This, in turn, allows for reactions and modifications to the crystalline structure, as demonstrated in Figure 3. Finally, the curve of milling time at twelve-hours showed a particulate size distribution between 94 and 224 nanometers. This is due to the deformation of the powder during the process. A secondary distribution is observed around 30 and 60 nanometers. This modifies the magnetic moments and facilitates the formation of a spinel structure, as demonstrated in Figure 3. The milling process generates products of varying sizes, and it is interesting to note that we are able to measure and compare the particle sizes of the nanoparticles. We observed the finest results in determining particle size when using the Spex 8000D mill in conjunction with chromium and iron oxide III. These results were compared with those from the SEM photos, and they showed the same tendency. I am pleased to inform you that the ultrasonic bath and Darvan 7N were effective in separating the agglomerates. By identifying cost-effective materials while maintaining those levels of magnetization, we can leverage them to develop new products.

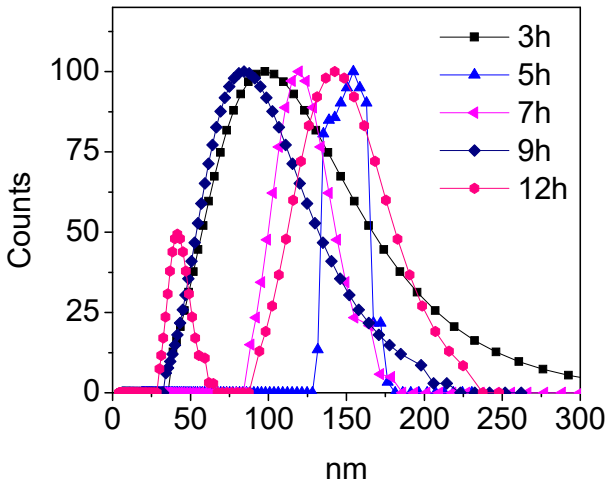


Fig. 5. Particle size behavior during the synthesis process.

3.4. MAGNETIZATION

The results observed on magentization were in Figure 6, the material's magnetization performance exceeds that of the $FeCr_2O_4$ phase. According to the literature, the value is approximately 2 emu/g and 1 emu/g [10,15]. The maximum value at 18,000 Oe corresponds to 10.59 emu/g. This can be attributed to the structural arrangement, which integrates elements of the material to create a spinel structure. This process takes 12 hours of milling, during which time an increase in magnetic moments is generated and the material's response to an external magnetic field is facilitated. The literature has discussed another effect that increases magnetization: the use of nanometric particles. The green process applied to precursor materials demonstrated an enhancement in the capacity to maintain magnetization. The values were observed to be consistent between 3 and 9 hours of milling. The research identified it method as an alternative method for producing electronic materials used in engineering. This method was developed in temperature-resistant room avoids the use of temperatures over 1200°C, ensuring environmental friendliness.

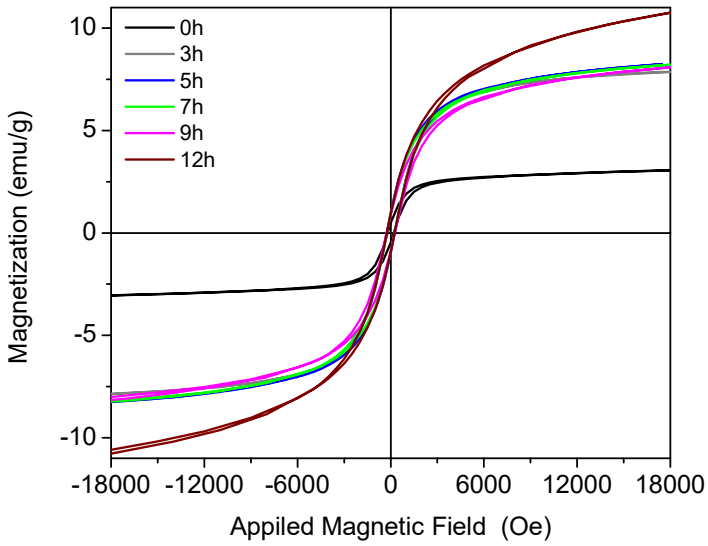


Fig. 6. Magnetic histeresys in different times of milling.

CONCLUSION

From green chemistry processes such as solid state reaction by mechanochemistry at room temperature, it was possible to document and generate knowledge of the synthesis reaction of advanced materials that gave rise to different crystalline phases of ferrite and chromite that emerged from the precursors Fe_2O_3 and Cr_2O_3, observing in the product an irregular morphology which was decreasing in size according to the particle size distribution analysis, appreciating a proportional relationship when determining spinel type structures by X-ray diffraction, nanometric sizes particles and the increase of magnetization after 12 hours of milling, obtaining a material with structures $FeCr_2O_4$, $(Cr_{0.6}Fe_{0.4})_2O_3$, $Cr_{0.2}Fe_{0.8}$ and precursors too. The magnetization reached values of 10.59 emu/g which are higher than those reported in the literature around 2 and 1 emu/g, giving rise to a soft magnetic material behavior.

REFERENCES

[1] M. Shakib Ahmed et al., (2024), "Prospects and challenges of energy storage materials: A comprehensive review", Chemical Engineering Journal Advances, vol 20, https://doi.org/10.1016/j.ceja.2024.100657, 100657.

[2] F. Agboldoko, G. ChekwubeEzeamii and O. Joseph Ojochogwu, (2024), "Green chemistry in manufacturing: Innovations in reducing environmental impact", World Journal of Advanced Research and Reviews: an International, vol 23, DOI: https://doi.org/10.30574/wjarr.2024.23.3.2938, no 03, pp. 2826–2841.

[3] Chengwei Wang et al., "A general method to synthesize and sinter bulk ceramics in seconds", Science,vol 368, DOI:10.1126/science.aaz7681, pp. 521-526.

[4] C. Benhalima, S. Amari, I. Beldi& B. Bouhafs, (2019), "First-Principles Study of Ferromagnetism in Iron Chromite Spinels: FeCr2O4 and CrFe2O4", SPIN, vol 9, doi:10.1142/s2010324719500140,no. 3, 1950014.

[5] S. S Hossain, & P. K. Roy, (2020),"Sustainable ceramics derived from solid wastes: a review", Journal of Asian Ceramic Societies, vol 8, https://doi.org/10.1080/21870764.2020.1815348, (4), 984–1009.

[6] Mubasher, M. Mumtaz, Najeeb Ur Rehman Lashari, Mehwish Hassan, SongponTangsee, M. Tahir Khan,(2021), "Multi-walled carbon nanotubes and chromium ferrites nanoparticles nanohybrids as anode materials for lithium-ion batteries", Journal of Alloys and Compounds, vol 872, https://doi.org/10.1016/j.jallcom.2021.159654, 159654.

[7] S. A. Gad, et al. (2020), "Impact of chromium doping on structural, optical, magnetic and electrical properties of nano-copper ferrite", Journal of Ovonic Research, vol 6, no 5, pp. 293-308.

[8] F.Georget, W. Wilson&K. L. Scrivener, (2021), "edxia: Microstructure characterisation from quantified SEM-EDS hypermaps", Cement and Concrete Research, vol 141, https://doi.org/10.1016/j.cemconres.2020.106327, March 2021, 106327.

[9] N. Kaur, & S. Tiwari, (2018),"Role of particle size distribution and magnetic anisotropy on magnetization of antiferromagnetic nanoparticles", Journal of Physics and Chemistry of Solids, vol 123, https://doi.org/10.1016/j.jpcs.2018.08.013, 279-283.

[10] A. Yogi, & D. Varshney, (2013),"Magnetic and structural properties of pure and Cr-doped haematite: α-Fe2−xCr x O3 (0 ≤ x ≤ 1)", Journal of Advanced Ceramics, vol 2, https://doi.org/10.1007/s40145-013-0084-7,no 4, pp. 360-369.

[11] T Amelia et al., (2020) "Synthesis and structural characterization of ironchromite nanoparticles: A preliminary study", Journal of Physics: Conference Series, doi:10.1088/1742-6596/1595/1/012027, 1595, 012027.

[12] A. V Bagade, P. A Nagwade, A. V Nagawade, S. R Thopate, S. N. Pund, (2022),"A Review on Synthesis, Characterization and Applications of Cadmium Ferrite and its Doped Variants", Oriental Journal of Chemistry, vol 38, DOI : http://dx.doi.org/10.13005/ojc/380101, no 1.

[13] Hashim, et al., (2014). “Study of structural, electrical and magnetic properties of Cr doped Ni–Mg ferrite nanoparticle”. Journal of Alloys and Compounds, vol 602, doi:10.1016/j.jallcom.2014.03.013, pp. 150–156.
[14] Prashanth Kumar, P. G., Shoukat Ali, R. ., Jagadisha, A. S., & Umesh, S. D. (2020). “Synthesis and studies of Cr doped Zn ferrites “. Materials Today: Proceedings. doi:10.1016/j.matpr.2020.07.014.
[15] S. Abhishnek et al., (2022), “Electronic and magnetic properties of FeCr2O4 nanoparticles by advanced synchrotron based soft X-ray magnetic circular dichroism”, Physica B: Condensed Matter, vol 647, https://doi.org/10.1016/j.physb.2022.414373, 414373.

Pedro,Vera-Serna: https://orcid.org/0000-0001-7085-7374
Luis A.,Garcia-Camacho: https://orcid.org/0009-0001-5403-0788

METHODS OF IMPLEMENTING DIGITAL MARKETING TOOLS IN THE INTERNATIONAL COMPANIESACTIVITIES

Roman BASISTYI [1], Liudmyla SHULHINA [2]

Master's Student, of the National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute"[1]

National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute"[2]

Abstract. Introduction. The article examines the methods of implementing digital tools in international markets, focusing on cultural, legal, and economic aspects that determine their adaptation. An analysis of key tools and models that can enhance the effectiveness of digital strategies for the U.S. and European markets is conducted.

Objective. The primary aim of the article is to study the specifics of digital marketing strategies in international markets and to identify key tools and metrics that contribute to their effective adaptation.

Materials and Methods. This research utilized analytical data on key digital marketing tools, such as SEO, SEM, content marketing, social media, and PPC advertising. The main research methods included comparative analysis.

Results. The study analyzed findings that demonstrated the success of using digital marketing tools in international markets depends on adapting to cultural and regional specifics. It also revealed that, to enhance effectiveness, specific tools should be used for each market.

Prospects. Further research is expected to analyze the effectiveness of digital tools for specific industries and adapt them to the conditions of particular regions.

Keywords: digital tools, international market, SEO, SMM, content marketing.

PROBLEM STATEMENT

In the context of globalization, adapting marketing strategies to the specifics of international markets becomes critical for business. Digital marketing tools require in-depth analysis to take into account the specifics of each market.

ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Modern research emphasizes the importance of adapting digital strategies to the cultural, economic and legal conditions of international markets. In particular, the works of Levchenko M. and Omelchak O. demonstrate the effectiveness of integrating online and offline channels, as well as targeted advertising to reach local audiences.The research ofYogesh K. Dwivedi, Nripendra P. Rana, Emma L. Slade, Nitish Singh, Hatice Kizginfocused on the role of social networks and content strategies, emphasizing the importance of personalization and localization of content for increasing brand recognition at the global level.

PURPOSE

The purpose of this article is to analyse the features of digital marketing strategies in international markets with an emphasis on tools that contribute to effective penetration of new markets, adaptation to regional characteristics, and increased competitiveness.The study examined key digital marketing tools such as SEO, SMM, content marketing, PPC advertising and their impact on business results in a global competitive environment. This article also aims to identify methodological aspects of adapting digital strategies to the cultural, economic and legal conditions of different markets.

PRESENTATION OF THE MAIN MATERIAL

Developing an effective digital strategy for entering new markets is a key factor in a company's success in the face of global competition and digital transformation. One of the main approaches to forming such a strategy is the use of comprehensive market analysis, which includes not only studying competitors, but also adapting the product or service to local needs and market characteristics.

Approaches to applying various digital marketing tools in international markets are systematized in Table 1, including SEO, content marketing, social media, and content localization. Each strategy has its own characteristics depending on the region, taking into account cultural, linguistic, economic, and legal aspects.

SEO and content marketing are the basic elements of a digital strategy for entering new markets. SEO allows you to improve your company's visibility in search engines, which is an important tool for attracting potential customers in new geographical regions. This increases the relevance of the website to users and ensures more organic traffic (Levchenko, Omelchak, 2022).

Another critical element is content localization. To successfully enter a new market, it is important to adapt marketing materials to the local culture, language, and consumer habits. This applies not only to translation, but also to adapting visual and textual elements to the specifics of the region (Yogesh, Emma, 2020).

Table 1. Features of digital instruments in international markets.

Digital tools	Application in international markets	Factors affecting efficiency
SEO (Search engine optimization)	Highly competitive in search engines; targeting local keywords	The level of competition in search engines; the specifics of local search queries
Content marketing	Adapting content to regional needs and language; focusing on value for local consumers	Language barriers, cultural differences; level of trust in the content source
SMM (Social media marketing)	Using regional platforms; local influencers to improve awareness	Social media popularity, regional preferences; influence of local trends
Localization of content	Translation and adaptation of content taking into account local cultural characteristics; adaptation of advertising campaigns	Cultural and linguistic features, requirements for local content; legal aspects

Source: systematized by the authors based on [1-5].

Targeted advertising and PPC (Pay-Per-Click) campaigns help to quickly attract new customers in different geographical regions. Using platforms such as Google Ads or Facebook Ads allows you to precisely customize advertising for specific audience segments based on demographic, behavioral and geographic characteristics.This is especially important when entering new markets, where consumer behavior may differ significantly from familiar conditions (Shafique, Samiran, 2024).

Adapting social media to local markets also plays a crucial role in building a strong brand presence. For example, platforms that are popular in one region may be less common in another.Therefore, it is important to understand the specifics of social media usage in different countries and adapt the content and approach to managing company pages according to local preferences (Omelchak, 2023). Platforms such as LinkedIn, WeChat may have different popularity depending on the region.

Content strategies are also crucial to ensuring successful entry into new markets. Publishing relevant content that is culturally relevant to the new audience helps build an emotional connection with customers and increase brand awareness. This can include creating videos, blogs, infographics, or other forms of content that are locally tailored (Koval, 2023).

When developing a digital strategy for entering new markets, it is important to consider the impact of macro factors such as cultural, legal, logistical, technological, economic, political, social, demographic and environmental aspects. Each of these factors significantly affects the effectiveness of applying individual digital strategy tools (Table 2).

Cultural factors have a major impact on consumer behavior and response to marketing campaigns. It is important to consider differences in the perception of visual images, linguistic expressions and symbols, which can have different meanings in different cultures. For example, the incorrect use of cultural elements can lead to negative brand perceptions or even cause resentment among consumers(Cassia, Magno, 2022).

Table 2. The influence of macro factors on the use of digital marketing tools.

Macro factors	SEO (Search engine optimization)	Content marketing	SMM (Social media marketing)	Contentlocalization
Cultural factors	Adaptation of keywords according to cultural feachers	Creating content that takes into account local traditions and preferences	Using platforms popular in the region	Translation and cultural adaptation of content
Legal aspects	Compliance with local SEO advertising requirements	Compliance with legislation according to content	Compliance of advertising content with local laws	Respecting copyright when translating
Logistical factors	Optimization for local delivery searches	Content about logistics capabilities	Communication with customers regarding delivery	Information about local delivery conditions
Technologi cal factors	Taking into account the popularity of search engines in the region	Using adapted content for creation technologies	Content adaptation for mobile platforms	Testing content display on different devices
Economic factors	Selecting keywords that match the audience's income level	Content focused on the audience's economic capabilities	Choosing platforms based on accessibility for the public	Adding localized price offers
Political factors	Avoiding keywords related to sensitive topics	Avoiding politically sensitive topics	Choosing safe advertising platforms	Taking into account the political situation in the region
Social factors	Using keywords that reflect social trends	Content aboutsocial preferences	Publishing content that matches trends	Taking into account social priorities
Demograp hic factors	Targeting age groups through search queries	Creating content for different age groups	Targeting based on demographic data	Personalized content for different groups
Environme ntal factor	Optimization of ecologically related queries	Creating content about the company's sustainable practices	Communication on environmental initiatives	Integrating environmental topics into content

Systematized by the authors based on [6-9].

Therefore, companies entering new markets should conduct thorough research into the local culture and adapt their advertising campaigns to its specificities.Legal aspects are also important for developing a digital strategy. Each country has its own legislation that regulates e-commerce, personal data protection, the use of advertising materials and other aspects of digital marketing. For example, advertising content requirements can vary significantly by country, so it is important for companies to ensure their campaigns comply with local laws to avoid legal issues and fines (Dewi, 2023).

Logistical factors determine a company's ability to deliver products and services to new markets on time. This includes the availability and quality of transport infrastructure, customs restrictions, transportation costs and warehousing services. Logistical difficulties, particularly when entering international markets, can be a serious challenge for companies that, Therefore, it is important to anticipate and minimize potential risks in advance (Lytvynenko, 2024).

In addition to cultural, legal, and logistical factors, technological and economic aspects also play an important role in developing a digital strategy for entering new markets. Technological factors directly affect a company's ability to interact with new consumers through digital channels.For example, the level of development of internet infrastructure and access to mobile devices can significantly change the way you communicate with customers. In countries with high mobile internet penetration, it is worth focusing on mobile advertising and adapting websites for mobile devices.You also need to consider local restrictions on the use of certain technologies or platforms, which may be prohibited in some regions (Liu, Chen, 2022).

Economic factors are important when planning a digital strategy. Population income levels, purchasing power, and macroeconomic conditions can significantly affect the perception of a product or service.Companies need to adapt their marketing messages, pricing policies, and sales channels to the real economic opportunities of consumers in the new market. For example, in low-income markets, it is important to consider product affordability by providing customers with different payment options or special offers.

You should also pay attention to political factors that can affect your digital strategy. Political stability, government policies on regulating the digital economy, and international relations can determine a company's ability to enter a new market. For example, trade barriers, sanctions, or changes in tax laws can affect a company's operations in certain regions(Usman, 2024).

From the above, it follows that to create a successful digital strategy for entering new markets, it is necessary to consider not only cultural, legal and logistical factors, but also technological, economic and political aspects. A comprehensive approach to analyzing these factors will help companies plan their actions more effectively and avoid risks that may arise in the process of adapting to new market conditions.

In addition to the factors mentioned, it is worth paying attention to social and demographic aspects, which also have a significant impact on the development of a digital strategy for entering new markets.

Social factors, such as the level of education, social preferences and values, play a key role in shaping consumer habits.For example, in countries with a high level of education, consumers are more likely to make informed choices, preferring products that meet their environmental or ethical standards. To successfully adapt a digital strategy, it is necessary to take these aspects into account and create appropriate content and messages that meet the social expectations of the audience (Rane, 2024).

Demographic factors such as age, gender, income level and household structure also influence marketing strategies. For example, digital channels such as social media or mobile apps may be more effective for younger audiences, while for older age groups, it is advisable to use other approaches, including email or content focused on convenience and ease of use. The strategy should be adapted to the demographic characteristics of the market, in particular, through audience segmentation and targeting based on demographic data.

Environmental considerations are also important and are becoming increasingly important in today's digital strategies. Consumers are increasingly paying attention to the environmental impact of companies and prefer brands that support environmental initiatives or use sustainable production

practices.Taking into account environmental aspects in digital strategies can increase consumer loyalty and strengthen the brand's position in new markets [9].

CONCLUSIONS AND PROSPECTS OF THE STUD

The study of the features of digital marketing strategies in international markets revealed the importance of adapting strategies to regional cultural, economicand other macro factors of the marketing environment. The use of tools such as SEO, content marketing, PPC advertising and social networks contributes to achieving business goals, improving customer interaction and increasing communication efficiency.

Prospects for further research include the development of innovative methods for assessing the effectiveness of digital strategies,analysis of consumer behavior in different cultural segments, as well as studying the latest tools for marketing process automation. This will allow enterprises to more accurately adapt their strategies to dynamic market conditions, while maintaining flexibility and efficiency in decision-making.

REFERENCES

[1] Levchenko, M. (2022). Doslidzhennia efektyvnosti intehratsii onlain ta oflain marketynhu cherez model ROPO. Ekonomika ta upravlinnia pidpryiemstvamy, (4), pp. 56-62.

[2] Yogesh, K., Nripendra, P., Emma, L., Nitish, S., Hatice, K. (2020). Editorial introduction: Advances in theory and practice of digital marketing,Journal of Retailing and Consumer Services,Volume 53,ISSN 0969-6989,https://doi.org/10.1016/j.jretconser.2019.101909.https://www.sciencedirect.com/science/article/pii/S0969698919309737.

[3] Shafique A., Samiran S. (2024). Navigating the modern marketing landscape:Strategies and Innovations in contemporarymarketing management, International Journal of Multidisciplinary Trends, 6(2), 06-10, DOI: https://dx.doi.org/10.22271/multi.2024.v6.i3a.386.

[4] Omelchak, O.(2023). Vykorystannia instrumentiv targetovanoi reklamy u mizhnarodnomu marketynhu. Marketynh ta tsyfrovi tekhnolohii, pp. 54-59.

[5] Koval, Ya. (2023). Kontent-stratehii v umovakh hlobalizatsii: suchasni tendentsii, Ekonomika i marketynh, pp. 99-105.

[6] Cassia,F., Magno,F. (2022). Cross-border e-commerce as a foreign market entry mode among SMEs: the relationship between export capabilities and performance, Review of International Business and Strategy, ISSN: 2059-6014, Vol. 32 No. 2, pp. 267-283. https://doi.org/10.1108/RIBS-02-2021-0027.

[7] Dewi, I. (2023).Personalization in Marketing: Effectiveness and Challenges, Journal Arbitration:Economy,Management and AccountingVolume 1, Number 02, (No 75-83), E.SSN 2987-0305 (Online),DOI: https://paspama.org/index.php/Arbitrase/article/view/58/62.

[8] Lytvynenko, P. (2024). Digital Marketing Analytics: Trends and Development Prospects, Journal of Economic Research, pp. 67-74.

[9] Liu, Y., Chen, Z. (2022). A new model to evaluate the success of electronic customer relationship management systems in industrial marketing: the mediating role of customer feedback management. Total Quality Management & Business Excellence, 34(5–6), 515–537. https://doi.org/10.1080/14783363.2022.2071694.

[10] Usman, F., Eyo-Udo, N., Etukudoh, E. (2024). A critical Review of AI-Driven Strategies for Entriepreneurial Success, International Journal of Management & Entrepreneurship Research, Volume 6, Issue 1,No. 200-215, DOI: 10.51594/ijmer.v6i.748.

[11] Rane, N., Paramesha, M., Choudhary, S., Rane, J. (2024). Artificial Intelligence, Machine Learning, and Deep Learning for Advanced Business Strategies: A Review. Partners Universal International Innovation Journal, 2(3), 147–171. https://doi.org/10.5281/zenodo.12208298.

MULTIMODAL AI MODELS FOR HUMAN-MACHINE INTERACTION IN FINANCIAL, INDUSTRIAL AND EDUCATION ENVIRONMENTS

Mgr. René KLAUČO, PhD.[1]
Prof. Ing. Ladislav VÁRKOLY, PhD.[2]

Founder, KLAUCODE – High-Performance digital platforms for modern business (https://klauco.de), Poprad, Slovakia[1]

Professional guarantor, INTERNET SCHOOL – Educational social network and digital library (https://internetovaskola.sk), Poprad, Slovakia[2]

ABSTRACT: The paper focuses on the field of artificial intelligence as a tool for transformation with a strong impact on industry, economy and society. The pace of innovation in AI is unprecedented, with new models and techniques emerging in extremely short time iterations. This dynamic creates a need to systematically track and evaluate different research directions within AI in order to subsequently identify areas with the highest current impact and, most importantly, future potential. This is essential in the education and training of future professionals for these fields. In this context, the paper focuses on the AI categories with the highest "popularity" at present, at the same time as the largest projected growth trend over the coming period. Geographically, it focuses on the regions of the US, EU and China, which are "drivers" of innovation and pre-represent global ecosystems for R&D and investment in this field, but also competitors. The available information suggests the dominance of several high momentum areas, notably Generative AI (especially LLM), AI for Science, Responsible/Safety AI or Reinforcement Learning. At the same time, from a regional perspective, the US confirms its dominance in AI investment and development of the most advanced models, while China dominates in the volume of publications and patents and is rapidly catching up in terms of quality. Europe has a strong talent base, underlining the growing importance of interdisciplinary research, the need for robust infrastructure (computing power, data) and the necessity to address ethical and security challenges associated with AI advancement, but the necessary investments to develop and scale innovation are still in process.

Key words: artificial intelligence, AI, LLM, Generative AI, AI for Science, Reinforcement Learning

INTRODUCTION

Artificial intelligence is going through a period of dynamic development. One of the most significant trends is the shift from unimodal systems processing one type of data to multimodal models. They allow parallel processing, interpretation and integration of information from multiple data modalities such as text, image, sound, video, biometric data or even more complex sensory data (e.g., depth, body position, physiological signals) [1]. This shift represents a fundamental change in the capabilities of AI, bringing it closer to the human way of perceiving and processing information from the outside world, while at the same time opening up new application possibilities [2].

In the context of this technological revolution, Human-Machine Interaction (HMI) becomes critical. Efficient, intuitive and secure HMI is a key enabler for the successful adoption and exploitation of the potential of AI systems, especially in complex and highly demanding domains such as finance, industry and education [3]. These domains present opportunities for AI capabilities to work with multiple types of information and bring about revolutionary changes. Unlike traditional graphical interfaces or voice assistants, multimodal systems seek to interpret the combined meaning derived from simultaneous inputs - for example, the tone of a voice along with facial expressions and the content of a text message. This synergy, where the whole is more than the sum of its parts, can lead to a higher level of efficiency and naturalness in solving complex tasks [1].

The integration of multimodal AI for HMI in the finance sector has gained great importance in the

analysis of complex data. Multimodal systems can contribute to better fraud detection and more personalized advice [5]. In industry, production efficiency, worker safety, and automation flexibility are key. Multimodal AI can optimize quality control, predictive maintenance, and enable safe human-robot collaboration [7].

In education, the goal is to increase student engagement, personalize the learning process, and provide a deeper understanding of learning strategies, which can be supported by multimodal analytics tools and adaptive systems [8].

1. MULTIMODAL AI

Multimodal AI is defined as a field of machine learning focused on the development of models capable of processing, integrating, interpreting and generating information from multiple types (modalities) of data simultaneously. These modalities typically include text, still images, video, audio (speech, music, environmental sounds), but can also be augmented with other sensory inputs such as data from depth sensors, information about body position and orientation, physiological signals (e.g., EEG, ECG), or data from various industrial sensors. A multimodal AI model can leverage the information contained in different modalities and formats to achieve a more comprehensive understanding of the problem and generate more robust and accurate outputs [1]. For example, a multimodal system can analyze a video recording by simultaneously processing the content of the conversation (text/speech), the tone of voice (audio), and facial expressions (image) to gain a much more comprehensive view than would be obtained from analysing a single modality [2].

1.1. BASIC PRINCIPLES OF OPERATION

The functioning of multimodal AI models involves several key steps, from the processing of individual data streams to their integration and final decision-making or output generation. The first step is the extraction of relevant information from the input modalities, where specialized neural network architectures optimized for the data type are used. For example, Convolutional Neural Networks (CNNs) are standardly used for image data processing [4]. For sequential data such as text or speech, recurrent neural networks (RNNs) were initially used and later their more advanced variants (LSTM, GRU). Nowadays, Transformer-based architectures (Transformers) dominate, which can model long-distance dependencies in sequences more efficiently [1].

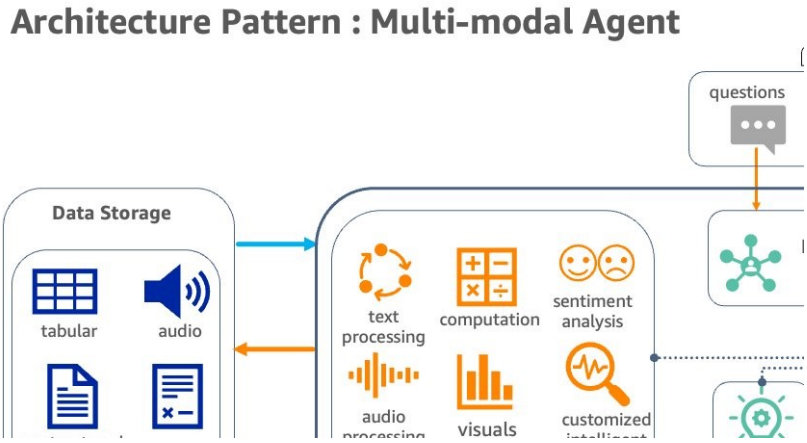


Fig. 1. Multi modal agent architecture pattern [23].

The next step is data fusion, i.e., the integration of the information from the previous step into a common representation or a common decision process. There are several basic data fusion strategies, which differ in which stage of processing the information fusion occurs [1]:

- Early Fusion: data from the modalities are merged at the beginning (before entering the main model).

- Late Fusion: the opposite of early fusion, each modality is processed separately at first and only combined in the final stage.
- Intermediate Fusion: a compromise between early and late mergers to combine their advantages.
- Hybrid approaches: more complex models that combine different levels of fusion or use more sophisticated mechanisms to dynamically weight the importance of individual modalities [4].

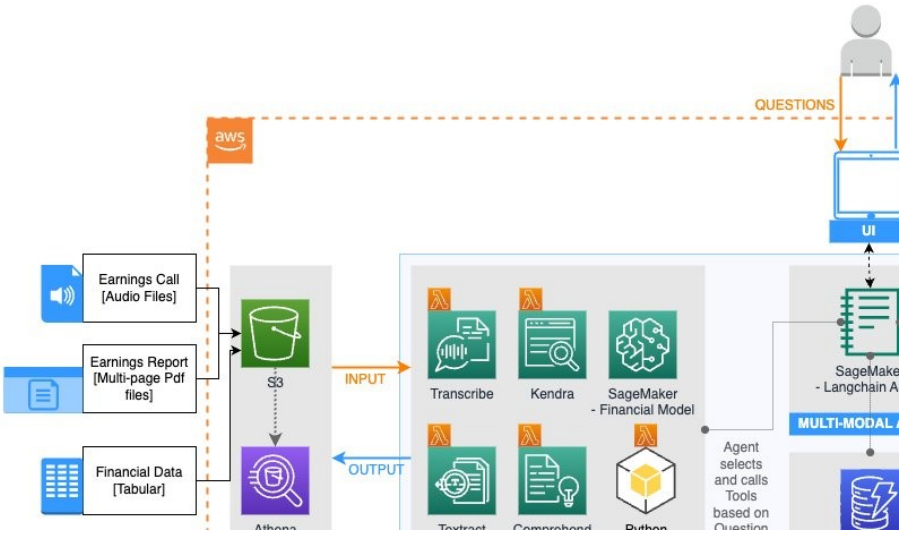


Fig. 2. Example of AWS technical architecture of multi modal agent [23].

The Transformer architecture, originally designed for natural language processing (NLP), has proven to be extremely flexible and powerful for multimodal tasks. Its key component, the "self-attenuation" mechanism, allows the model to dynamically consider the importance of different parts of the input data, even across different modalities [1]. This feature is the basis of many modern multimodal large language models (MLLMs) [14].

The Vision Transformer (ViT) model applies Transformer architectures to computer vision tasks, where they achieve state-of-the-art results in image classification and other CV tasks, while scaling better and working more efficiently as data size increases [13].

The CLIP (Contrastive Language-Image Pre-training) model developed by OpenAI can very efficiently analyze the similarity between arbitrary text and an image, enabling, e.g., "zero-shot" image classification (classifying images into categories not seen by the model during training, based only on their textual description) and semantic retrieval of images according to textual queries and vice versa [11].

1.2. ADVANTAGES AND BENEFITS

The ability to process and integrate information from multiple sources brings a number of benefits to multimodal AI:

- **More comprehensive understanding and higher accuracy:** by combining information from different modalities, multimodal systems enable a deeper understanding of the data or situations being analyzed. Different modalities often provide complementary information or help resolve ambiguities present in other modalities. This leads to more accurate predictions and decisions in tasks such as image recognition, language translation, sentiment analysis, or speech recognition [1].
- **Robustness and robustness to "noise", inconsistency or missing data:** The real world is often imperfect - sensors can fail, data can be "noisy" or incomplete. Multimodal systems are inherently more resilient to these problems. If information from one modality is missing or unreliable, the system can still rely on data from other available modalities to maintain a certain level of performance (an important property for deployment in mission-critical applications) [1].
- **More natural and intuitive HMI:** Human communication and perception is multimodal (speech,

gestures, facial expressions, gaze). Multimodal AI enables the creation of more natural interfaces where users can interact with the system using a combination of voice, touch, gestures, or visual cues, leading to a more intuitive and satisfying user experience [1].

- **Broader range of applications:** the ability to work with different types of data opens up opportunities for new and more advanced applications of AI in a variety of applications that were previously difficult to address. Examples include advanced virtual assistants, healthcare diagnostics combining image and text data (methods for detection and resulting disease prevention), autonomous vehicles integrating visual, radar and lidar data, advanced weather prediction models or multimedia content analysis [14].
- **Robustness and robustness to "noise", inconsistency or missing data:** The real world is often imperfect - sensors can fail, data can be "noisy" or incomplete. Multimodal systems are inherently more resilient to these problems. If information from one modality is missing or unreliable, the system can still rely on data from other available modalities to maintain a certain level of performance (an important property for deployment in mission-critical applications) [1].
- **More natural and intuitive HMI:** Human communication and perception is multimodal (speech, gestures, facial expressions, gaze). Multimodal AI enables the creation of more natural interfaces where users can interact with the system using a combination of voice, touch, gestures, or visual cues, leading to a more intuitive and satisfying user experience [1].
- **Broader range of applications:** the ability to work with different types of data opens up opportunities for new and more advanced applications of AI in a variety of applications that were previously difficult to address. Examples include advanced virtual assistants, healthcare diagnostics combining image and text data (methods for detection and resulting disease prevention), autonomous vehicles integrating visual, radar and lidar data, advanced weather forecasting models or multimedia content analysis [14].

1.3. CHALLENGES AND LIMITATIONS

Despite its enormous potential, the development and deployment of multimodal AI also faces significant challenges and issues that need to be addressed for quality improvement and error elimination [1]:

- **Representation:** Finding appropriate mathematical representations for heterogeneous data from different modalities in a way that reliably captures their specific properties and interrelationships [1].
- **Alignment:** Identifying and matching corresponding features across different modalities, e.g., how to pair a particular word in a description with the corresponding area in an image, or how to synchronize speech with lip movements in a video, etc. This requires specific techniques for temporal and spatial matching. Incorrect matching can lead to misinterpretations no matter how well the modalities are handled. Efficient alignment strategies are essential for reliable inference and generation in multimodal AI [1].
- **Reasoning:** combining information and knowledge obtained from different modalities to perform complex reasoning tasks that often require multiple inference steps [1].
- **Generation:** Generating new data in one or more formats (modalities) so that it is coherent, realistic, and error-free [1].
- **Transference:** Efficient transfer of learned knowledge from one modality to another modality (e.g., from text to visual) or to a multimodal task [1].
- **Quantification:** Methods for measuring and evaluating the performance of multimodal models, understanding their inner workings and reliability. This requires the development of new metrics and new evaluation methods [1].
- **Missing Modalities:** In real-world applications, data is often incomplete - a sensor may fail, a user may choose not to provide a certain type of input (e.g., turn off a camera), or some modalities are unavailable due to other reasons such as privacy or technical limitations [7].

Standard multimodal models trained on complete data may fail or significantly reduce their reliability in the absence of inputs. This problem highlights the critical difference between theoretical models and practical applicability. Robustness against missing modalities is a necessity for reliable deployment in complex environments where incomplete data streams are the rule rather than the exception [13].

- **Complexity, computational complexity and data availability:** Multimodal models are often significantly larger and computationally more demanding to train and infer compared to unimodal ones. Increasing efficiency leads to increasing performance or decreasing computational complexity and, in this context, to savings [1]. Training high-quality multimodal models requires access to large, high-quality, and consistent datasets [13].
- **Ethics and Bias:** Models integrating data from multiple sources are more sensitive to the risk of inheriting, combining, or amplifying social biases present in these data. For example, biases in face recognition may combine with biases in language models, leading to discriminative effects [12].

2. HUMAN-MACHINE INTERACTION

Human-machine interaction (HMI), sometimes referred to as human-computer interaction (HCI), focuses on the design, evaluation, and implementation of interactive computing systems for human use [3]. The goal of HCI is to create systems that are not only functional, but also usable, efficient, safe, and satisfying to the user [14]. Usability is a measure of how easily and efficiently a user (human) can interact with a given system and achieve expected goals. It is primarily concerned with simplicity, quality of user interface, speed, reliability of the system, accuracy of results and low error rate. Other important elements include reducing cognitive load (intuitive operation), quality UI/UX, accessibility, etc. which are important elements for all digital products and online platforms. The goal is to ensure that systems can be used by people with different physical, sensory or cognitive abilities. This includes, for example, support for screen readers, high contrast, alternatives to audio notifications, keyboard or voice control [3]. Inclusive design goes even further and seeks to create solutions that are suitable for the widest possible range of users with different needs, preferences and in different contexts of use.

In this context, setting up metrics, tracking events and evaluating user behaviour and interactions is important, and this is now a detailed area used in digital e-commerce products in particular. There are several sets of design principles and heuristics, e.g., Shneiderman's "Eight Golden Rules" where he highlights [15]:

- consistency (terminology, appearance, behaviour),
- making "shortcuts" available to frequent users,
- providing informative feedback,
- designing dialogues to lead to successful completion of tasks,
- offering simple error prevention and handling,
- enabling easy undoing of actions (undo),
- fostering an internal sense of control (users control events, the system responds),
- reducing the burden on short-term memory (using elements that are easily recognizable, simple and lightweight interface).

2.1. ROLES AND CHALLENGES OF MULTIMODALITY IN IMPROVING HMI

Multimodal AI brings new opportunities, but also challenges, to fulfil and extend traditional HMI principles:

- More natural interaction: the most striking promise is to bring human-machine interaction closer to natural human communication. A system's ability to understand and respond to a combination of modalities such as speech, gestures, gaze, and contextual information (e.g., camera images) enables more fluid and intuitive dialogues [1].
- Increased efficiency and flexibility: providing multiple input and output modalities gives the user

the ability to choose the most appropriate one for a given task, context or personal preference, e.g., entering a command can be faster by combining voice and pointing on the screen [4].

- Reducing cognitive load: distributing information and interaction across multiple sensory channels can potentially reduce the load on one particular channel, especially the visual channel, which is often overloaded in traditional AI [3]. For example, an important alert can be conveyed by sound or haptic response, freeing up visual capacity for the main task.
- Personalization: multimodal systems can collect richer information about the user and their state - not only what they are saying or doing, but also how they are feeling (voice analysis, facial expression) or what they are focusing on (gaze tracking) [2].
- Improved accessibility: offering alternative modalities of interaction is of direct benefit to users with different disabilities or limitations. A user who cannot use a keyboard can use voice control; a user with a hearing impairment can receive visual notifications instead of audible ones [3].
- Contextual Awareness: Although multimodal systems have access to richer data, truly understanding complex human and situational context remains a challenge [18]. The system needs to know not only what the user is doing, but also why, where, with whom, and what mental and emotional state they are in, in order to interact appropriately and effectively [19].
- Intervention Timing & Interruptibility: Predicting and responding at the right moment for the system to reach the user, provide information, suggest or perform an action. Inappropriate interruptions can be extremely disruptive, reducing productivity and even increasing stress [18].
- User Engagement: Maintaining long-term user interest and willingness to interact with multimodal systems can be challenging, especially if the systems require too much active input, are perceived as too complex or invasive (e.g., constant monitoring). The key is to find the right balance between passive data collection (which is less burdensome) and the required active input from the user [18].
- Trust & Explainability: since multimodal systems often deal with sensitive data (biometrics, emotions) and make complex decisions, it is essential that users trust these systems. Trust requires transparency and the ability of the system to explain its decisions or recommendations [16].
- Fusion and interpretation of ambiguity: How should the system interpret a situation where signals from different modalities conflict (e.g., the user says "yes" but shakes her head)? Proper fusion and interpretation of such ambiguous or conflicting inputs is a non-trivial problem.

3. MULTIMODAL AI APPLICATIONS

3.1. MULTIMODAL AI IN THE FINANCIAL SECTOR

The financial sector, characterized by high demands for security, accuracy, trust and efficiency in processing complex data, presents an opportunity for multimodal AI applications. The integration of different data modalities can significantly improve HMI in areas such as fraud detection, customer service, risk management and market analysis.

Traditional methods of fraud detection based on rules or analysis of transaction data alone are hitting their limits. Multimodal AI offers a more robust approach by integrating behavioural biometrics with transactional data. Behavioural biometrics analyzes unique patterns of user behaviour as they interact with the system - e.g., keystroke dynamics (typing speed, key hold time, rhythm), mouse movement characteristics (speed, trajectory, click frequency), or touchscreen gestures. These behavioural patterns are unique to each user and difficult to mimic [6]. A multimodal system combines this behavioural data with traditional transactional data (purchase history, transaction amount, geolocation, device usage information). Using advanced AI techniques, especially deep learning e.g. RNN (recurrent neural networks for transaction sequence analysis), CNN (convolutional neural networks for pattern extraction from behavioural data) and autoencoders (for anomaly detection). Using this data, the system builds a comprehensive profile of a user's "standard" behaviour. Any significant deviations from this profile in real time are then flagged as suspicious.

Tab. 1. Examples of multimodal AI applications in the financial sector.

Area	Multimodal Capabilities	Benefits for HMI
Fraud Detection	Fusion of behavioural biometrics (keyboard, mouse) and transactional data; Microexpression (CV) analysis.	Increased security; Smoother interaction (implicit authentication); Reduction of false alarms.
KYC / Onboarding / Authentication	Fusion of behavioral biometrics (keyboard, mouse) and transactional data; Microexpression (CV) analysis.	Enhanced security; Smoother interaction (implicit authentication); Reduced false positives.
Customer Service / Financial Advice	Natural language processing (text, voice); Sentiment analysis (voice, face, text); Document analysis.	More natural and empathetic communication; Personalised advice; More efficient handling of queries.
Market analysis / Risk management	Sentiment analysis (text, audio, video); Integration of structured data with unstructured data (reports, graphs)	More comprehensive understanding of the market and risks; Decision support.

Another example of the application of multimodal AI is the customer identity verification (KYC) process, which is mandatory for financial institutions. Financial institutions are gradually implementing biometric-based verification, e.g. facial recognition, to verify identity when opening new accounts or authorising transactions. These systems dramatically speed up the onboarding process, reduce the need for manual verification and branch visits, reduce error rates, and increase security [5]. The use of biometrics (face, voice, and blood vessel structure recognition) as a primary or secondary authentication method greatly enhances user convenience.

In addition to fraud detection and KYC, multimodal AI is also used for other forms of risk management e.g. multimodal customer sentiment analysis - combining analysis of text stimuli (reviews, emails), tone of voice in phone calls and facial expressions in video calls can provide a more comprehensive picture of customer satisfaction, needs and potential risks [2].

Chatbots and virtual assistants are becoming a common part of customer service. Multimodal capabilities are taking them to a new level, and future trends in this area include the development of emotionally intelligent AI (able to recognize and respond appropriately to the user's emotions) [17].

Understanding financial market sentiment is crucial for investment decision making. Multimodal AI allows sentiment analysis not only from textual sources (financial news, articles, social media posts, blogs), but also from audio and video content, e.g., analysis of tone of voice during or facial expressions can provide additional signals that are not contained in text [3]. At the same time, multimodal models integrate and analyze structured financial data (stock prices, financial statements, predictions of economic indicators e.g. S&P500 index, etc.) together with unstructured data such as text messages, articles, images (charts, satellite images of factories or fields), video and audio recordings. The ability to find hidden patterns and correlations in this combined data can lead to more accurate market predictions and better investment strategies [14].

3.2 MULTIMODÁLNA AI V PRIEMYSLE

Industrial environments, from production lines to logistics centres and energy facilities, are characterised by complex processes, the need for high efficiency, stringent safety requirements and human interaction with increasingly sophisticated machines and robots. Here, multimodal AI offers particularly significant potential for optimizing operations, enhancing safety and improving HMI in challenging environments.

Tab. 2. Examples of multimodal AI applications in industry

Area	Multimodal Capabilities	Benefits for HMI
Quality Control	Multimodal Capabilities Benefits for HMI Quality Control Computer vision (image, video); Sensory data (sound, vibration).	Higher inspection accuracy and speed; Reduced human error; Early defect detection.
Predictive maintenance (PdM)	Fusion of sensor data (vibration, temperature, acoustics, pressure); Time series analysis.	Optimization of maintenance; Reduction of downtime; Extension of machine life; HMI focused on interpretation of predictions.
Collaborative robots (Cobots)	3D vision, LiDAR, Depth sensors, Tactile sensors; Gesture/speech recognition.	Safe human-robot collaboration; Flexible automation; Intuitive programming/control (learning by demonstration).
Safety monitoring	Computer vision; Wearable sensors (IMU, PPG, etc.); Sensor fusion.	Early detection of hazardous situations/accidents; Health and fatigue monitoring; Workplace safety enhancement.
Control Systems/Remote Assistance	Voice control, Gestures, Haptic feedback, AR/VR.	More intuitive control of complex systems; Reduced cognitive load on operators; Effective remote support.

Product quality assurance is a critical task in manufacturing. Traditional manual inspection is often slow, costly and prone to human error and fatigue. Multimodal AI and computer vision-based systems can analyze images or videos of products on the production line and detect visual defects (scratches, cracks, incorrect dimensions, missing components) with high accuracy and speed [7]. A multimodal approach can further enhance this capability by combining visual analysis with data from other sensors - for example, analysing the sound or vibration of a product during testing can reveal internal defects that are not visible [2].

Predictive maintenance, as opposed to reactive (repair after failure) or preventive (scheduled maintenance at fixed intervals), attempts to predict when a machine is likely to fail and schedule maintenance just before. Multimodal AI is key to PdM because it allows data from different sensors monitoring the machine's condition to be analyzed and integrated in real time. These sensors can measure vibration, temperature, pressure, acoustic emissions, power consumption, oil quality and other parameters. The fusion of data from multiple modalities provides a more comprehensive picture of machine health and enables more accurate fault prediction. For example, combining vibration analysis with thermal imaging can reveal bearing overheating earlier than would be evident from just one type of data. As a result, maintenance scheduling is optimized, downtime is minimized, equipment life is extended, and overall maintenance costs are reduced. Instead of reacting to failures or following fixed schedules, technicians interact with an AI system that provides specific predictions of failure types and recommends optimal intervention times. This shifts the interaction from routine or reactive tasks to supporting data-driven decision-making. This requires new skills in interpreting AI recommendations and potentially new interfaces that can effectively visualize complex sensor data and predictions [20].

The use of multimodal AI is also indispensable in the field of robotics. Traditional industrial robots work separately from humans in protective cages for safety reasons. Cobots are designed to work safely in close proximity to humans or to collaborate directly with them on common tasks. Key to their safe and efficient operation are advanced multimodal sensor systems. These systems typically combine 3D computer vision (stereo cameras, structured light), LiDAR, depth sensors, laser sensors and sometimes tactile sensors (touch and force sensors). These allow the cobot to sense its surroundings in real time, detect the presence and location of humans, anticipate their movements, and dynamically adjust its speed and trajectory to avoid collision [9].

Industrial workplaces are associated with a high risk of accidents. Multimodal AI offers new opportunities for proactive monitoring of worker safety and health. This approach combines data from different sources e.g. wearable sensors combined with computer vision. Workers can be equipped with sensors integrated into clothing, helmets or other personal protective equipment (PPE). These sensors may include inertial measurement units (IMUs containing accelerometers and gyroscopes to detect falls, sudden movements or body position), heart rate sensors, body temperature sensors, barometric pressure sensors (to detect working at height) and others. Cameras placed in the workplace can monitor worker activities, detect dangerous situations (e.g. entering a restricted area), improper use of PPE, or identify falls. By combining and fusing data from these different modalities using AI, it is possible to obtain a comprehensive picture of the workplace situation and identify risks in real time [21].

In cases where on-site expert intervention is needed but the expert is not physically present, augmented reality (AR) and virtual reality (VR) technologies combined with multimodal communication can help. A field technician equipped with AR goggles can share their view (video) and communicate (voice) with a remote expert. The expert can guide the technician by voice, display instructions or diagrams directly in the technician's field of view (AR visualization), and possibly use gestures to show specific parts of the device.

3.3 MULTIMODAL AI IN EDUCATION

Education is another area where multimodal AI promises to bring significant change. Traditional educational methods and tools often fail to fully account for students' individual needs, keep them engaged, or provide deeper insights into the effectiveness of their learning processes. Multimodal AI offers tools to personalize learning, analyze learning more deeply, and create more engaging content.

Tab. 3. Examples of multimodal AI applications in education.

Area	Multimodal Capabilities	Benefits for HMI
Multimodal Learning Analytics (MMLA)	Analysis of gaze, body language (Kinect), facial expression, voice, physiology (sensors), interaction logs.	Deeper understanding of learning processes, engagement, cognitive load; Personalized feedback.
Adaptive Learning Systems / Smart Tutors	Natural language processing (text, voice); Multimodal content generation (text, image); Response analysis.	Personalised learning journeys; Interactive and engaging teaching; More natural communication with the tutor.
Content Creation / Multimedia Learning	Generative AI (text, image, audio, video); Application of multimedia learning principles.	More effective and engaging learning materials; Improved comprehension and retention (if well designed).

Adaptive learning systems are able to adapt learning content, pace and methods to the individual characteristics of each learner [7]. Rather than relying solely on test answers or speed through materials, multimodal AI can analyze a broader range of data - for example, how a student interacts visually with content (gaze tracking), what their emotional reactions are while learning (facial expression analysis, voice analysis), or how they respond to different types of media. Based on these multimodal signals, the system can better understand the student's learning style, level of comprehension, engagement, and potential difficulties, and subsequently tailor instruction much more accurately and efficiently.

Multimodal Learning Analytics (MMLA) is an emerging field that aims to leverage data from multiple sources and modalities to gain a deep and comprehensive understanding of how learners learn, collaborate, and interact in different learning environments [8]. MMLA uses a wide range of technologies to capture different aspects of the learning process such as audio/video recordings, eye-tracking, body/gesture tracking, wearable sensors (Wearables), and telemetry data of interactions.

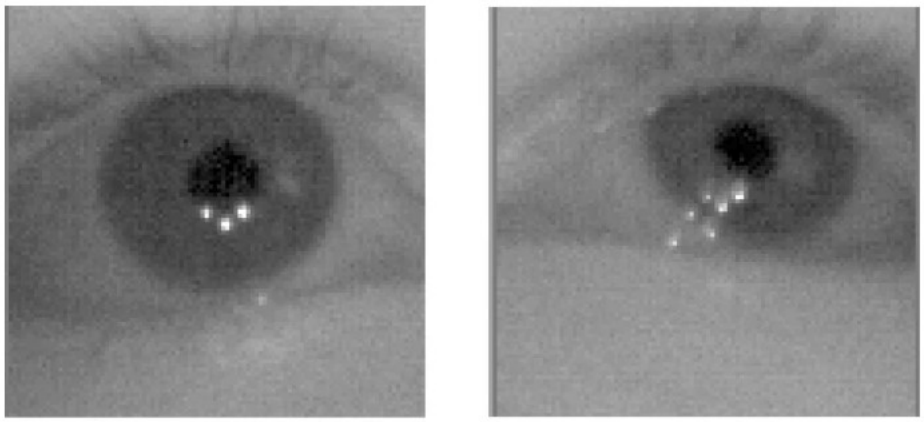


Fig. 3. Example of various methods of high-speed eye tracking [24].

The aim is to identify patterns of behaviour that correlate with parameters of learning effectiveness, such as:

- Engagement: a measure of a student's active participation and focus,
- Cognitive Load: a measure of the mental effort expended on a task,
- Emotional States: the detection of emotions such as frustration, confusion, joy, or boredom,
- Collaboration: the analysis of patterns of interaction and communication in group tasks,
- Learning Strategies and Comprehension: how students approach tasks, what strategies they use (e.g., in reading based on a gaze analysis) [22].

The main goal of MMLA is to provide more detailed, contextualized, and actionable feedback to teachers, students, and developers of educational materials [8]. Teachers can better understand the individual needs of their students, identify those in need of support, and adapt their teaching methods. Interpreting “source” MMLA data is a suitable task for large language models (LLMs) to automatically synthesize into comprehensible and pedagogically relevant reports [22]. MMLA offers the potential for understanding and personalizing learning through rich behavioral data, but at the same time it poses significant ethical and practical HMI challenges. These relate to student privacy (collecting sensitive data such as gaze or physiology), proper interpretation of data, the potential for algorithmic bias in assessment, and the burden on educators who need to evaluate these complex analyses.Modern generative AI models can be used for automated or semi-automated creation of educational materials [14]. Combining VR/AR technologies with multimodal inputs (voice commands, hand and body movement tracking, haptic feedback) allows for the creation of highly immersive and interactive learning experiences. Students can safely experiment in virtual labs, explore 3D models of complex systems, or be present during real experiments to validate models.

CONCLUSION

Multimodal artificial intelligence represents a major evolutionary step in AI, fundamentally changing the way machines can perceive, understand and interact with the world and with humans. The ability to process and integrate information from a variety of data modalities - text, image, audio, video, and sensory data - enables these systems to achieve more comprehensive understanding, higher accuracy, and robustness compared to unimodal approaches. The present paper focuses on the application areas of multimodal AI in the financial sector, industry and education, but multimodal AI technologies have the potential to bring transformational change in every sector. In the financial sector, multimodal AI can enhance security through advanced detection, streamline KYC and onboarding processes, or improve the customer experience. However, it also brings challenges related to the protection of sensitive biometric data and the risk of algorithmic bias. In industrial environments, multimodal AI optimizes manufacturing processes, improves worker safety, and offers advanced HMI for managing complex systems. Key challenges are integration, scalability and ensuring reliability in harsh environments.

In education, multimodal AI opens up opportunities for deeper personalisation of the learning process through adaptive systems and intelligent tutors. Multimodal learning analytics (MMLA) provides insights into students' learning strategies, engagement and emotional states by analyzing their behaviors captured by various sensors. AI can also help in creating more effective and engaging multimodal learning content. Ethical issues around student privacy and the interpretation of MMLA data are particularly pressing here. Other challenges relate to data quality and availability, complexity of models, their explainability, robustness (especially to missing data), and above all, ethical implications regarding bias, privacy, and accountability. The future of HMI powered by multimodal AI is moving towards more integrated, intelligent and adaptive systems that are more akin to human communication and collaboration. This evolution can lead to systems that are not just tools, but assist in solving complex tasks. Multimodal AI represents a technology with enormous transformative potential, but its responsible deployment requires a thoughtful and critical approach.

REFERENCES

[1] STRYKER, C., 2024,What is multimodal AI?.Online document. Retrieved from:https://www.ibm.com/think/topics/multimodal-ai

[2] What is Multimodal AI? Technology that Sees, Hears, and Understands, 2024. Online document. Retrieved from: https://konghq.com/blog/learning-center/what-is-multimodal-ai

[3] Human-Machine Interface Design. Fiveable library. Online document. Retrieved from:https://library.fiveable.me/introduction-industrial-engineering/unit-8/human-machine-interface-design/study-guide/KhyeAEh6VYKIU1UT

[4] Multimodal AI Models and Modalities. Copilotly. Online document. Retrieved from: https://www.copilotly.com/ai-glossary/multimodal-ai-models-and-modalities

[5] Finance Companies That Use Computer Vision.Visionify. Online document. Retrieved from: https://visionify.ai/articles/computer-vision-finance-companies

[6] BEAS, L., LOVETH, C., OKUNOLA, A. et. al.: Multi-Modal AI for Fraud Detection: Integrating Behavioral Biometrics and Transaction Data in Financial Security. ResearchGate, 2025. Online document. Retrieved from: https://www.researchgate.net/publication/390236459_Multi-Modal_AI_for_Fraud_Detection_Integrating_Behavioral_Biometrics_and_Transaction_Data_in_Financial_Security

[7] Explore cutting-edge AI problem statements and harness the power of artificial intelligence to create innovative solutions that can transform industries and improve lives. In: Make a Thon 6.0, 2025. Online document. Retrieved from:https://make-a-thon-6-0.vercel.app/problems/ai

[8] SANKAR, A., JOSHITH, V. P.: Multimodal Learning Analytics (MMLA) In Education - A Game Changer for Educators. ResearchGate, 2025. Online document. Retrieved from: https://www.researchgate.net/publication/389285462_Multimodal_Learning_Analytics_MMLA_In_Education_-_A_Game_Changer_for_Educators

[9] Vision Transformer (ViT) Architecture. 2025. Online document. Retrieved from: https://www.geeksforgeeks.org/vision-transformer-vit-architecture/

[10] Multimodal AI MarketTill 2035. In: Roots Analysis Market Report. Online document. Retrieved from: https://www.rootsanalysis.com/multimodal-ai-market

[11] RENGIFO, J., MURÚA, T.: Exploring CLIP alternatives - Analyzing alternatives to the CLIP model for image-to-image, and text-to-image search. 2025. Online document. Retrieved from: https://www.elastic.co/search-labs/blog/openai-clip-alternatives

[12] Unlocking the Potential of Multimodal AI in 2024. 2024. Online document. Retrieved from: https://www.toolify.ai/ai-news/unlocking-the-potential-of-multimodal-ai-in-2024-1362345

[13] WU, R., WANG, H., CHEN, H. T.: A Comprehensive Survey on Deep Multimodal Learning with Missing Modality. ArXiv, 2024. Online document. Retrieved from: https://arxiv.org/html/2409.07825v1

[14] BEGUM, I.: HCI and its use in design and development of good user interface. In: IRET – International Journal in Research in Engineering and Technology, 2014. Online document. Retrieved from: https://www.scribd.com/document/331005708/HCI-AND-ITS-EFFECTIVE-USE-IN-DESIGN-AND-pdf
[15] STOFFOVÁ, V.: Use of ICT in the teacher profession – Creation of didactic applications. In: DIDINFO – sborníkkonference. Liberec, 2018. ISSN978-80-7494-424-6. Online document. Retrieved from: https://www.didinfo.net/images/DidInfo/files/Didinfo_2018.pdf
[16] JIANG, L.: SynergyAI: A Human–AI Pair Programming Tool Based on Dataflow. MDPI, 2025. Online document. Retrieved from: https://www.mdpi.com/2078-2489/16/3/178
[17] Conversational content generation: Chatting with Algorithms - The Magic Behind Conversational Content. FasterCapital, 2025. Online document. Retrieved from: https://fastercapital.com/content/Conversational-content-generation--Chatting-with-Algorithms--The-Magic-Behind-Conversational-Content.html
[18] SANO, A., JOHNS, P., CZERWINSKI, M.: Designing opportune stress intervention delivery timing using multi-modal data. In: 2017 Seventh International Conference on Affective Computing and Intelligent Interaction (ACII). ResearchGate, 2017. Online document. Retrieved from: https://www.researchgate.net/publication/322881821_Designing_opportune_stress_intervention_delivery_timing_using_multi-modal_data
[19] YUAN, F., XIANYI, G., LINDQVIST, J.: How Busy Are You?: Predicting the Interruptibility Intensity of Mobile Users. In: the 2017 CHI Conference. Online document. Retrieved from: https://www.researchgate.net/publication/316708988_How_Busy_Are_You_Predicting_the_Interruptibility_Intensity_of_Mobile_Users
[20] DWIVEDI, P., KHAN, Z., ANSARI, H. et al.:Predictive Maintenance and Monitoring of Industrial Compressors Using MachineLearning - A Proactive Approach. In: Metallurgical and Materials Engineering. 2025. Vol 31. p. 372-381. Online document. Retrieved from: https://metall-mater-eng.com/index.php/home/article/download/1387/769/4956
[21] PARK, S., YOUM, M., KIM, J.: IMU Sensor-Based Worker Behavior Recognition and Construction of a Cyber–Physical System Environment. PMC – PubMed Central, 2025. Online document. Retrieved from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11768975/
[22] DAVALOS, E., ZHANG, Y., SRIVASTAVA, N. et al.: LLMs as Educational Analysts: Transforming Multimodal Data Traces into Actionable Reading Assessment Reports. Online document. Retrieved from: https://arxiv.org/html/2503.02099v1
[23] NATH, S., LI, J., MUSTI, M. et. al: Generative AI and multi-modal agents in AWS - The key to unlocking new value in financial markets.2023. Online document. Retrieved from: https://aws.amazon.com/blogs/machine-learning/generative-ai-and-multi-modal-agents-in-aws-the-key-to-unlocking-new-value-in-financial-markets/
[24] HOSP, B., EIVAZI, S., MAUER, M. et. al.: RemoteEye - An open-source high-speed remote eye tracker. SpringerNature Link, 2020. Online document. Retrieved from: https://doi.org/10.3758/s13428-019-01305-2

Mgr. René Klaučo, PhD.: https://orcid.org/0009-0008-2590-6198

Prof. Ing. Ladislav Várkoly, PhD.

THE SIMILARITY BETWEEN IMPROVING COMPUTER PERFORMANCE AND BASAL STIMULATION METHODS

Mgr. Marcela MUŠÁKOVÁ, MBA[1], Prof. Ing. Ladislav VÁRKOLY, PhD.[2], Mgr. René KLAUCO, PhD.[3]

CEO, Terézia n.o., Lokca, Slovakia[1]

Professional guarantor, INTERNET SCHOOL – Educational social network and digital library, Poprad, Slovakia[2]

Founder, KLAUCODE – High-Performance digital solutions for modern business, Poprad, Slovakia[3]

riaditel@terezia-lokca.sk[1], kolysama7@gmail.com[2], rene@klauco.de[3]

ABSTRACT: This conference paper explores the parallels between optimizing computer applications and stimulating the human body through the concept of Basal Stimulation. Just as one can equate visual impairment due to damage to the retina of the eyes to "burned out" pixels on a screen, one can equate an increase in computer performance (e.g., "making the computer faster") to an improvement in human body function through targeted stimulation. Supporting the enhancement of quality of life and sensory perception is addressed by methods such as 'Somatic Stimulation' and 'Vestibular Stimulation'. This paper presents the concept of Basal Stimulation, which focuses on maintaining and improving motor and sensory pathways, similar to software optimization to prevent performance deterioration. Techniques such as "Initial Touch" and "Contact Breathing" are presented as specific interventions, similar to software updates or debugging. This analogy suggests that understanding and applying the principles of stimulation can significantly impact a person's quality of life, especially for those with limited mobility or sensory impairments. This paper is based on the practical application of Basal Stimulation methods at Theresa, n. o., Lokca.

Key words: basal stimulation, somatic stimulation, vestibular stimulation, motor and sensory pathways

INTRODUCTION

In the environment of modern medicine and special education, interdisciplinary approaches are increasingly being sought to enable new perspectives on the care of people with limited mobility or sensory impairments. One such approach is Basal Stimulation, a therapeutic-treatment concept that finds application in work with people with severe central nervous system impairment, in geriatric care or with patients in a minimally conscious state.

In this paper, we attempt an unconventional connection between the world of information technology and human neurophysiology through an analogy between optimization of computational systems and goal-directed stimulation of the human body. Just as a modern computer requires regular maintenance, tuning, and updating, the human body needs external stimuli that activate sensory and motor pathways, prevent their decay, and promote neuroplasticity. Using selected methods of Basal Stimulation such as Initial Touch, Contact Breathing, Somatic Stimulation and Vestibular Stimulation as examples, we show how purposefully administered stimulation can lead to improved quality of life for people with severely limited mobility or communication skills. We draw on the practical experience of the organisation Terézia, n. o., Lokca, where these techniques are systematically applied in everyday care.

1. BASAL STIMULATION

Basal stimulation is a comprehensive educational and nursing concept that is based on the principles of early human development, particularly the way in which individuals from birth gain experience through their own bodies. It aims to activate the basic physical, sensory, emotional and communicative functions that are essential for the development of identity and contact with the environment. This approach

originated as a response to the needs of people with severe physical, intellectual or combined disabilities, but has gradually spread to the fields of geriatrics, intensive medicine or palliative care [1].

Figure 1. Terézia n.o., Lokca.

Basal stimulation methods have been applied in Terézia, n.o. since 2022. Currently, 75% of the professional staff is trained in the concept of basal stimulation. The individual techniques of the concept are defined in the care plan of the social service recipients and are subsequently translated into the individual plans of the social service recipients.

Tab. 1. Definitions of Basal Stimulation.

according to prof. Andreas Fröhlich, author of the concept	Basal stimulation is a way of contacting people who have limited ability to communicate and move, through basic sensory stimuli that are understandable even in the case of deeper perceptual and movement impairments
from the perspective of special pedagogy	Basal stimulation is a didactic-therapeutic approach that uses primary sensory experiences (touch, pressure, vibration, positioning, movement) to promote personality development and learning in people with severe disabilities.
from a nursing perspective	It is a nursing intervention aimed at preserving or restoring body perception, improving orientation in space and time, as well as reinforcing a basic sense of security and confidence through targeted stimuli.
from a neurophysiological point of view	Basal stimulation promotes the activation of sensory and motor nerve pathways through repetitive stimuli, thereby contributing to the plasticity of the nervous system and slowing or reversing regressive processes caused by inactivity, disease or aging.

2. BASIC PRINCIPLES OF BASAL STIMULATION

Basal stimulation supports the perception of one's own body, the development of one's own identity, the perception of the surrounding world, the establishment of communication with the environment, the mastery of orientation in space and time, locomotor (movement) abilities, the improvement of the body's functions, the psychomotor development of man, respect for human autonomy, dignified survival and other factors in order to enable the living of life in the highest possible degree of quality (even in severe conditions with a poor prognosis).

Tab. 2. Basic principles of basal stimulation [2].

Individualisation of stimuli	Each stimulus is tailored to the individual, his/her condition and current possibilities
Sensory activity	Different types of stimulation are used - tactile (touch), vestibular (balance), proprioceptive (intrathecal), auditory (hearing), olfactory (smell) and others
Promoting the bodily self	Through bodily contact and stimulation, the perception of one's own body is developed, which is the basis for a sense of identity and self-determination
Relational dimension	Stimulation takes place in a secure relationship with another person - be it a therapist, carer, teacher or medical staff

2.1. INITIAL TOUCH

The initiating touch is a purposeful touch on the patient's body, through which information is given to the patient about the beginning of the interaction ("now I have come", "I am here for you") and its ending ("now we will say goodbye") [3]. It serves as a ritualized greeting and farewell and helps the patient to recognize the form of the initiation of contact. It provides a sense of respect, reassurance and trust [4]. The site of the initial touch is chosen individually (e.g., shoulder, hand) and should be consistent across caregivers and family members. Information about the chosen touch site should be visible. This technique is particularly useful for patients who have difficulty processing auditory information or are easily startled by sudden touch [3]. Initial touch emphasizes the importance of nonverbal communication and establishing a predictable and safe interaction for individuals with sensory or cognitive impairments. The ritualized nature and consistent application are intended to provide the patient with a sense of security, reduce anxiety, etc. [4].

2.2. SOMATIC STIMULATION

Somatic stimulation focuses on stimulating the perception of body schema and skin receptors through touch [4]. It involves deliberate and clear touching using both hands. Individuals are divided into soothing stimulation, which is performed in the direction of hair growth (top to bottom), and stimulating stimulation, which is performed against the direction of hair growth (bottom to top) [4]. Encouraging stimulation is used to stimulate attention and increase the level of consciousness of the treated, potentially prior to rehabilitation [7]. Soothing stimulation may include general baths or massage [4]. It can be applied using a variety of aids such as washcloths, towels, body lotions or terry socks [5]. It includes techniques such as stimulating or relaxing baths (total or partial) [6]. The aim is to enable patients with motor disorders to regain sensation of the affected body part [5]. The quality of somatic stimulation depends on the quality of the nursing touches [8]. The distinction between soothing and stimulating somatic stimulation demonstrates the nuanced use of touch to achieve different physiological and attentional states. The use of common objects such as towels and body lotions highlights the accessibility and low-cost nature of somatic stimulation [5].

Somatic stimulation allows re-perception of the body schema and stimulation of skin receptors. The best form we can stimulate is a form of touch. If a person is bedridden for a long time, unable to move, or if their movement is severely restricted compared to a healthy person, they gradually cease to perceive the boundaries of their body. In somatic stimulation, we gradually name the parts of the client's body that we are currently moving through as we touch their body. The possibilities of somatic stimulation according to the concept of Basal Stimulation [9]:

- soothing somatic stimulation,
- stimulating somatic stimulation,

- neurophysiological stimulation,
- positioning,
- massage stimulating breathing (MSD),
- contact breathing.

2.3. CONTACT BREATHING

Contact breathing is one form of somatic stimulation in basal stimulation, which aims to re-perceive the body schema and stimulate skin receptors through touch [4]. It is often mentioned together with massage to stimulate breathing [5]. It can be performed with or without vibration [7]. It involves the therapist's hands guiding and stimulating the breathing movements, with the therapist having to pick up the frequency and rhythm of inhalation and exhalation [10]. It may be particularly relevant for patients with rapid or slow breathing and can influence the patient's activity level by ensuring sufficient oxygenation. Contact breathing demonstrates the close association between touch and respiratory function, suggesting a way to influence physiological states through manual interaction. The mention of contact breathing along with massage to stimulate breathing suggests that these are related but potentially distinct techniques within the broader category of respiratory support in basal stimulation.

There are more possibilities for contact breathing. It is possible to work with only one hand of the therapist placed on the client's chest, or with the client's own hand, or with the client's and therapist's hands simultaneously. The client can thus be aware of his own breathing, aware of his own breathing. In contact breathing, where the therapist has both hands on the client's chest and accompanies the client in inhalation and exhalation, it is possible to support the exhalation by very light chest compressions and it is also possible to add vibrations at the time of exhalation. Vibration is added to promote expectoration of mucus. This technique is used in immobile clients [5].

2.4. MASSAGE STIMULATING BREATHING

Breathing is a basic human need; without breathing, life is impossible. People with altered perception of body schema exhibit superficial and rapid breathing. This causes inadequate ventilation of all parts of the lungs, leading to impaired gas exchange between the external and internal environment. Insufficient oxygenation takes away from the physical strength of these clients. MSD is applied to clients with pain, depressive conditions, sleep disorders, dementia or Alzheimer's disease, shallow, shallow breathing, and palliative clients. MSD also contributes to the release of mucus, to better expectoration. Research shows that regular practice of the MSD technique contributes to a reduction in the perception of pain, calming. It is also advisable to perform it before the client sleeps. The technique is simple and pleasant for the client [11].

2.5. VESTIBULAR STIMULATION

Vestibular stimulation stimulates the vestibular apparatus in the inner ear, which is responsible for balance and spatial orientation [4]. Proper functioning of the vestibular system affects upright posture and visual perception. It is essential for maintaining balance and perceiving one's own position in space [7]. It involves slow, rhythmic movements such as rocking, swaying, slow head turning, etc. [6]. It is important for the prevention of dizziness and mood changes in long-term recumbent patients. It helps individuals with limited mobility to become aware of their body in space, which is crucial for rehabilitation. Stimulation should be slow and gentle to avoid overloading the receptors of the vestibular apparatus. It can be provided in a variety of ways such as rocking beds, rocking chairs, swings or fittlepods [7]. Vestibular stimulation targets a critical sensory system, often overlooked in individuals with limited movement, emphasizing the importance of spatial perception for overall well-being and rehabilitation. The variety of methods for delivering vestibular stimulation suggests the flexibility of this technique and the ability to adapt it to different patient conditions and available resources.

People with limited motor activities receive a minimum of vestibular stimuli. Through the vestibular stimulation concept of Basal Stimulation, these clients can be provided with stimuli to their balance system, better spatial orientation and perception of movement. Vestibular perception allows linear, rotational and static head movements to be recorded. It informs us about our position and movement in space. Vestibular stimulation options [7]:

- very slow and easy turning movements of the head,
- rocking movements in bed, e.g. in the mummy position,
- practising the so-called oat cob movement in the oat field (the so-called lying figure of eight).

2.6. POSITIONING

Mummy position - the aim of this position is to understand the limits of your body as intensely as possible and to bring sensations from your own body. The position is suitable for people with reduced mobility, seniors with dementia, people who are disoriented, restless, depressed, aggressive. Procedure: the person being treated is placed on a spread blanket, the head is supported by a pillow, the upper limbs are placed on the chest or next to the body. We wrap the client tightly starting from the feet to the shoulders. Only the head remains sticking out. Push the ends of the blanket underneath the person being treated (but be careful not to push).

Nest position - This position allows to enhance the feeling of pleasant rest, security and improved perception of the limits of one's own body. In positioning it is important that the client feels the touch, the pressure - of a pillow, blanket, towel on their own body. If the body is thus stimulated by touch, pressure, its sensation is not lost. In positioning it is important to use a rolled-up blanket, towel, positioning roller or pillow to frame the whole body around [12].

3. TECHNOLOGY AND STIMULATION OF THE HUMAN BODY

Basal stimulation focuses on optimizing sensory and motor pathways, similar to how computer optimization increases processing speed and efficiency. This analogy suggests that basal stimulation views the human body as a complex system that can be fine-tuned to improve performance, albeit by biological rather than computational means. The loss of a pixel on a screen represents a specific visual deficit, analogous to the impairment of a specific sensory function in humans. Both scenarios lead to a reduced ability to perceive information accurately. This analogy points to the idea that sensory impairments can be localized and specific, affecting particular aspects of perception, much like a discrete impairment in a computer system. Stimulation techniques, such as somatic and vestibular stimulation, target specific sensory and motor pathways to improve their function, much as specific steps are taken to solve problems in a computer system.

Somatic stimulation can be seen as a way of reactivating or recalibrating sensory receptors, while vestibular stimulation helps to restore balance and spatial perception, similar to correcting errors related to these functions in a computer. This analogy suggests an approach to problem solving in basal stimulation where specific techniques are applied to address identified functional deficits in sensory and motor systems. Initial touch creates clear communication protocols, much like software updates ensure seamless interaction between the user and the system. Contact respiration focuses on regulating the underlying physiological process, similar to how bug fixes address and eliminate critical software errors. These analogies emphasize the proactive and corrective nature of basal stimulation techniques in maintaining and improving bodily functions.

Although the user question provides analogies to computer systems, it is important to recognize that the brain and body are much more complex and operate on different principles than current digital technologies [13]. Some argue that the brain may function more like an analog computer [14]. The brain-computer analogy is often used metaphorically rather than literally [15]. Although analogies can be useful for conceptual understanding, the report should emphasize the limitations of directly comparing biological systems with technical computing systems given the fundamental differences in their functioning and complexity.

4. BENEFITS OF BASAL STIMULATION

Basal stimulation aims to provide environmental stimuli and compensate for the lack of independent movement. It stimulates development through many environmental stimuli and multisensory experiences. It helps patients to perceive their own body - body perception [3]. Promotes overall development in those who are limited in communication, perception or movement. Provides a necessary daily dose of stimuli from one's own body and surroundings. Helps individuals feel the limits of their body and perceive the world around them [6]. It focuses on sensorimotor and cognitive development, creating communication channels for those who cannot express themselves verbally. It provides rehabilitative and compassionate care for the body, helping to develop a positive body perception. It is invaluable in critical care [17]. It reduces stress in borderline stressful situations and promotes the development of communication and motor skills [18]. It improves sensory perception, body orientation and non-verbal communication skills [19]. The benefits span the physical, sensory, communication and emotional domains, suggesting a broad positive impact on individuals with limitations.

Research suggests that sensory stimulation, including basal stimulation, can have significant benefits for individuals with dementia and other conditions affecting communication and well-being. It can improve verbal and non-verbal communication in individuals with dementia, improve quality of life and mood and alleviate behavioural symptoms in people with dementia, improve daily functioning [20], provide relief to the child and family in palliative care [17], and reduce feelings of isolation, anxiety and depression [20]. It can also improve cognitive and emotional functioning by engaging different senses [21].


č. 04 /2024
Číslo certifikace

INSTITUT Bazální stimulace podle Prof. Dr. FRÖHLICHA, s. r. o.
J. Opletala 680, 738 02 Frýdek-Místek • IČ: 25889966, DIČ: CZ25889966

11. 03. 2027
Platnost certifikátu

Vzdělávací společnost má licenci od Internationaler Förderverein Basale Stimulation® e.V. pro pořádání certifikovaných kurzů Bazální stimulace v zemích EU, Švýcarsku a Norsku a akreditace Ministerstva zdravotnictví ČR, Ministerstva práce a sociálních věcí ČR, Ministerstva školství, mládeže a tělovýchovy ČR, Ministerstva zdravotnictví Slovenské republiky

uděluje certifikaci

PRACOVIŠTĚ BAZÁLNÍ STIMULACE
podle Prof. Dr. FRÖHLICHA®

Terézia, n.o.
Sládkovičova 450/10, 036 01 Martin; Južná 698/3, 029 51 Lokca

Uvedený poskytovatel sociálních služeb prošel dne 11. 3. 2024 odborným auditem a splnil stanovená kritéria pro certifikaci zařízení v konceptu Bazální stimulace podle Prof. Dr. Fröhlicha®. Jedním z předpokladů certifikace je proškolení personálu přímé péče v akreditovaných vzdělávacích programech Bazální stimulace podle Prof. Dr. Fröhlicha®, které jsou mezinárodně licencované Internationaler Förderverein Basale Stimulation® e. V. s platností ve všech zemích EU, Švýcarsku a Norsku. Základní akreditovaný kurz proběhl ve dnech 28.-29.9.2022.

iBS® INSTITUT BAZÁLNÍ STIMULACE
www.bazalni-stimulace.cz

PhDr. Karolína Malon Friedlová, PhD.
Ředitelka
Praxisbegleiter für Basale Stimulation nach Prof. Dr. Fröhlich®, Nr. 608 v EU

BASALE STIMULATION
INTERNATIONALER FÖRDERVEREIN E.V.

Figure 2. CertificateTerézia n.o., Lokca.

Basal stimulation uses movement and targeted physical interventions to engage and potentially improve motor pathways, which is particularly relevant for individuals with limited mobility or neurological conditions. Movement is an essential element of basal stimulation. A variety of physical postures and manual joint vibration are used [6]. It helps to maintain or stabilize body structure in the brain, which is key to mobility [22]. Microstimulation through movement can provide the brain with necessary information about the body, preserve body perception, and promote self-movement [23]. It can improve motor skills and functional activities in patients after stroke. Electrical stimulation techniques, which share some principles with sensory stimulation, are used to restore functional abilities and activate motor pathways [24].

Basal stimulation explicitly targets multiple sensory modalities to improve perception and awareness, addressing sensory deficits that often accompany limited mobility or neurological conditions. It supports all sensory areas in people with physical and intellectual disabilities and focuses on improving sensory perception. It includes various forms of sensory stimulation such as tactile, auditory, visual, olfactory and gustatory. Sensory stimulation is important for infant development and can improve well-being in adults with developmental disabilities, people with neurocognitive disorders, and older adults. It can help individuals with dementia connect with their environment and improve cognitive and emotional functioning [20] and stimulate neural pathways in the brain, thereby improving cognitive function [21]. It is effective in increasing the level of alertness in patients with disorders of consciousness [25]. Bilateral pathways from the basal forebrain to sensory cortical areas may contribute to synchronous sensory processing [26]. The efficacy of basal stimulation likely depends on its ability to promote neuroplasticity and engage underlying neurological pathways related to sensory processing, motor control, and vigilance.

CONCLUSION

Basal stimulation is an important concept in rehabilitation and care that focuses on stimulating the basic sensory and motor abilities of individuals with various limitations. Its holistic approach, taking into account individual needs and biography, allows for improvements in the areas of perception, communication, movement and overall quality of life. The work of Professor Dr. Andreas Fröhlich laid a solid foundation for this concept, which continues to evolve and find application in a variety of clinical and nursing settings, as demonstrated by the work of Theresa, n. o.

Research literature supports the efficacy of basal stimulation and related sensory stimulation techniques in a variety of populations, including premature infants, individuals with disabilities, post-stroke patients, and individuals with dementia. Although there is extensive evidence of the benefits of basal stimulation, future research should focus on a deeper understanding of its mechanisms of action, optimization of techniques, and investigation of long-term effects. Further studies with larger sample sizes and standardised methodologies will contribute to strengthening the evidence base and expanding the applications of this promising therapeutic approach.

REFERENCES

[1] PINČÁKOVÁ, M.: Edukácia žiaka s ťažkým zdravotným znevýhodnením prostredníctvom bazálnej stimulácie - Osvedčená pedagogická skúsenosť edukačnej praxe In: Moderné vzdelávanie pre vedomostnú spoločnosť. 2013. Online document. Retrieved from: https://mpc-edu.sk/sites/default/files/projekty/vystup/5_ops_pincakova_margita_-_edukacia_ziaka_s_tazkym_zdravotnym_znevyhodnenim.pdf

[2] FRIEDLOVA, K. M.: Bazální stimulace podle prof. Dr. Fröhlicha. Asociace poskytovatelů sociálních služeb, 2024. 978-80-88361-40-4.

[3] Bazálna stimulácia - Spolu to zvládneme, o.z.Online document. Retrieved from:https://burko.sk/bazalna-stimulacia

[4] BÓRIKOVÁ, I., LEPIEŠOVÁ, M.: Bazálna stimulácia. Institut bazální stimulace, 2021. Online document. Retrieved from: https://portal.jfmed.uniba.sk/download.php?fid=1234

[5. Bazálna stimulácia – Bdelakoma. Online document. Retrieved from:https://www.bdelakoma.sk/bazalna-stimulacia

[6] Basal stimulation for promoting the development of people with disabilities. Speciální ZŠ Zahrádka, 2025.Online document. Retrieved from: https://www.zszahradka.cz/en/stranka-basal-stimulation-76

[7] Bazálna stimulácia – séria článkov. Infora, 2025. Online document. Retrieved from:https://www.infora.sk/clanky

[8] Využitie princípu bazálnej stimulácie v starostlivosti o pacientov s ..., accessed on April 2, 2025, https://www.seniorzone.cz/33/vyuzitie-principu-bazalnej-stimulacie-v-starostlivosti-o-pacientov-s-alzheimerovou-chorobou-uniqueidmRRWSbk196FNf8-jVUh4ErIHWTr4_CGKTaJcc3HSKBQ/

[9]Bazálna stimulácia | Centrum pre deti a rodiny Košice - Hurbanova, accessed on April 2, 2025, https://cdrkosice.edupage.org/a/bazalna-stimulacia
[10] Postupy fyzioterapeutickej intervencie u predčasne narodeného dieťaťa - VitalClinic, accessed on April 2, 2025, https://vitalclinic.sk/postupy-fyzioterapeutickej-intervencie-u-predcasne-narodeneho-dietata/
[11] MICHALKOVÁ, M.: Polohovací špeciál. In: Workshop v oblasti polohovania, 2019. Online document. Retrieved from: http://www.zmyselzivota.sk/canisterapia/polohovaci_workshop.html
[12] BOROVSKÁ, M.: Viacnásobné postihnutie – využitie bazálnej stinulácie u detí mladšieho školského veku. In: Štandardy – národný projekt. Odborné postupy v pedagogickej a poradenskej praxi. Online document: Retrieved from: https://vudpap.sk/wp-content/uploads/2022/08/Viacnasobne-postihnutie-vyuzitie-bazalnej-stimulacie-u-deti-mladsieho-skolskeho-veku.pdf
[13] AERTER, P. J.: The computational power of the human brain. PMC - PubMed Central, 2023. Online document. Retrieved from:https://pmc.ncbi.nlm.nih.gov/articles/PMC10441807
[14] DIEPENBROCK, G.: Philosopher wins NSF grant to study how our brains are like analog computers. In: KU News. Online document. Retrieved from: https://news.ku.edu/news/article/2018/03/27/philosopher-wins-nsf-grant-study-how-our-brains-are-analog-computers
[15] BASAL STIMULATION - Neuron Rehabilitation. Online document. Retrieved from: https://neuron-rehabilitation.eu/basic-stimulation
[16] BRETTE, R.: Brains as Computers - Metaphor, Analogy, Theory or Fact? In: Frontiers, 2022. Online document. Retrieved from: https://www.frontiersin.org/journals/ecology-and-evolution/articles/10.3389/fevo.2022.878729/full
[17] STANO, K.: Basal stimulation - A Parent's Role in Care. In: Fontan Heart. Online document. Retrieved from: https://www.fontanheart.com/chd-single-ventricle-heart-basal-stimulation/
[18]POTMESILOVA, P., POTMESIL, M., MARECKOVA, J.: Basal stimulation as developmental support in At-Risk newborns. PMC – PubMed Central, 2023. Online document. Retrieved from:https://pmc.ncbi.nlm.nih.gov/articles/PMC9954985
[19] Basal stimulation. Rehamedi. Online document. Retrieved from:https://rehamedi.de/en/glossar/basal-stimulation/
[20] Benefits of Sensory Stimulation For Dementia. Altoida, 2023. Online document. Retrieved from: https://altoida.com/blog/benefits-of-sensory-stimulation-for-dementia
[21] Transform Dementia Care with Multi-Sensory Stimulation. PhysioInq, 2023. Retrieved from: https://www.physioinq.com.au/blog/transform-dementia-care-with-multi-sensory-stimulation
[22] The MiS Micro-Stimulation®, a revolution in care and therapy. Thomashilfen. Online document. Retrieved from: https://www.thomashilfen.com/micro-stimulation
[23] Increase the quality of care with Basal Stimulation. Statewide Home Health Care, 2019. Online document. Retrieved from: https://www.shhc.com.au/blog/statewide-home-health-care-blog/volker-health-care-beds/increase-the-quality-of-care-with-basal-stimulatio/
[24] STROKE, J.: Rewiring the Lesioned Brain - Electrical Stimulation for Post-Stroke Motor Restoration. PMC – PobMed Central, 2020. Retrieved from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7005350
[25] WOODS, B., RAI, H. K. et. al: Can cognitive stimulation benefit people with dementia? Cochrane, 2023. Online document. Retrieved from: https://www.cochrane.org/CD005562/DEMENTIA_can-cognitive-stimulation-benefit-people-dementia
[26] JUN, J., LI, B., SUN, L. Z.: Electro-acupuncture stimulation acts on the basal ganglia output pathway to ameliorate motor impairment in Parkinsonian model rats. PMC– PubMed, 2010. Online document. Retrieved from: https://pubmed.ncbi.nlm.nih.gov/20364891

Mgr. Marcela Mušáková

Prof. Ing. Ladislav Várkoly, PhD.

Mgr. René Klaučo, PhD.: https://orcid.org/0009-0008-2590-6198

ANALYSIS REGULATORS WITH NON-CONVENTIONAL ALGORITHMS USING DIFFERENTIAL EQUATIONS OF INTEGRAL AND NON-INTEGRAL ORDER

Leszek GOŁDYN [1], Ryszard SZCZEBIOT [2]

University of Lomza, Faculty of Computer Science and Technology, Lomza, Poland [1,2]

lgoldyn@al.edu.pl[1], ryszard@szczebiot.pl[2]

ABSTRACT: In the paper, a comparative simulation study of the operation of control systems using different controllers was carried out. An exemplary first-order inertial element with amplification was selected as the control object. A classic PID controller with real derivative action was used as the controller in the first system. In the next two systems, two different controllers with unconventional algorithms using fractional-order differential equations were used. For simulation purposes, models of fractional-order controllers were described using Taylor formulas. Justifying the equality in the approach to differential equations of different orders (integer and fractional), the time characteristics of different orders were determined by simulation and presented in graphical form on a collective graph.

Key words: fractional order differential equation, unconventional algorithm controller, fractional order controller,PID controller

INTRODUCTION

The year 1695 is considered to be the date of the creation of fractional differential calculus. In that year, the Marquis Guillaume François Antoine de l'Hospital (a student of Bernoulli and Leibniz) wrote a letter to his master Gottfried Wilhelm Leibniz asking [1]:

„*What will happen if in the already introduced and recognized derivative notation* $\frac{d^n y}{dx^n}$ *forn*$\in$ *N you insert*$n = \frac{1}{2}$ *?"*

In a letter dated September 30, 1695, Leibniz replied:

"*... This is an apparent paradox from which, one day, useful consequences will be drawn. ...*"

1. COMPARISON OF CONTROL SYSTEMS USING CLASSICAL PID CONTROLLERS AND CONTROLLERS WITH NON-CONVENTIONAL ALGORITHMS

The paper compares the operation of a classical control system with the operation of control systems using unconventional algorithms, e.g. fractional orders. It is practically impossible to implement an ideal derivative element model used in classical PID controllers.

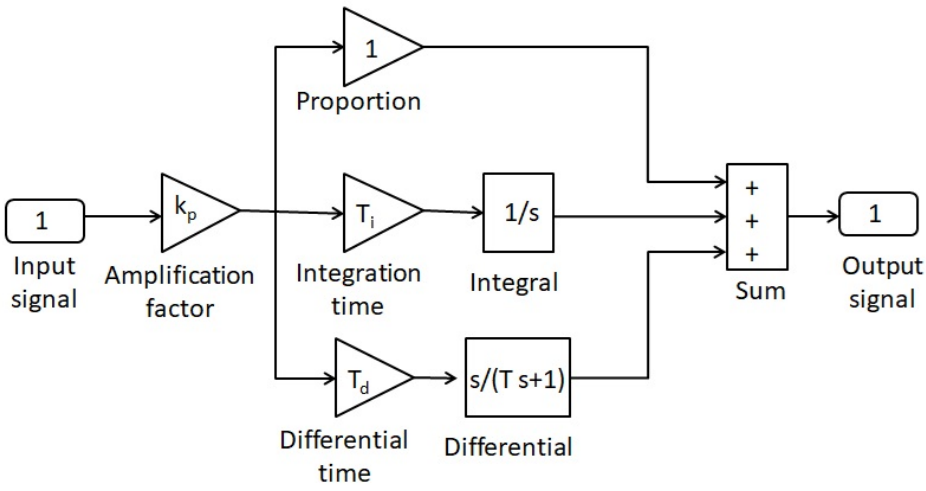


Fig. 1. Block diagram of the actual PID controller.

Therefore, the comparative simulation used a model of a real PID controller with an operator transfer function in the form of:

$$G_{PID}(s) = k_p\left(1 + \frac{1}{T_i s} + \frac{T_d s}{Ts + 1}\right) \tag{1}$$

The block diagram of the controller according to equation (1) is shown in Fig. 1.

2. NON-CONVENTIONAL FRACTIONAL ORDER REGULATORS

Fractional controllers are a typical example of controllers with unconventional algorithms. Their implementation from the practical point of view is quite difficult and complex but possible to perform in a digital way.

A formal description of the modeling of unconventional controllers is given in [2], citing here the description of this model.

The difference in comparison to the classical PID controllers is that the integration or signal differentiation operation is performed by a non-integer function. There are several definitions and calculation methods. They differ in complexity and accuracy of calculations. Most of them are based on the *Γ(x)* function.

Controller with a dynamic fractional differential can be based on Riemann-Liouville's definitions and models. There are also available models of MittagLeffler, Caputo and Grunwald-Letnikova [4]. The transmission of the fractional controller is labeled as G_{ulam}, while the input signal transformation as *X(s)* and the output *Y(s)*. This can be written as follows:

$$G_{ulam}(s) = \frac{Y(s)}{X(s)} \tag{2}$$

If the input signal to the controller is a unit pitch x(t) = 1 with a Laplace transform:

$$X(s) = \frac{1}{s} \tag{3}$$

The output from the controller is the function $y(t) = \frac{1}{\sqrt{t}}$, whose Laplace transform has the form:

$$Y(s) = \sqrt{\frac{\pi}{s}} \tag{4}$$

Then the transmittance of such a fractional controller can be written as:

$$G_{ulam}(s) = \frac{Y(s)}{X(s)} = \frac{\sqrt{\frac{\pi}{s}}}{\frac{1}{s}} = \frac{s\sqrt{\pi}}{\sqrt{s}} = \frac{s\sqrt{\pi}}{s^{\frac{1}{2}}} \tag{5}$$

Finally, the transmittance of the fractional controller has been written as:

$$G_{ulam}(s) = \sqrt{\pi} \cdot s^{\frac{1}{2}} \tag{6}$$

This form of equation is very inconvenient due to the fraction in the exponent of the complex variable s. To describe it, use the Taylor series formula:

$$f(x) = f(a) + \frac{x-a}{1!} f^{(1)}(a) + \frac{(x-a)^2}{2!} f^{(2)}(a) + \ldots + \frac{(x-a)^n}{n!} f^{(n)}(a) + R_n(x,a) \tag{7}$$

where the expression is called the rest of Taylor's formula and satisfies condition:

$$\lim_{x \to a} \frac{R_n(x,a)}{(x-a)^n} = 0 \tag{8}$$

Taylor function approximation is local, ie it refers to the point a. If there is a need to speak of other values, then it is assumed that they are sufficiently close to the point a, that is, in the neighborhood. In order for Taylor polynomial (6) polynomials to approximate functions with specified precision it is necessary to more accurately estimate the remainder or express it explicitly.

The approximation $s^{1/2}$ using the Taylor formula in the neighborhood of the point $a=1$ shows the relation:

$$\begin{aligned} s^{\frac{1}{2}} = & 1+0.5(s-1)-0.1250(s-1)^2+0.0625(s-1)^3-0.0391(s-1)^4+0.0273(s-1)^5-0.0205(s-1)^6+ \\ & +0.0161(s-1)^7-0.0131(s-1)^8+0.0109(s-1)^9-0.0093(s-1)^{10}+0.008(s-1)^{11}-0.007(s-1)^{12}+ \\ & +0.0062(s-1)^{13}-0.0055(s-1)^{14}+0.005(s-1)^{15}-0.0045(s-1)^{16}+0.0041(s-1)^{17}- \\ & -0.0038(s-1)^{18}+0.0035(s-1)^{19}-0.0032(s-1)^{20}+0.003(s-1)^{21}-0.0028(s-1)^{22}+ \\ & +0.0026(s-1)^{23}-0.0024(s-1)^{24}+0.0023(s-1)^{25}-0.0022(s-1)^{26}+0.002(s-1)^{27}- \\ & -0.0019(s-1)^{28}+0.0018(s-1)^{29}-0.0017(s-1)^{30}+0.0017(s-1)^{31}-0.0016(s-1)^{32}+ \\ & +0.0015(s-1)^{33}-0.0014(s-1)^{34}+0.0014(s-1)^{35}-0.0013(s-1)^{36}+0.0013(s-1)^{3}- \\ & -0.0012(s-1)^{38}+0.0012(s-1)^{3}-0.0011(s-1)^{40}+0.0011(s-1)^{41}-0.001(s-1)^{42}+ \\ & +0.001(s-1)^{43}-0.00097(s-1)^{44}+0.00094(s-1)^{45}-0.00091(s-1)^{46}+0.00088(s-1)^{47}- \\ & -0.00085(s-1)^{48}+0.00082(s-1)^{49}-0.0008(s-1)^{50} \end{aligned} \tag{9}$$

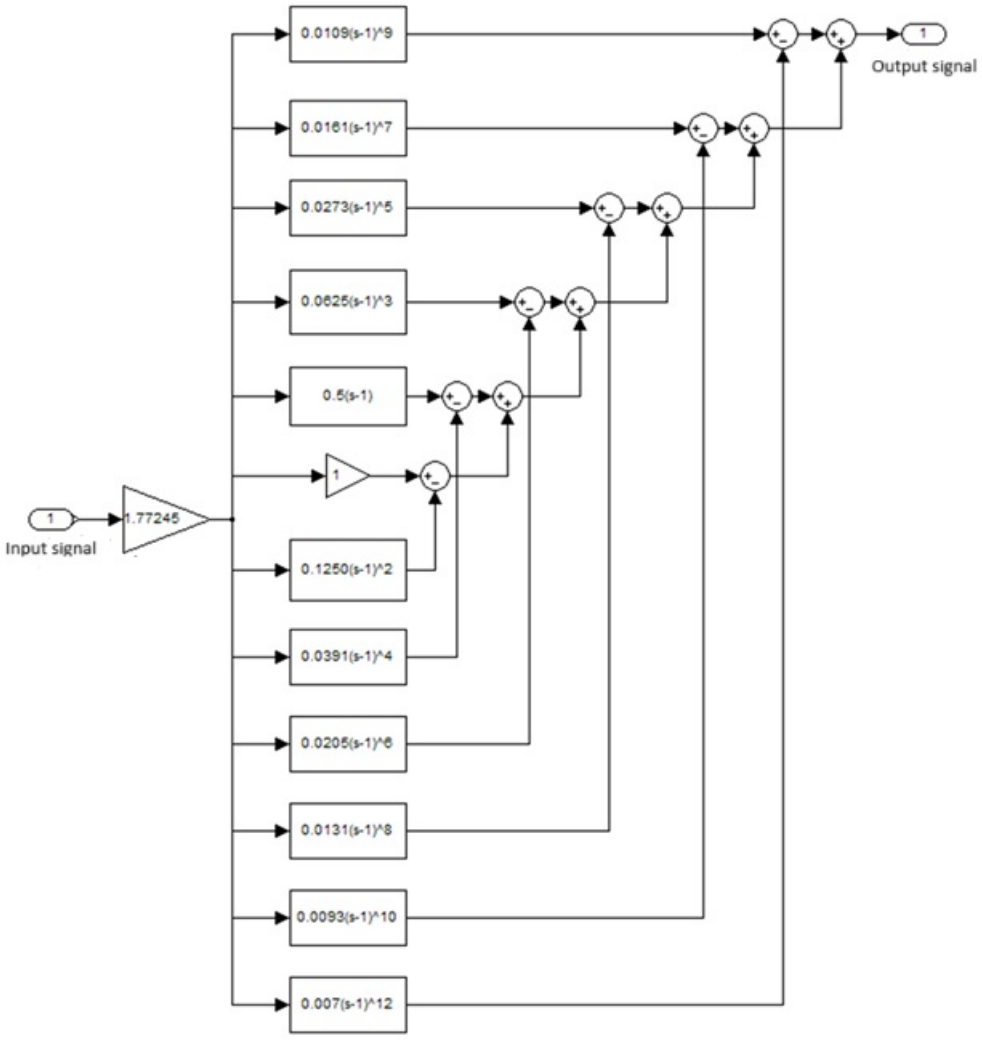


Fig. 2. Block diagram of a positive fractional regulator with transfer function (10).

We can also create other fractional controllers. Let the input signal to the controller be again a unit step *x(t)=1*, and the output signal from the controller be the function y(t)= $\sqrt{t}$, whose Laplace transform has the form:

$$Y(s) = \frac{\sqrt{\pi}}{2} \cdot \frac{1}{s^{\frac{3}{2}}} \tag{11}$$

then the transfer function of such a fractional controller can be written as:

$$G_{ulam}(s) = \frac{\frac{\sqrt{\pi}}{2} \cdot \frac{1}{s^{\frac{3}{2}}}}{\frac{1}{s}} = \frac{\sqrt{\pi}}{2} \cdot \frac{s}{s^{\frac{3}{2}}} \tag{12}$$

Ultimately, the transfer function of the fractional controller is as follows:

$$G_{ulam}(s) = \frac{\sqrt{\pi}}{2} \cdot s^{-\frac{1}{2}} \tag{13}$$

Once again, it is necessary to use Taylor's formula, and the approximation $s^{-1/2}$ in the vicinity of point *a=1* is presented by the equation:

$$\begin{aligned} s^{-\frac{1}{2}} = {} & 1-0.5(s-1)+0.375(s-1)^2-0.3125(s-1)^3+0.2734(s-1)^4-0.2461(s-1)^5+0.2256(s-1)^6- \\ & -0.2095(s-1)^7+0.1964(s-1)^8-0.1855(s-1)^9+0.1762(s-1)^{10}-0.1682(s-1)^{11}+ \\ & +0.1612(s-1)^{12}-0.1550(s-1)^{13}+0.1494(s-1)^{14}-0.1445(s-1)^{15}+0.1399(s-1)^{16}- \\ & -0.1358(s-1)^{17}+0.1321(s-1)^{18}-0.1286(s-1)^{19}+0.1254(s-1)^{20}-0.1224(s-1)^{21}+ \\ & +0.1196(s-1)^{22}-0.117(s-1)^{23}+0.1146(s-1)^{24}-0.1123(s-1)^{25}+0.1101(s-1)^{26}- \\ & -0.1081(s-1)^{27}+0.1061(s-1)^{28}-0.1043(s-1)^{29}+0.1026(s-1)^{30}-0.1008(s-1)^{31}+ \\ & +0.0993(s-1)^{32}-0.0978(s-1)^{33}+0.0964(s-1)^{34}-0.095(s-1)^{35}+0.0937(s-1)^{36}- \\ & -0.0924(s-1)^{37}+0.0912(s-1)^{38}-0.0901(s-1)^{39}+0.0889(s-1)^{40}-0.0878(s-1)^{41}+ \\ & +0.0868(s-1)^{42}-0.0858(s-1)^{43}+0.0848(s-1)^{44}-0.0839(s-1)^{45}+0.0830(s-1)^{46}- \\ & -0.0821(s-1)^{47}+0.0812(s-1)^{48}-0.0804(s-1)^{49}+0.0796(s-1)^5 \end{aligned} \tag{14}$$

So the controller's transfer function is:

$$\begin{aligned} G_{ulam}(s) = \frac{\sqrt{\pi}}{2} \cdot s^{-\frac{1}{2}} \approx {} & 0.886225(1-0.5(s-1)+0.375(s-1)^2-0.3125(s-1)^3+0.2734(s-1)^4-0.2461(s-1)^5+0.2256(s-1)^6 \\ & -0.2095(s-1)^7+0.1964(s-1)^8-0.1855(s-1)^9+0.1762(s-1)^{10}-0.1682(s-1)^{11}+ \\ & +0.1612(s-1)^{12}-0.1550(s-1)^{13}+0.1494(s-1)^{14}-0.1445(s-1)^{15}+0.1399(s-1)^{16}- \\ & -0.1358(s-1)^{17}+0.1321(s-1)^{18}-0.1286(s-1)^{19}+0.1254(s-1)^{20}-0.1224(s-1)^{21}+ \\ & +0.1196(s-1)^{22}-0.117(s-1)^{23}+0.1146(s-1)^{24}-0.1123(s-1)^{25}+0.1101(s-1)^{26}- \\ & -0.1081(s-1)^{27}+0.1061(s-1)^{28}-0.1043(s-1)^{29}+0.1026(s-1)^{30}-0.1008(s-1)^{31}+ \\ & +0.0993(s-1)^{32}-0.0978(s-1)^{33}+0.0964(s-1)^{34}-0.095(s-1)^{35}+0.0937(s-1)^{36}- \\ & -0.0924(s-1)^{37}+0.0912(s-1)^{38}-0.0901(s-1)^{39}+0.0889(s-1)^{40}-0.0878(s-1)^{41}+ \\ & +0.0868(s-1)^{42}-0.0858(s-1)^{43}+0.0848(s-1)^{44}-0.0839(s-1)^{45}+0.0830(s-1)^{46}- \\ & -0.0821(s-1)^{47}+0.0812(s-1)^{48}-0.0804(s-1)^{49}+0.0796(s-1)^{50}) \end{aligned} \tag{15}$$

The block diagram of the thirteenth-degree negative fractional controller based on the transfer function (15) is shown in Fig. 3.

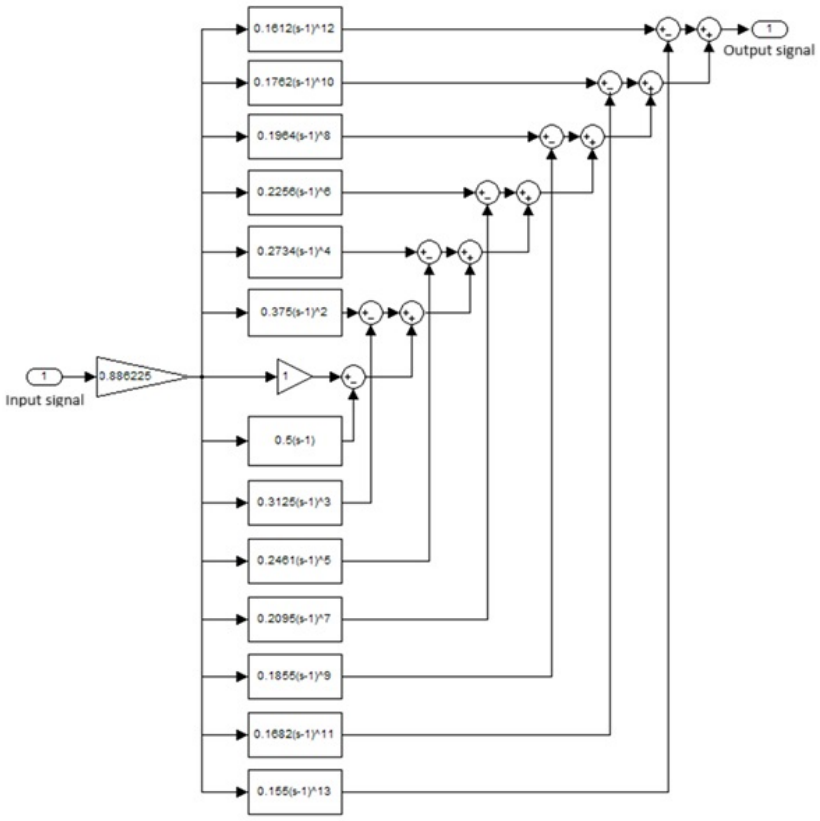


Fig. 3. Block diagram of a negative fractional regulator with transfer function (15).

For an example control object (first-order inertia with amplification), a simulation analysis was performed using a classical PID controller and a positive and negative unconventional fractional-order controller.

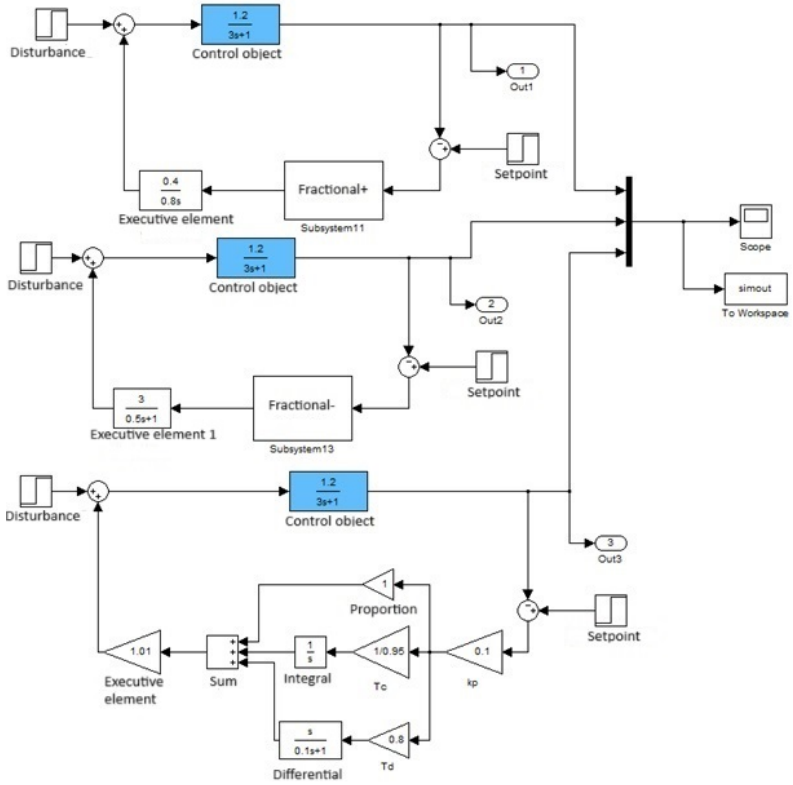


Fig. 4. Block diagram for the analysis of simulation tests of control systems with selected controllers.

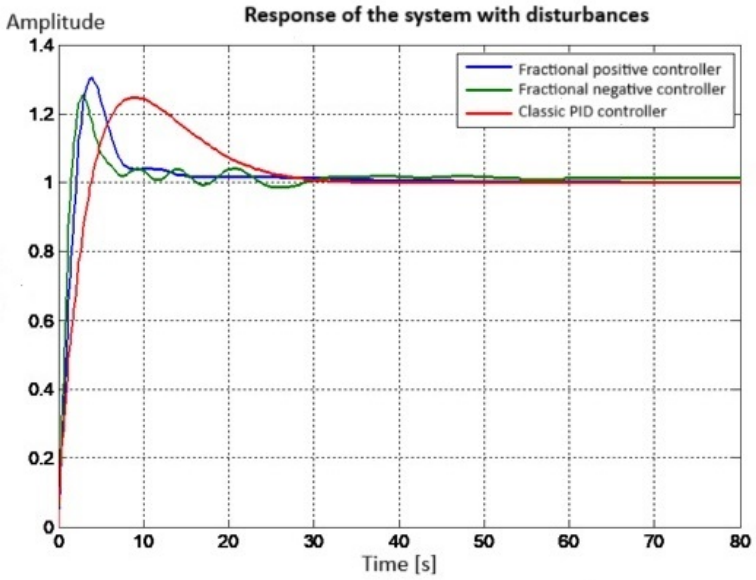


Fig. 5. Comparative dynamic characteristics of control systems with classical and unconventional controllers.

After performing the analysis, we can see that the fractional controller is definitely better than the classic PID controller, because it reacts faster to the change of the input signal. This allows for a faster reaction of a given system in which the fractional controller is located.

The rise and regulation times, compared to the classic controller, decreased, there was no overshoot, and the system was characterized by greater resistance to interference and returned to equilibrium in a shorter time. By increasing the gain coefficients of the synthesized fractional controllers accordingly, it is possible to reduce the regulation errors and bring the steady-state value closer to the setpoint, as well as reduce the regulation times and oscillations.

3. UNCONVENTIONAL MODELING WITH FRACTIONAL ORDER EQUATIONS

The exemplary model differential equation was comparatively solved by changing its order from 1 to 6 by 0.2. The whole family of waveforms was obtained, shown in Fig. 6.

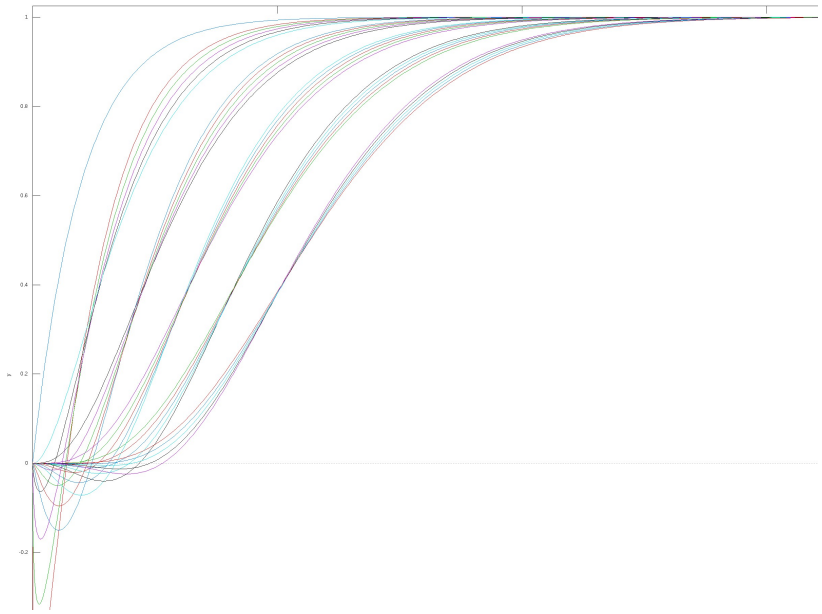


Fig. 6. Dynamic characteristics solutions of the order of 1 to 6 equations [3].

The presented curves [2, 3] lead to a very important, even fundamental engineering conclusion about the continuity of solutions of integral and fractional order differential equations. The solution y(t) of the integral order equation is contained in the set of solutions of the fractional order equation:

$$\lim_{v \to 1^{\pm}} y_v(t) = y_1(t) \tag{16}$$

CONCLUSION

The task of the control system is to maintain constant output parameters, at a steady state of operation. Automatic control systems have very complex structures, and depending on the requirements they have, they contain more or less control and regulating elements. Among the devices used, it is necessary to use a regulator. Classical regulators are gradually being replaced by digital regulators, thanks to which it is possible to obtain:

- reducing the complexity of executive systems,
- increasing the reliability of automatic control system components,
- the ability to easily and quickly change the control program,
- changing and using unconventional controllers.

Taking into account the analysis of the dynamic characteristics of solutions of the order of 1 to 6 equations, it can be concluded that the so-called classical differential-integral calculus [5] and fractional-order differential-integral calculus constitute one compatible family.

Along with the new dynamic elements, a seemingly new mathematical tool has appeared: fractional-order differential-integral calculus.

Lower fractional-order differential equations describe more precisely (they constitute a better mathematical model) many physical phenomena, e.g. inductive couplings in electrical engineering or classical electrical circuits, in mechanics, in control and regulation systems. Currently, fractional-order differential equations are used in the construction of fractional-order controllers and they fulfill their role very well in control systems.

REFERENCES

[1] CAMPISTROUS, Luis Augusto; LOPEZ, J. M.; RIZO, C. (2009), Reflexiones sobre la didáctica del cálculo a propósito de una lectura del primer texto publicado sobre esta materia por el Marqués Guillaume François Antoine L'Hospital: Analyse des infiniment petits pour l'intelligence des lignes courbes.

[2] GOŁDYN Leszek, SZCZEBIOT Ryszard, (2017), VARIABLE PID CONTROLLERS AND UNCONVENTIONAL CONTROLLERS, Present Day Trends of Innovations 7, Lomza State University of Applied Sciences, Łomża 2017, ed. Ladislav Várkoly, Michal Zábovský, Ryszard Szczebiot, pp. 94-108, ISBN 978-83-60571-49-1

[3] GOŁDYN Leszek, SZCZEBIOT Ryszard, (2017), PARAMETRIC IDENTIFICATION OF MATHEMATICAL MODELS OF INTEGER AND FRACTIONAL ORDERS, Present Day Trends of Innovations 7, Lomza State University of Applied Sciences, Łomża 2017, ed. Ladislav Várkoly, Michal Zábovský, Ryszard Szczebiot, pp. 108-119, ISBN 978-83-60571-49-1

[4] Caputo's definitions for the description and initialization of fractional partial differential equations. *IFAC-Papers On Line*, 2017, 50.1: 8574-8579.

[5] Kaczorek T., Dzieliński A., Dąbrowski W., Łopatka R.,(2005) Podstawy teorii sterowania, WNT, Warszawa.

Leszek Gołdyn: https://orcid.org/0000-0002-0689-8590

Ryszard Szczebiot: https://orcid.org/0000-0002-9084-915X

Hybrid LSTM Models with Attention Mechanism for Forecasting Smog Episodes under Extreme Conditions

Dr Eng. Aneta Wiktorzak

University of Lomza, Lomza, POLAND

awiktorzak@al.edu.pl

ABSTRACT: This article presents the application of a hybrid model based on LSTM networks with an attention mechanism for forecasting PM10 and PM2.5 pollutant concentrations under extreme weather conditions. The objective of the study was to improve the accuracy of smog prediction during high-risk periods when standard models tend to become unstable. The LSTM+Attention model was compared with classical approaches (pure LSTM and NARX). The network was trained using data from over 40 InConTech sensors located in the Podlaskie Voivodeship, as well as meteorological data from the IMGW API. The results confirm that incorporating the attention layer significantly enhances prediction performance, especially during sudden meteorological shifts and pollution spikes.

Key words: LSTM+Attention, prediction, PM10, PM2.5

INTRODUCTION

Air pollution is one of the most pressing challenges faced by modern societies, both in terms of public health and environmental protection. Particulate matter PM10 and PM2.5 are atmospheric aerosols with diameters of up to 10 and 2.5 micrometers, respectively. These particles are capable of penetrating the human respiratory system, and the smaller ones can even enter the bloodstream. According to data from the World Health Organization (WHO), long-term exposure to high concentrations of these pollutants can lead to chronic respiratory and cardiovascular diseases, and increase the risk of premature death.

In Poland, the problem of smog is particularly severe during the autumn and winter months. Due to low temperatures and emissions from the residential sector (e.g., burning coal in household furnaces), pollution levels rise sharply. Additionally, adverse meteorological conditions such as temperature inversions and lack of wind contribute to the accumulation of particulate matter in the lower layers of the atmosphere.

In response to these challenges, recent years have seen growing interest in the use of artificial intelligence tools to forecast air pollution levels. Machine learning algorithms, particularly those based on deep learning [11], have proven effective in analyzing time series data and predicting values based on historical trends. Among these tools, recurrent neural networks (RNNs), and especially their enhanced version Long Short-Term Memory (LSTM) play a key role [1].

LSTM is a sequence-processing architecture designed to store and update information over longer time horizons, which is crucial in air quality forecasting, where the impact of a meteorological event may be delayed by several hours. However, in practice, traditional LSTM models, while effective at predicting general trends, may struggle to respond adequately to sudden environmental changes [4].

This study proposes an extension of the LSTM architecture with an attention mechanism [2], enabling the network to "focus" on relevant segments of the input sequence by assigning them greater importance during decision-making. This approach has already proven successful in machine translation and speech recognition tasks, and its application to air pollution forecasting represents a promising new research direction. The presented study builds on the author's earlier work in smog modeling and prediction using artificial intelligence, with particular emphasis on model explainability and robustness to input variability.

The following sections detail the data sets used, the model architecture, training methodology, and a comparative analysis of model performance with and without the attention layer. Examples of predictions under extreme conditions are also presented, along with an assessment of the potential practical applications of the developed solution in early warning systems and air quality management.

1. DATA AND METHODOLOGY

1.1. DATA SETS

To conduct the study, integrated data sources were used, including both air quality measurements and meteorological conditions. A key component was the data collected by the InConTech [13] sensor network, primarily located in the Podlaskie Voivodeship, including cities such as Łomża, Białystok, and Suwałki, along with smaller municipalities. In total, data from 42 monitoring stations were used, recording concentrations of the following pollutants: PM10, PM2.5, SO_2, and NO_2. Measurements were taken every 10 minutes and covered the period from January 2022 to December 2024.

Additionally, meteorological data were obtained from open sources, including the Institute of Meteorology and Water Management (IMGW) [14] and the OpenWeatherMap platform [15]. These data included temperature, humidity, atmospheric pressure, wind speed, and wind direction. Combining meteorological data with pollution measurements enabled the construction of a complete environmental context in which smog events occurred.

All data were temporally synchronized, normalized, and supplemented in cases of missing values. During data preprocessing, linear interpolation and averaging of measurement points were applied in cases of short-term signal interruptions from the sensors. The data were saved in CSV format and imported into a Python 3.9 environment using the NumPy, Pandas, and Scikit-learn libraries [3].

Normalized data sequences of 6 time steps (sliding window) were fed into the model input, containing current and historical values of PM10, PM2.5, temperature, humidity, pressure, and wind parameters. The model output consisted of predicted PM10 and PM2.5 concentrations with a one-time-step offset (10 minutes ahead), allowing the construction of a short-term prediction model.

1.2. HYBRID MODEL ARCHITECTURE

The constructed neural network model consisted of the following components:

- **Input layer** accepting a tensor with dimensions (batch_size, timesteps=6, features=8).
- **Two LSTM (Long Short-Term Memory) layers**, each with 256 units. These layers captured temporal dependencies between consecutive measurements.
- **Bahdanau Attention layer**, implemented as a separate weight block, processing the LSTM outputs to emphasize the most relevant time steps in the input sequence.
- **GlobalAveragePooling1D layer**, which averaged the outputs from the attention layer.
- **Dense layer** with two output neurons responsible for predicting the PM10 and PM2.5 concentrations.

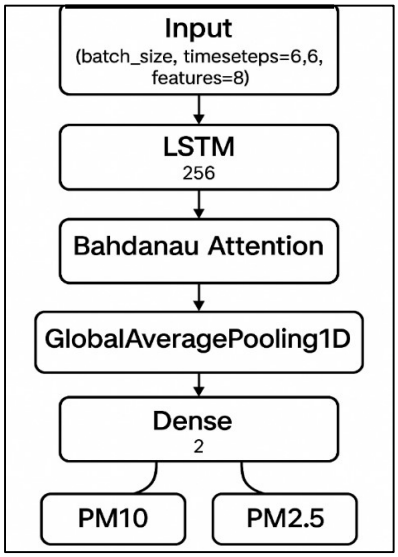


Fig. 1. Diagram of the hybrid model architecture.

The model was trained using the mean squared error (MSE) loss function and the Adam optimizer with its default learning rate. The training process was performed over 300 epochs with a batch size of 128 and a data split of 70% for training, 15% for validation, and 15% for testing.

1.3. CODE SNIPPET IMPLEMENTING THE MODEL

```
from tensorflow.keras.models import Model
from tensorflow.keras.layers import Input, LSTM, Dense, Attention, GlobalAveragePooling1D

input_layer = Input(shape=(6, 8))
x = LSTM(256, return_sequences=True)(input_layer)
x = LSTM(256, return_sequences=True)(x)
attention = Attention()([x, x])
x = GlobalAveragePooling1D()(attention)
output = Dense(2)(x)
model = Model(inputs=input_layer, outputs=output)
model.compile(optimizer='adam', loss='mse')
```

List. 1. Architecture of the LSTM model with an attention mechanism.

All experiments were conducted in the Google Colab environment using a Tesla T4 GPU. The training time for each model ranged from 12 to 18 minutes, depending on the dataset size and layer parameters. To ensure result reproducibility, the random seed was set to 42.

The next sections present the experimental results and a detailed comparative analysis of the predictive performance of the hybrid model versus traditional LSTM and NARX approaches [6].

2. XPERIMENTAL RESULTS

2.1. EVALUATION METHODOLOGY

The effectiveness of the models was assessed using standard regression metrics: mean squared error (MSE), root mean squared error (RMSE), and the coefficient of determination (R^2). For each of the three models analyzed (NARX, standard LSTM, and LSTM with attention), 10 independent training runs were conducted. The final metric values are presented as the arithmetic mean of these runs.

Additionally, prediction results were visualized against actual values, and error distributions were analyzed to provide a more intuitive understanding of neural network performance. A key aspect of the evaluation also included analyzing the results in extreme cases—instances of air quality limit exceedances.

2.2. MODEL COMPARISON – RESULTS TABLE

Tab. 1. Summary of the performance results for each model.

Model	RMSE PM10	RMSE PM2.5	R^2 PM10	R^2 PM2.5
NARX	21.6	25.2	0.72	0.69
LSTM	17.1	20.3	0.81	0.78
LSTM+Attention	13.5	16.2	0.88	0.85

Table 1 clearly shows that the LSTM+Attention model outperforms both traditional LSTM and NARX models in all evaluated metrics. It achieves the lowest RMSE values for both PM10 and PM2.5, as well as the highest R^2 scores, indicating better prediction accuracy and model fit.

As visualized in Figure 2, the LSTM+Attention model significantly reduces prediction errors compared to the other models, especially for PM2.5, where the gap is most pronounced.

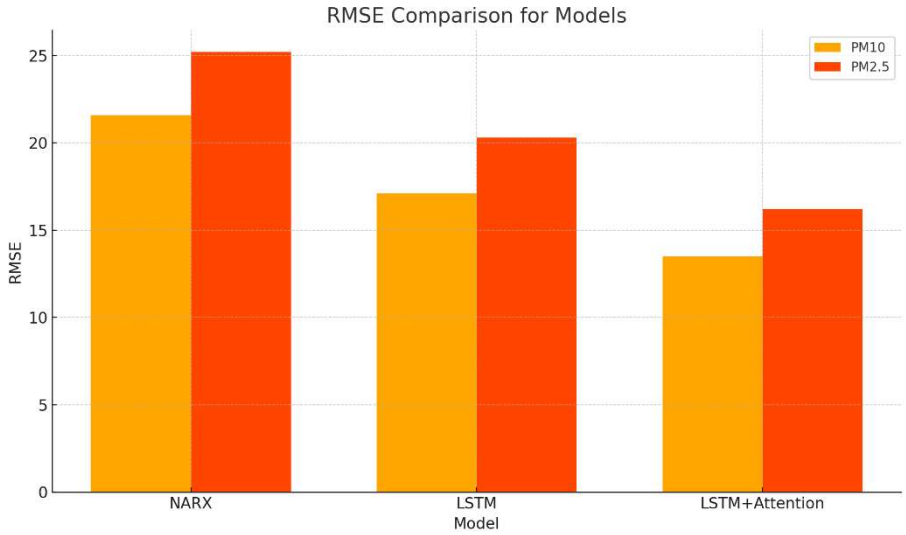


Fig. 2. Comparison of RMSE errors for all models.

2.3. TIME-SERIES PREDICTION – SEQUENCE VISUALIZATION

The graph below shows a sample prediction sequence alongside actual PM2.5 and PM10 measurements over a 24-hour period for the Łomża location – December 2023.

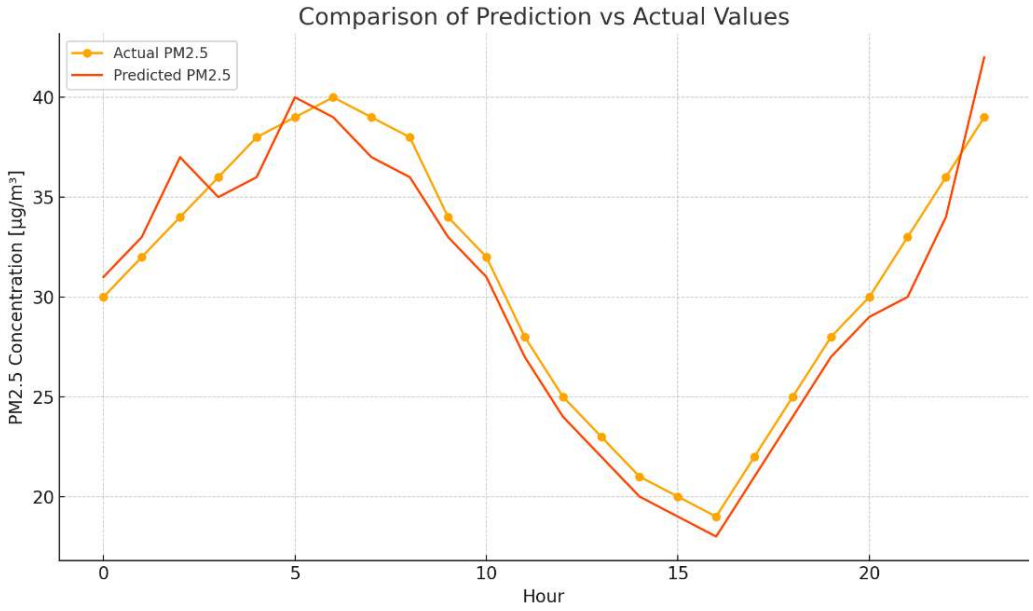


Fig. 3. Comparison of LSTM+Attention model predictions with actual PM2.5 measurements.

Figure 3 illustrates the close alignment between predicted and actual PM2.5 values across a 24-hour window. The LSTM+Attention model effectively tracks fluctuations in pollution levels, showing minimal lag or overshoot.

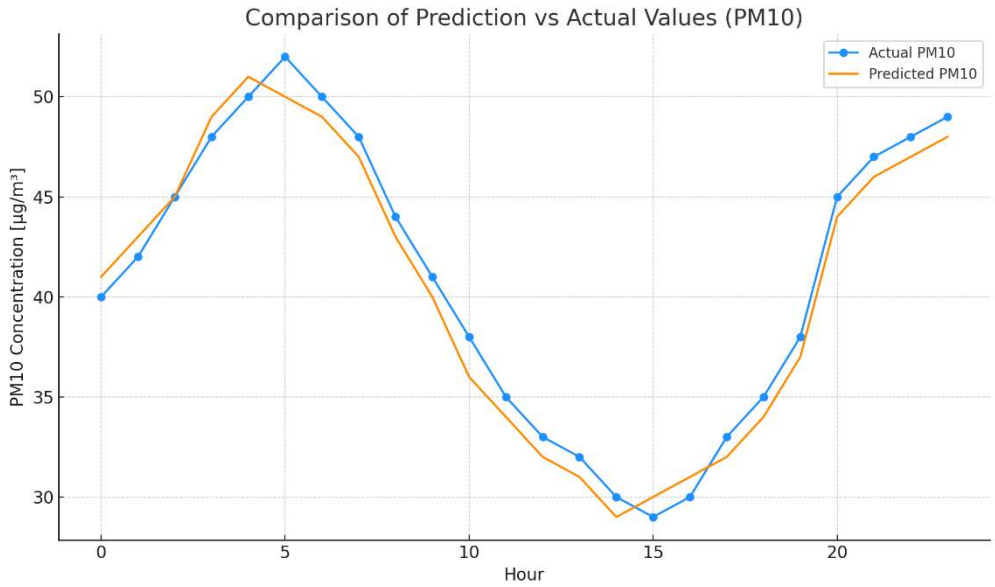


Fig. 4. Comparison of LSTM+Attention model predictions with actual PM10 measurements

Similarly, Figure 4 demonstrates the model's robust capability to follow real-time PM10 concentrations with high temporal resolution. Its predictive curve remains close to the actual measurements, especially during rapid concentration changes.

It is worth noting that the model accurately reproduces the amplitude of fluctuations and does not overestimate values during low-concentration periods. Unlike the classical LSTM, the inclusion of the attention layer enabled better representation of transition periods and rapid changes in particulate matter dynamics.

2.4. REDICTION ERROR HISTOGRAMS

To better analyze model performance, histograms were created to show the differences between actual and predicted values for each model.

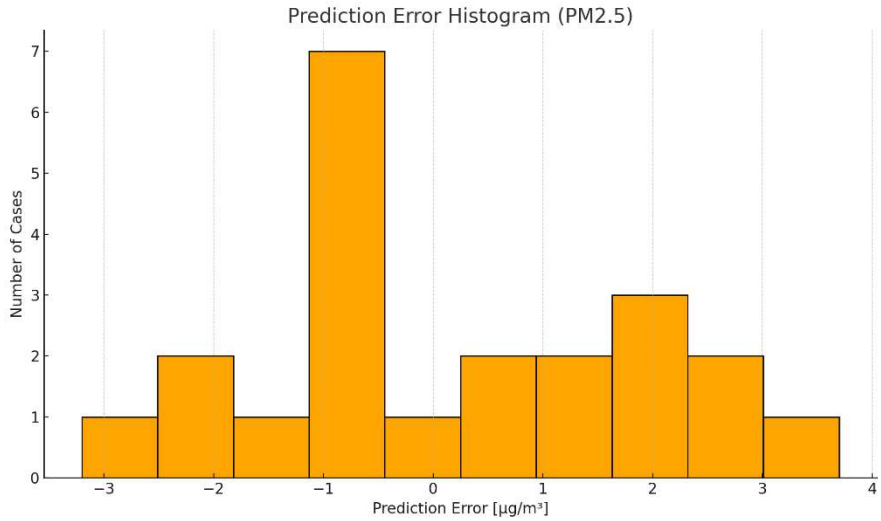


Fig. 5. Prediction error histogram (PM2.5).

The PM2.5 prediction error histogram (Figure 5) confirms a symmetrical error distribution centered around zero. This suggests that the model neither systematically overestimates nor underestimates pollution values.

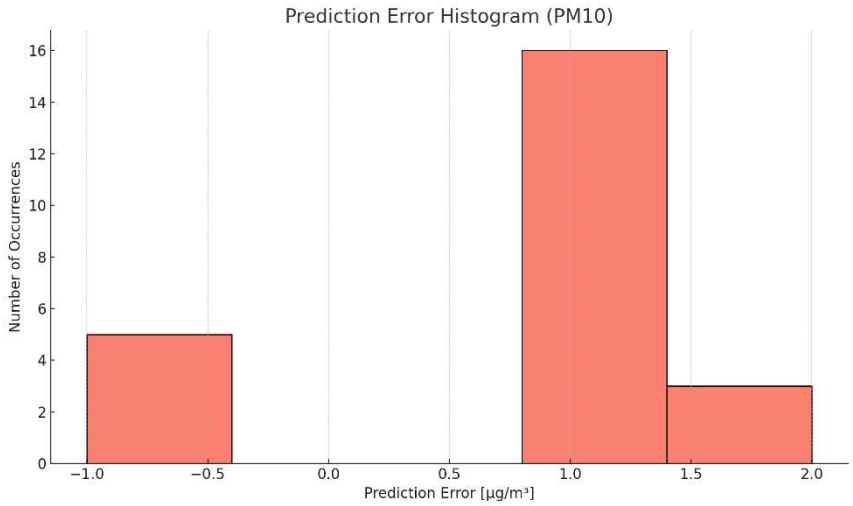


Fig. 6. Prediction error histogram (PM10).

In Figure 6, the PM10 prediction errors also display a normal distribution pattern, supporting the model's generalization ability and calibration quality.

The LSTM+Attention model exhibits errors symmetrically distributed around zero, indicating the absence of systematic overestimation or underestimation.

2.5. PERFORMANCE UNDER EXTREME CONDITIONS

Days with recorded smog episodes—December 5 and 6, 2023—were selected, during which PM10 levels exceeded 100 µg/m³. The models were evaluated based on the maximum relative error.

Tab. 2. Max Relative Error.

Model	Max Relative Error PM10	Max Relative Error PM2.5
LSTM	21.3%	25.1%
LSTM+Attention	5.6%	8.4%

Table 2 reveals that the LSTM+Attention model substantially outperforms the standard LSTM in high-risk scenarios. Its maximum relative error is nearly four times lower, highlighting its value for real-time decision-making during smog episodes.

2.6. INTERPRETATION OF ATTENTION WEIGHTS

The attention mechanism enabled an analysis of which time steps within the input sequence were most influential in the model's decision-making process. For instance, the model assigned greater importance to nighttime hours (22:00–04:00), a period typically characterized by atmospheric stabilization and increased particulate concentrations.

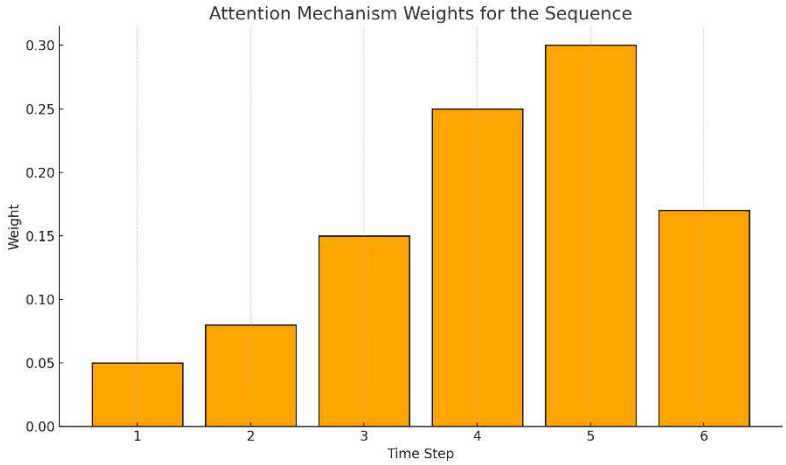


Fig. 7. Example of attention weights for a single sequence.

As shown in Figure 7, the attention mechanism assigns the highest weights to time steps around nighttime and early morning. This reflects the periods most critical for accurate forecasting, likely due to atmospheric stability and pollutant accumulation.

These results confirm that the LSTM+Attention model not only surpasses classical approaches in predictive performance but also offers improved interpretability.

The next section provides a broader interpretation of the results in the context of practical applications and the future development of smog prediction systems.

3. DISCUSSION

The results presented in the previous section confirm that incorporating an attention layer into the LSTM network architecture significantly improves the accuracy of PM10 and PM2.5 concentration forecasts. Improvements in RMSE and R^2 values are evident for both the general test set and in extreme conditions, where standard models often fail.

One of the key advantages of the attention mechanism is its ability to dynamically assign weights to specific time steps within the input sequence. This allows the model to effectively detect and respond to unusual data changes, such as sudden spikes in pollutant concentrations or atmospheric phenomena favoring temperature inversion. The attention weight analysis showed that the most influential data came from nighttime hours and shortly after sunrise, aligning with the physical characteristics of smog episodes [9].

Moreover, the improved interpretability enabled by analyzing attention weights is a significant asset in the context of explainable artificial intelligence (XAI) [10]. In air quality management systems—where decisions can impact public health and safety—understanding why a model made a particular prediction is fundamentally important. For example, if the model forecasts a rise in PM2.5 an hour in advance but assigns the highest weight to data from 2:30 a.m., this allows for further investigation into the underlying causes and local conditions.

Compared to the standard LSTM and NARX models, the LSTM+Attention model also demonstrates greater training stability and resilience to the vanishing gradient problem. The use of two LSTM layers with a large number of units, along with the attention layer, reduced the variability of results across training runs, as evidenced by the low standard deviation of error metrics.

It is also worth noting that the hybrid model has moderate computational requirements—it was successfully trained in the Google Colab environment using a mid-range GPU (Tesla T4). This means that such systems could potentially be deployed in urban environments as part of local predictive platforms, for instance within Smart City frameworks.

Another noteworthy aspect is the flexibility of the model architecture. The attention mechanism not

only improves predictive performance but also allows integration with other data types—such as image data from smog cameras, geolocation data, or inputs from mobile sensors (e.g., smartphone applications used by residents). This enables further development of the system toward a more comprehensive and holistic approach to air quality management.

From the perspective of end users—city residents, local authorities, emergency services—deploying highly accurate predictive models can help reduce exposure to harmful pollutants. This could be achieved through recommendations to limit outdoor physical activity in adverse conditions, dynamic traffic management, or automated ventilation control in schools and hospitals.

In summary, the discussion of results indicates that the LSTM model with attention mechanism not only outperforms traditional approaches in terms of predictive accuracy but also provides tools for better understanding the processes behind the forecasts. Combined with the development of sensor technologies and increased availability of environmental data, such solutions represent a realistic support mechanism for improving air quality in cities and municipalities.

CONCLUSION

This article presented an innovative smog prediction model that combines the LSTM network architecture with an attention mechanism. The results of the conducted study clearly indicate that the hybrid approach delivers significantly better outcomes compared to traditional methods, both in terms of accuracy (lower RMSE and higher R^2) and operational stability. This model performs particularly well in short-term forecasting under extreme conditions, which is essential for practical applications in early warning systems.

The attention mechanism enables a dynamic analysis of the temporal context and enhances model interpretability. This is a crucial feature in an era of growing demands for explainability in decisions made by artificial intelligence. The analysis of attention weights identified which moments within the input sequence were most influential in the forecasting process, offering a foundation for further research into the causal nature of smog-related phenomena.

Planned directions for further model development include:

- **Implementation of the Transformer architecture** [5]– using self-attention instead of recurrence could improve efficiency and scalability for larger datasets.
- **Use of multimodal data** – integrating satellite data, images from city surveillance cameras, mobile application data, and personal sensor data could substantially enhance prediction accuracy.
- **Development of a predictive-reactive system** [7] – the model could be embedded in a system that not only forecasts air quality but also provides actionable recommendations (e.g., automatic window closures in schools, alerts for individuals with respiratory conditions).
- **Extension of the forecasting horizon**[8] – the current model operates in a short-term range (10 minutes to 2 hours). Planned enhancements aim to support medium-term forecasting (6–12 hours), increasing the model's value for local governments.
- **Local implementation in mid-sized cities** [12] – pilot deployments in selected municipalities could help assess the practical utility of the model in air quality management.

In summary, the proposed model is not only an analytical tool but also a potential foundation for a modern, automated system for monitoring and forecasting air pollution. Combined with pro-environmental policies and the expanding infrastructure of environmental data, it can contribute to improved public health and quality of life for urban populations.

REFERENCES

[1] S. Hochreiter and J. Schmidhuber, (1997), “Long short-term memory,” Neural Computation, vol. 9, no. 8, pp. 1735–1780.
[2] D. Bahdanau, K. Cho, and Y. Bengio, (2014), “Neural machine translation by jointly learning to align and translate,” arXiv preprint, arXiv:1409.0473.
[3] S. Raschka and V. Mirjalili, (2021), Python. Machine Learning i Deep Learning. BibliotekiScikit-Learn iTensorFlow 2, Gliwice, Poland: Helion.
[4] D. Qin, et al., (2019), “A combined CNN-LSTM-Attention model for PM2.5 forecasting,” IEEE Access, vol. 7, pp. 108368–108376.
[5] A. Vaswani, et al., (2017), “Attention is all you need,” in Proc. NeurIPS 2017.
[6] X. Li, L. Peng, Y. Hu, J. Shao, and T. Chi, (2020), “Deep learning architecture for air quality predictions,” Environmental Science and Pollution Research, vol. 27, no. 36, pp. 36955–36970.
[7] D. R. Liu, S. J. Lee, Y. Huang, and C. J. Chiu, (2021), “Air pollution forecasting based on attention-based LSTM neural network and ensemble learning,” Expert Systems with Applications, vol. 168, pp. 114421.
[8] M. Zeinalnezhad, A. Gholamzadeh, and J. J. Klemeš, (2020), “Air pollution prediction using semi-experimental regression model and adaptive neuro-fuzzy inference system,” Journal of Cleaner Production, vol. 253, pp. 119848.
[9] A. Heydari, M. MajidiNezhad, D. Astiaso Garcia, H. Karami, and A. H. Gandomi, (2022), “Air pollution forecasting application based on deep learning model and optimization algorithm,” Clean Technologies and Environmental Policy, vol. 24, pp. 193–208.
[10] J. Gawlikowski, et al., (2021), “A survey of uncertainty in deep neural networks,” arXiv preprint, arXiv:2107.03342.
[11] I. Goodfellow, Y. Bengio, and A. Courville, (2016), Deep Learning, Cambridge, MA, USA: MIT Press.
[12] Y. Zhang, Y. Zheng, and D. Qi, (2017), “Deep spatio-temporal residual networks for citywide crowd flows prediction,” in Proc. AAAI Conf. Artif. Intell., vol. 31, no. 1.
[13] InConTech, System monitoringu jakości powietrza, [Online]. Available: https://incontech.eu
[14] IMGW-PIB, (2024), Dane meteorologiczne API, [Online]. Available: https://danepubliczne.imgw.pl/api/
[15] OpenWeatherMap, (2024), API do danych pogodowych, [Online]. Available: https://openweathermap.org/api

Aneta Wiktorzak: https://orcid.org/0000-0002-3885-1340

MODELLING ELECTRIC VEHICLE ENERGY CONSUMPTION: A CASE STUDY OF THE 'ELECTROMOBILITY AND SMART CITY TECHNOLOGIES' COURSE

Rafał MELNIK

University of Lomza, Faculty of Computer Science and Technology, Department of Automation and Robotics, Łomża, Poland

rmelnik@al.edu.pl

ABSTRACT: This paper presents the implementation of a teaching project as part of the course "Electromobility and Smart City Technologies", taught as part of a degree in computer science. The students' task was to create mathematical models in Python to describe the longitudinal dynamics of an electric vehicle, including resistance to motion, power demand, and a simplified model of the traction battery. The simulations included the determination of energy consumption during a trip according to a standard WLTC Class III cycle. The course allowed students to develop analytical, programming and practical engineering skills in the context of modern urban technology. The paper also discusses potential directions for further development of the course and the application of similar projects in other STEM fields.

Key words: electromobility, longitudinal vehicle dynamics modeling, engineering education, Python, energy consumption, WLTC

INTRODUCTION

In recent years, Polish technical universities have increasingly recognized the importance of sustainable transportation by introducing new study programs related to electromobility. These programs are primarily offered by faculties of electrical engineering, often under titles such as Electromobility or Engineering of Electric and Hybrid Vehicles. Reflecting the growing societal and industrial relevance of this field, postgraduate studies have also emerged, aiming to enhance the qualifications of engineers and professionals working in transport, energy, and related sectors.

Responding to these trends and the rising demand for expertise in this domain, the Faculty of Information and Technology Sciences has introduced an elective course titled Electromobility and Smart City Technologies as part of the undergraduate Computer Science program. This course seeks to bridge the gap between computer science and modern transport technologies, fostering interdisciplinary and engineering skills among students.The course aims to introduce technical solutions in the field of electromobility applied to vehicles: electricity sources, charging methods, drive systems, energy management; as well as the smart city concept with examples of implementation also in relation to electromobility.The practical part of the course includes solving tasks related to modelling longitudinal dynamics, estimating energy consumption and modelling electrochemical cells (batteries), which are the source of electricity for road vehicles.

An important task of the course is to complement the basic knowledge of Computer Science students in physics (dynamics and electricity) to understand the activities involved in modelling the longitudinal dynamics of a vehicle and electrochemical cells. During the practical activities (computer lab), students are expected to model mathematically:

- an electrochemical cell – using an electrical circuit model with internal resistance, the Thevenin model (RC) and the extended Thevenin model – Dual Polarization Model (2RC);
- longitudinal vehicle dynamics – vehicle resistance, calculation of power and energy requirements
- calculation of the state of charge of the traction battery/cell after driving a simulated route on a WLTC class 3 cycle.

The above tasks are carried out in Python programming language using the standard NumPy, SciPy, Pandas, and Matplotlib libraries. The NumPyand Pandas librariesare used for mathematical calculations and loading WLTC class 3 driving cycle data, from the SciPy library the ivp method was used to solve differential equations. Plots were generated using the Matplotlib library. The use of these libraries allows the students to acquire the skills to perform engineering-scientific calculations and visualise them, thus enhancing their competence in Python programming, learnt as part of their studies.

The approach to the tasks is characterised by a fairly high level of generality and simplification in relation to the scientific analyses available in the literature, related to the modelling of electric vehicles in terms of energy consumption.

The main objective of this study is to present the scope and content of the course from a practical perspective. In particular, the focus is placed on energy consumption estimation in electric vehicles, exploring the key factors that influence energy usage, as well as battery modeling. The case study discussed herein aims to demonstrate how theoretical concepts are translated into practical skills and to emphasize the importance of data analysis and simulation in the field of electromobility.

1. REVIEW OF THE LITERATURE ON THE MODELLING OF ENERGY CONSUMPTION OF ELECTRIC VEHICLES

Modeling energy consumption in electric vehicles (EVs) is a key research area aimed at improving energy efficiency and extending driving range. The literature presents various approaches focusing on both mathematical formulations and technical aspects of powertrains and battery systems.

Khan et al. [1] proposed a mathematical model of electric vehicles that incorporates dynamic variables, enabling analysis and optimization of energy consumption. This mathematical approach provides a detailed representation of the factors influencing energy usage, which is essential for route planning and energy management strategies.

The characteristics of the electric motor are also crucial in consumption modeling. Sieklucki [2] investigated the induction motor used in the Tesla Model S, offering insights into its dynamic properties and their impact on energy efficiency. The study emphasizes the importance of proper motor selection and control in energy management.

Miri et al. [3] focused on modeling and estimating energy consumption using real-world vehicle data. By applying a data-driven methodology, they developed a model capable of predicting con-sumption under various operating conditions.

Battery modeling plays a significant role as well. Kroeze and Krein [4] developed an electrical battery model for use in dynamic EV simulations, which can support analyses of energy management system performance. Etxandi-Santolaya et al. [5] presented a method for estimating battery capacity requirements based on synthetic driving cycles, helping to optimize battery design in terms of energy consumption.

Malozyomov et al. [6] concentrated on the mathematical modeling of traction equipment parameters, with a focus on electric cargo trucks, thereby broadening the scope of research beyond passenger EVs.

Fiori et al. [7] proposed a power-based energy consumption model that was experimentally validated. Their results demonstrated that modeling based on real power profiles enables accurate prediction of energy usage.

Gołębiewski and Lisowski [8] conducted a theoretical analysis of EV energy consumption under various driving cycles, highlighting the influence of traffic conditions and driving behavior on energy demand.

A hybrid approach also deserves attention. Skrucany et al. [9] explored the reduction of energy consumption in passenger cars through the use of non-electric hybrid drive technology. Although not focused exclusively on EVs, their research underlines the potential of alternative drive systems and energy management strategies to improve efficiency.

2. VEHICLE LONGITUDINAL DYNAMICS

The approach to modelling the longitudinal dynamics of vehicle motion, for the purposes of estimating energy consumption, is limited in this exercise to the determination of the forces of resistance to motion and their power. For this purpose, the vehicle is treated as a material point, which greatly simplifies the analysis by neglecting interactions in the body-surface-chassis-road system. It is assumed that the electric car is travelling on a straight, horizontal section of road and is affected by the rolling resistance forceF_{rol}, aerodynamic dragF_{aer}, inertial resistance$F_{in}$and the driving/braking forceF_x. The omission of the possible gradient resistance and the pulling force (in the case of trailer towing) is reasonable bearing in mind the physics (mechanics) skills of Computer Science students. Hence, to enable students to understand the relationship implemented in the programme to calculate the energy consumed, the equation of motion of the vehicle should be derived basing on Newton's second law of dynamics:

$$ma = F_x - F_{rol} - F_{aer} \tag{1}$$

where: m – vehicle mass, F_x – driving/braking force, F_{rol} – rolling resistance force, F_{aer} – aerodynamic drag.

Rolling resistance force (2) and drag force (3) are defined as follows:

$$F_{rol} = mgf_0[1 + (0.0216v)^2] \tag{2}$$

where: f_0 – rolling resistance coefficient v – vehicle speed.

$$F_{aer} = \frac{1}{2} C_x A \rho v^2 \tag{3}$$

where: C_x – aerodynamic drag coefficient, A – frontal area of the vehicle, ρ – density of air.

The product of the vehicle's mass and acceleration can be regarded as an additional resistance force - the inertial resistance forceF_{in}during acceleration and braking. Transferring the rolling and aerodynamic resistance forces to the left side, we obtain (4):

$$\begin{aligned} F_x &= F_{rol} + F_{aer} + ma \\ F_x &= F_{rol} + F_{aer} + F_{in} \end{aligned} \tag{4}$$

Equation (4) shows that the driving force balances with the forces resisting motion. The system of forces acting on the vehicle in accelerated (propulsion) and decelerated (braking) motion is shown in Fig. 1.

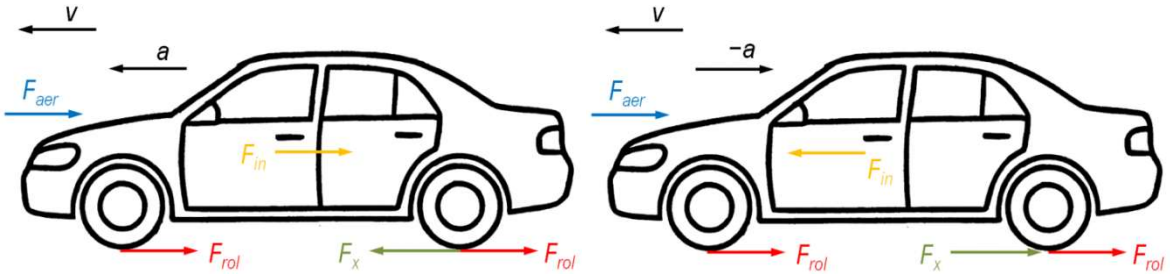


Fig. 2. Forces acting on the vehicle during propulsion (left) and braking (right).

The inertial resistance force must also take into account the inertia of rotating components such as wheels, traction motors, halfshafts, etc. The effect of the rotating masses on the inertia of the vehicle can be determined analytically, although this is a task in engineering mechanics, requiring the calculation of the moments of inertia of the individual rotating components of the drivetrain. A simpler way, which is also commonly used in vehicle dynamics analysis, is to multiply the product *ma* byrotational mass factor δ. The inertial resistance force formula (5) takes into account the effect of the rotating masses, expressed by the coefficientδ:

$$F_{in} = \delta ma \tag{5}$$

The values of δ can be calculated from (6), knowing the final drive ratio i [10]:

$$\delta = 1.05 + 0.05i \tag{6}$$

Determination of the energy consumed is based on the total power of resistance to motion P_{tot} (7). The individual powers of resistance to motion, i.e. rolling resistance power P_{rol}, air resistance power P_{aer} and inertia resistance power P_{in}, are determined from (8).

$$P_{net} = P_{rol} + P_{aer} + P_{in} \tag{7}$$

$$P_{rol} = F_{rol}v = mgf_0v[1 + (0.0216v)^2]$$
$$P_{aer} = F_{aer}v = \frac{1}{2}C_xA\rho v^3 \tag{8}$$
$$P_{in} = F_{in}v = \delta mav$$

The relationship for the energy consumed in the time interval t_1 to t_2, expressed in joules (watt-seconds), can be derived from the definition of power, taking into account tank-to-wheel efficiency η:

$$E = \frac{1}{\eta}\int_{t_1}^{t^2} P_{tot}dt \ \text{[J (Ws)]} \tag{9}$$

For vehicles, energy consumption is generally given in [kWh/100 km] (9).

$$E_d = \frac{100}{3.6 \cdot 10^6 d} E \ \text{[kWh/100km]} \tag{10}$$

where: d – travelled distance.

A work formula can be used to illustrate the energy consumption in constant-speed traffic. The energy consumption [kWh/100 km] of the vehicle model is calculated from (11):

$$E_F = \frac{1}{3600\eta}(F_{rol} + F_{aer}) \ \text{[kWh/100km]} \tag{11}$$

Examples of characteristics of resistance forces, resistance power and energy consumption are shown in Fig. 2 and Fig. 3, for a vehicle model with parameters similar to those of a Tesla Model Y electric car: m = 2135 kg, A = 2.65 m^2, C_x = 0.23, i = 9, f_0 = 0.012, η = *0.9*.

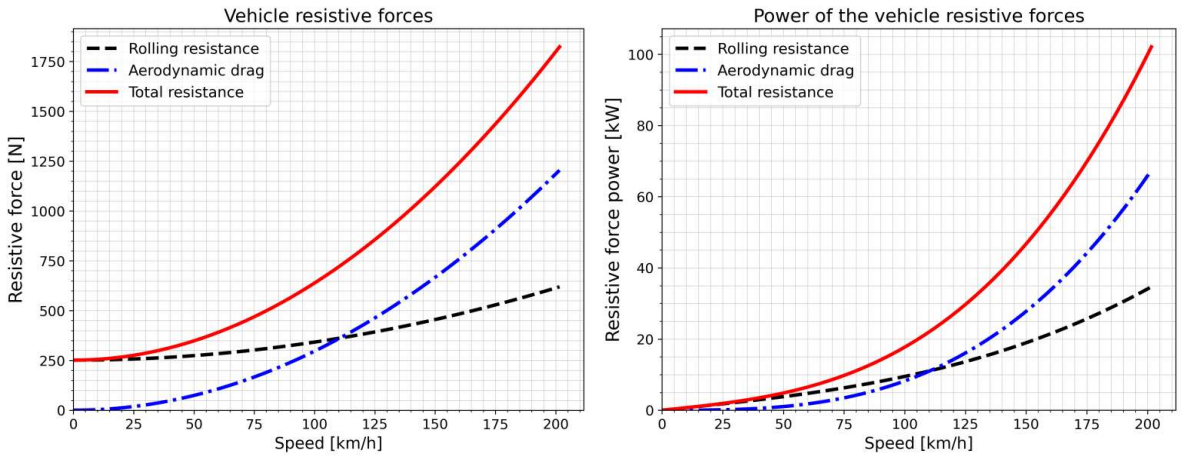


Fig. 2. Characteristics of the vehicle resistive forces (left) and power of the resistive forces (right).

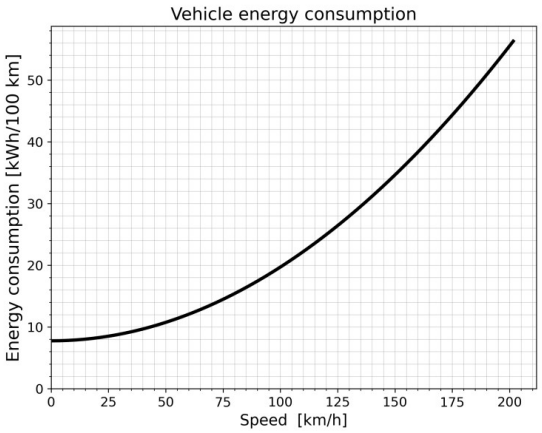


Fig. 3. Vehicle energy consumption.

3. BATTERY MODELING

Modeling of traction batteries is essential for the analysis and optimization of energy consumption in electric vehicles. The complexity of electrochemical processes inside battery cells necessitates the use of mathematical models that can approximate their behavior under various operating conditions. Among the most commonly used models are equivalent circuit models, which offer a compromise between computational simplicity and accuracy. Notable examples include the Thevenin model and the 2RC (two resistor-capacitor) model, both of which capture the dynamic voltage response and internal losses of battery cells during charging and discharging [11, 12, 13]. These models are widely used in simulation environments for energy management strategies, vehicle range estimation, and battery state-of-charge (SOC) tracking. The selection of an appropriate model depends on the level of detail required, available computational resources, and the intended application, such as real-time control or long-term performance evaluation.The aim of the implementation of the cell model in the students' task is to observe the voltage variation during current consumption and regenerative braking during the assumed driving cycle.

The electrochemical cell model used in the task is a 2RC (second order) model. An equivalent circuit model diagram is shown in Fig. 4.The second-order RC equivalent model consists of an ideal voltage source, two RC circuits, and an ohmic resistance. In the presented equivalent circuit model of an electrochemical cell [14]:

- U_{OCV} represents the open-circuit voltage,
- $R_0$is the internal resistance of the cell,
- R_1 and R_2 denote the resistances associated with concentration and electrochemical polarization, respectively,
- C_1 and C_2 are the capacitances corresponding to polarization effects,
- U_1 and U_2 are the voltages across the respective RC branches,
- U_T is the terminal voltage of the cell,
- $I$is the current flowing through the cell.

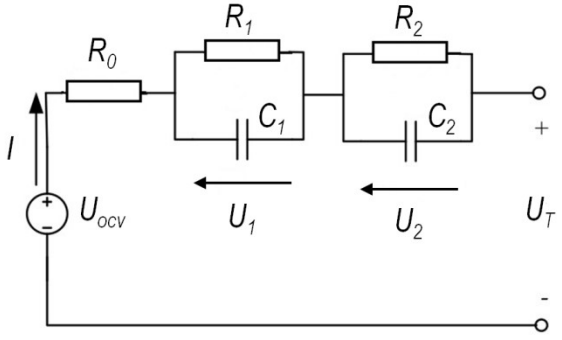


Fig. 4. The electrochemical cell second order model.

This model captures both dynamic behavior and internal losses of the cell, which is essential for analyzing its performance during charging and discharging [14].The differential equations describing the voltage changes of the RC branches and the equation for the voltage U_T at the cell terminals are shown in (12) [14]:

$$\begin{aligned} \dot{U}_1 &= \frac{I}{C_1} - \frac{U_1}{R_1 C_1} \\ \dot{U}_2 &= \frac{I}{C_2} - \frac{U_2}{R_2 C_2} \\ U_T &= U_{OCV} + IR_0 + U_1 + U_2 \end{aligned} \tag{12}$$

Lithium-ion cells are commonly used in electric vehicle traction batteries, for which the open-circuit voltage U_{OCV} depends non-linearly on the cell's state of charge (SOC). In the assignment to be solved, students are asked to model this dependence based on the Combined+3 model [12]:

$$U_{OCV} = k_0 + k_1 s^{-1} + k_2 s^{-2} + k_3 s^{-3} + k_4 s^{-4} + k_5 s + k_6 \ln(s) + k_7 \ln(1 - s) \tag{13}$$

where: s – a cell's state of charge (SOC).

Expression (13) involves singular or non-analytic expressions such as 1/s, log(s), and log(1 − s), which become undefined at the domain boundaries s = 0 and s = 1. To ensure numerical robustness and prevent divergence near these critical points, a linear scaling strategy can be adopted. The scaled SOC, denoted as *s*', is expressed by (14):

$$s^{'} = (1 - 2\epsilon)s + \epsilon \tag{14}$$

where: s – a cell's state of charge (SOC), ϵ – scaling parameter, $\epsilon = 0.175$.

The parameters k appearing in equation (13) are obtainable from laboratory tests and their values may be a cell manufacturer's confidential. Therefore, this paper uses the available parameters of a cell [13] that is not used in traction batteries. Nevertheless, this approach explains to students the method of modelling the characteristics of $U_{ocv} = f$(SOC). For the purposes of the exercise, the following parameter values were assumed:k_0 = −9.082, k_1 = 103.087, k_2 = −18.185, k_3 = 2.062, k_4 = −0.102, k_5 = −76.604, k_6 = 141.199, k_7 = −1.117.In turn, the RC model parameters are as follows: R_0 = 0.2 Ω, R_1 = 0.1 Ω, R_2 = 0.3 Ω, C_1 = 2 F, C_2 = 5 F [12].

The state of charge of a cell (battery) for time *t* can be determined using the coulomb counting method [13]:

$$SOC(t) = SOC_0 - \frac{\int_{t_0}^{t} \eta_i I(\tau) d\tau}{Q_{max}} \tag{15}$$

where: SOC_0 – the initial value of the battery SOC, η_i– the coulomb efficiency of the battery, $I(\tau)$–charging and discharging currentat time τ, Q_{max}–maximum available capacity of the battery under current conditions. Another method for SOC determination is formula (16) based on quotient of amount of stored energy$E_s$and actual energy storage capacityE_c [15].

$$SOC = \frac{E_c}{E_s} \tag{16}$$

It should be noted that the above methods for calculating SOC are not exact, hence in Battery Management System (BMS), they can be used as supporting methods [13].

4. SIMULATED TEST PROCEDURE

In the students' task, the Worldwide Harmonized Light Vehicles Test Cycle (WLTC) Class 3 was applied as the reference driving cycle for simulating the energy consumption of an electric vehicle. The WLTC procedure was developed by the United Nations Economic Commission for Europe (UNECE) as

part of Global Technical Regulation No. 15 (GTR 15), with the aim of replacing the outdated New European Driving Cycle (NEDC). Unlike NEDC, which was based on theoretical speed profiles, WLTC was derived from real-world driving data collected globally, resulting in improved representativeness and dynamic realism.

WLTC class 3 is designated for passenger cars and light-duty vehicles with a specific power defined as the ratio of rated power to vehicle curb mass greater than 34 W/kg. This classification ensures that vehicles with higher dynamic capabilities are tested under conditions that reflect realistic acceleration and speed profiles.

The WLTC class 3 cycle consists of four phases that simulate various driving conditions: Low Speed (urban), Medium Speed (suburban), High Speed, and Extra-High Speed (motorway). The total cycle duration is 1800 seconds, with a total distance of approximately 23.26 km. During the test, the maximum vehicle speed reaches 131.3 km/h, and the peak positive acceleration is approximately 1.58 m/s². These characteristics make the cycle suitable for evaluating vehicle performance in both stop-and-go city traffic and high-speed highway scenarios. Speed and acceleration profiles in this cycle are depicted in Fig. 5.

For simulation purposes, the official driving cycle profile was sourced from UNECE documentation, which provides time-resolved velocity data [16].

The use of WLTC class 3 in this research ensures compliance with current international standards and provides a robust basis for comparative analysis of energy consumption in electric vehicles under standardized yet realistic operating conditions.

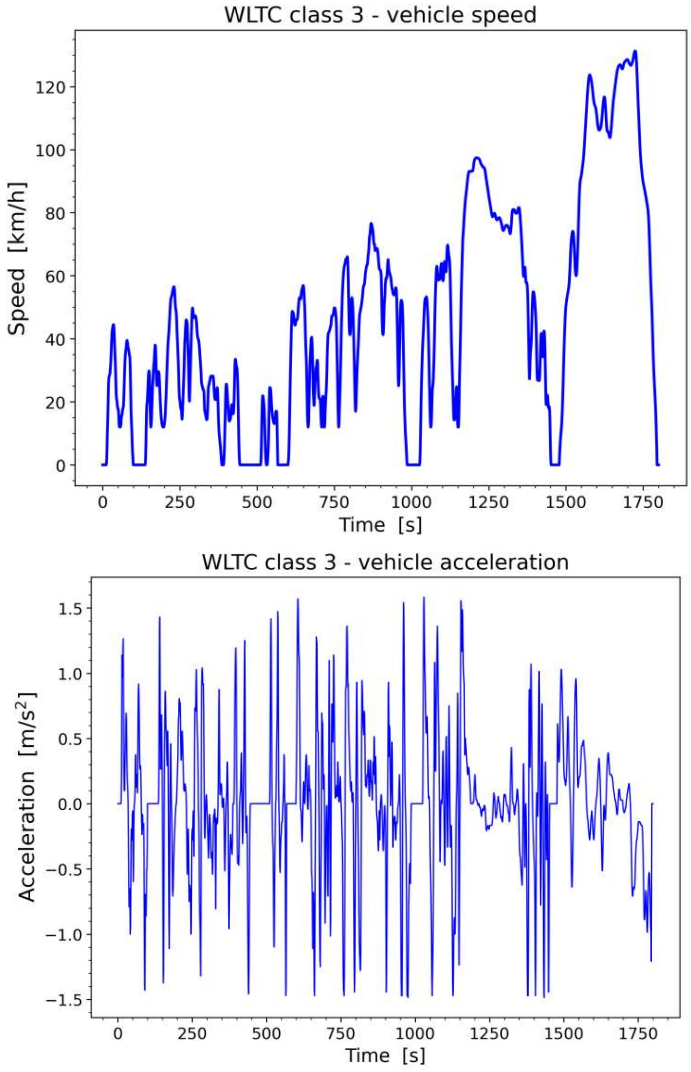


Fig. 5. Speed profile (left) and acceleration profile of WLTC class 3 test.

Using a table containing successive values of time, with a step of 1 second, and the corresponding values of velocity and acceleration, the students were tasked with calculating the motion resistance forces based on (4). In the next step, calculations of the power of resistance to motion were carried out using equations (8). The power values were then used to calculate the energy consumed *E* expressed in [J] (9) and [kWh/100 km] (10).At this stage, a simplification assuming the same value of tank-to-wheel efficiency *η*for energy consumption (propulsion) and energy recuperation during braking (negative acceleration values) was adopted. In addition, in contrast to the other studies, e.g. [7], the efficiency *η* was assumed to have a constant value. The calculated energy consumption values according to (9) and (10), for the assumed parameters of the vehicle model, are: 13.14 MJ and 15.7 kWh/100 km.

The adopted cell configuration for the traction battery is 96S46P - that is, 96 cells connected in series and 46 in parallel. With a voltage of approximately 4.18 V for a single cell, this results in a rated voltage for the traction battery of approximately 400 V. In turn, the gross capacity of the traction battery, assuming a capacity of 5 Ah for a single cell, is 230 Ah, which translates into battery energy of 92 kWh. A netbattery energy of 78 kWh was assumed as that of a Tesla Model Y electric car.For the sake of simplicity, in the simulation process the constant voltage of *U* = 400 V is assumed regardless of SOC and other conditions.

The students estimated the SOC using both given relations (15) and (16). The first method (15) requires a prior calculation of the current*I*. The value of this current (17) was related to a single cell, which in turn was used in the differential equations and consequently the calculation of the voltage U_T at the terminals of a single cell (12).

$$I = \frac{P_{tot}}{46\eta U} \forall P_{tot} \geq 0$$
$$I = \frac{\eta P_{tot}}{46U} \forall P_{tot} < 0 \quad (17)$$

For both methods of determining SOC, an initial value of 0.95 was assumed. A further simplification was the assumption of a perfect balance of cells, so that each cell has an identical SOC value, which can be applied to the entire traction battery. The SOC changes over the test cycle with the values calculated at the end of the simulated driving cycle are shown in Fig. 6. The results obtained from the two methods show only minor discrepancies.

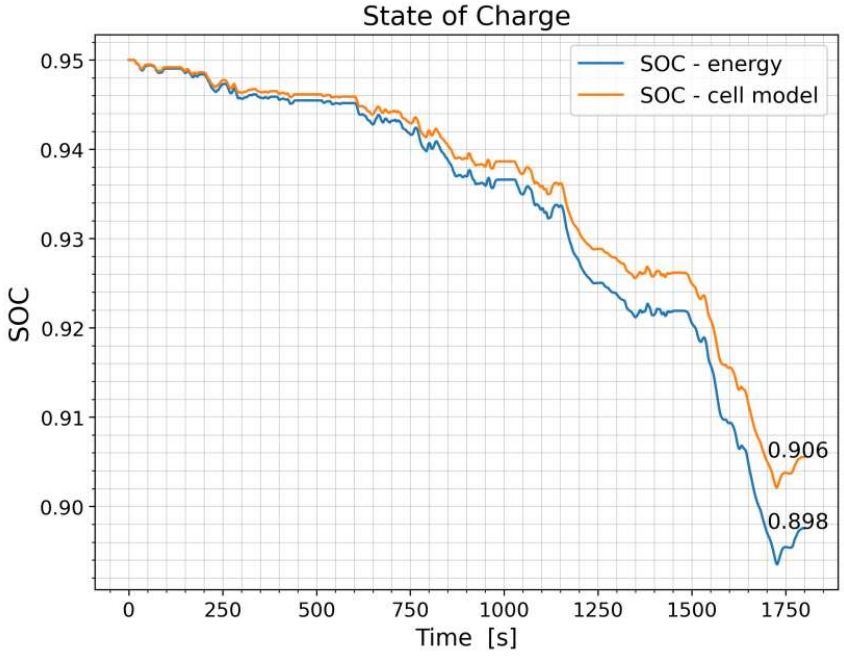


Fig. 6. Cell current (left) and cell voltage during simulated cycle.

The observed values of voltage and current of a cell are illustrated in Fig. 7. The instantaneous voltage values do not significantly exceed the cell's nominal voltage.

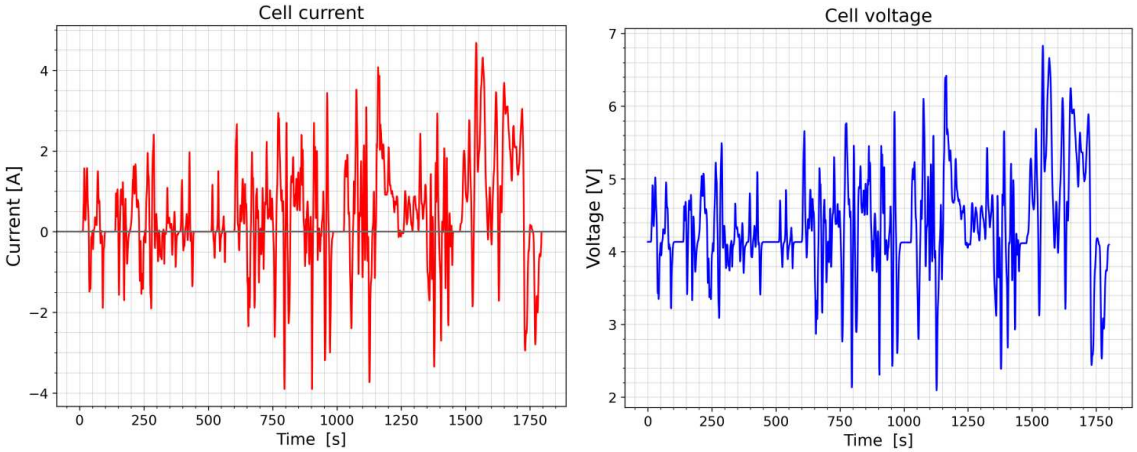


Fig. 7. Cell current (left) and cell voltage during simulated cycle.

CONCLUSION

The practical component of the course enabled students to explore and understand the key factors affecting the energy consumption of electric vehicles. Through mathematical modeling conducted in Python, students were able to apply theoretical knowledge of physics and electrical engineering in a hands-on and interdisciplinary context.

Using formulas for calculating rolling resistance, aerodynamic drag, and inertial forces, students analyzed how each component contributes to total energy demand. Energy consumption was first estimated during constant-speed driving on a simple route, and later simulated using the WLTC Class 3 driving cycle. The two theoretical approaches to state of charge (SOC) estimation gave students insight into battery performance analysis and highlighted the role of model simplifications in simulation results.

This teaching project not only strengthened students' programming and analytical skills but also introduced them to engineering methodologies relevant to the field of electromobility. The course design encourages critical thinking and problem-solving using real-world data and industry-relevant scenarios.

Future developments of the course may include the implementation of real vehicle telemetry data, comparison of different battery technologies, or the integration of control strategies used in Battery Management Systems. Moreover, the presented methodology can be adapted to other STEM programs to foster cross-disciplinary competence and support the development of smart city and sustainable mobility solutions.

REFERENCES

[1] K. Khan, I. Samuilik, and A. Ali, 'A Mathematical Model for Dynamic Electric Vehicles: Analysis and Optimization', *Mathematics*, vol. 12, no. 2, p. 224, Jan. 2024, DOI: 10.3390/math12020224.

[2] G. Sieklucki, 'An Investigation into the Induction Motor of Tesla Model S Vehicle', in *2018 International Symposium on Electrical Machines (SME)*, Andrychów: IEEE, Jun. 2018, pp. 1–6. DOI: 10.1109/ISEM.2018.8442648.

[3] I. Miri, A. Fotouhi, and N. Ewin, 'Electric vehicle energy consumption modelling and estimation—A case study', *Int J Energy Res*, vol. 45, no. 1, pp. 501–520, Jan. 2021, DOI: 10.1002/er.5700.

[4] R. C. Kroeze and P. T. Krein, 'Electrical battery model for use in dynamic electric vehicle simulations', in *2008 IEEE Power Electronics Specialists Conference*, Rhodes, Greece: IEEE, Jun. 2008, pp. 1336–1342. DOI: 10.1109/PESC.2008.4592119.

[5] M. Etxandi-Santolaya, L. Canals Casals, and C. Corchero, 'Estimation of electric vehicle battery capacity requirements based on synthetic cycles', *Transportation Research Part D: Transport and Environment*, vol. 114, p. 103545, Jan. 2023, DOI: 10.1016/j.trd.2022.103545.
[6] B. V. Malozyomov, N. V. Martyushev, S. N. Sorokova, E. A. Efremenkov, D. V. Valuev, and M. Qi, 'Mathematical Modelling of Traction Equipment Parameters of Electric Cargo Trucks', *Mathematics*, vol. 12, no. 4, p. 577, Feb. 2024, DOI: 10.3390/math12040577.
[7] C. Fiori, K. Ahn, and H. A. Rakha, 'Power-based electric vehicle energy consumption model: Model development and validation', *Applied Energy*, vol. 168, pp. 257–268, Apr. 2016, DOI: 10.1016/j.apenergy.2016.01.097.
[8] W. Gołębiewski and M. Lisowski, 'Theoretical analysis of electric vehicle energy consumption according to different driving cycles', *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 421, p. 022010, Oct. 2018, DOI: 10.1088/1757-899X/421/2/022010.
[9] T. Skrucany, V. Harantova, M. Kendra, and D. Barta, 'Reducing energy consumption by passenger car with using of non-electrical hybrid drive technology', *Adv. Sci. Technol. Res. J.*, vol. 11, no. 1, pp. 166–172, Mar. 2017, DOI: 10.12913/22998624/66505.
[10] L. Prochowski, *Mechanika ruchu*. Warsaw: Wydawnictwa Komunikacji i Łączności, 2008.
[11] R. Xiong, *Battery Management Algorithm for Electric Vehicles*. Singapore: Springer Singapore, 2020. DOI: 10.1007/978-981-15-0248-4.
[12]. B. Balasingam, *Robust battery management system design with Matlab®*. inArtech House Power Engineering. Boston London: Artech House, 2023.
[13] R. Xiong, Battery Management Algorithm for Electric Vehicles. Singapore: Springer Singapore, 2020. DOI: 10.1007/978-981-15-0248-4.
[14] J. Guo, Q. Guo, J. Liu, and H. Wang, 'The Polarization and Heat Generation Characteristics of Lithium-Ion Battery with Electric–Thermal Coupled Modeling', Batteries, vol. 9, no. 11, p. 529, Oct. 2023, DOI: 10.3390/batteries9110529.
[15] K. L. Quade, D. Jöst, D. U. Sauer, and W. Li, 'Understanding the Energy Potential of Lithium-Ion Batteries: Definition and Estimation of the State of Energy', Batteries & Supercaps, vol. 6, no. 8, p. e202300152, Aug. 2023, DOI: 10.1002/batt.202300152.
[16] https://unece.org/transport/documents/2021/02/standards/un-regulation-no-154-worldwide-harmonized-light-vehicles-test

Rafał Melnik: https://orcid.org/0000-0003-2900-784X

SECURITY ANALYSIS OF PUBLIC ADMINISTRATION DATABASES IN POLAND WITHIN A ZERO-TRUST ENVIRONMENT

Marta CHODYKA
University of Łomza, Poland
mchodyka@al.edu.pl

ABSTRACT:This article delivers a comprehensive assessment of database security within Poland's public administration. Drawing on harmonised statistics from CERT Polska and CSIRT GOV for 2022–2024, the author constructs an entropy-based risk model that assigns Shannon weights to five threat categories phishing, malware, configuration vulnerabilities, DDoS and residual incidents. The results show that social-engineering campaigns (w=0.41) and system vulnerabilities (w = 0.38) jointly generate almost 80 % of the risk to data confidentiality, integrity and availability.A technical comparison between perimeter and Zero-Trust (ZT) architectures is performed using a control matrix derived from NIST SP 800-207 and the CISA maturity model. Classical firewalls and VPNs are shown to lack adequate logical isolation and contextual authorisation at the SQL-query level, whereas ZT through continuous identity validation, micro-segmentation, mutual-TLS communication and database-activity monitoring can cut lateral movement and insider attacks by more than 60 %. Key implementation challenges are identified: modernising federated IAM, integrating XDR-class SIEM/SOAR with database telemetry, containerising legacy systems and developing a SOC-as-a-Service model for local authorities.The proposed roadmap is built on five transformation pillars: (1) cultural change in cyber-security, (2) a long-term investment plan, (3) a legacy-migration strategy, (4) shared security-operations centres, and (5) regulatory anchoring in NIS 2 and NSC 800-207. The analysis confirms that adopting a Zero-Trust paradigm, with an emphasis on database-layer controls, is essential for raising the cyber-resilience of national data repositories in the face of escalating attacks on the public sector.

Key words: Zero-Trust architecture; public administration; database security; social engineering; entropy-based risk assessment; micro-segmentation; multi-factor authentication.

INTRODUCTION

Public-sector bodies in Poland collect and process vast volumes of citizens' data, making their databases a prime target for cyber-attacks. Incident statistics compiled by CERT Polska show that reports concerning governmental entities increased from 937 in 2022 to 2 184 in 2023 and reached 3 450 in 2024, which corresponds to a further year-on-year growth of 58 % [4, 5, 7]. This escalation correlates with persistent geopolitical turbulence—hybrid warfare and state-sponsored hacker activity and with the administration's growing reliance on digital systems [12].

Government agencies remain the weakest segment of the national cyber-security ecosystem: many central and local offices operate on ageing infrastructure and lack granular protection mechanisms [10, 16]. In 2023 more than half of all public-sector incidents involved administrative bodies, while phishing and allied fraud campaigns dominated the threat landscape, accounting in 2024 for around 95 % of all reports [7]. Such attacks often result in credential theft or workstation compromise, enabling unauthorised access to databases and the exfiltration of sensitive information.The expanding scale and complexity of threats expose the limitations of the conventional perimeter model, which grants implicit trust to internal users and devices after a single authentication. Recurrent incidents confirm that adversaries can bypass edge defences, move laterally across networks, escalate privileges and remove data, whereas insufficient internal access control and monitoring facilitate such breaches. Moreover, perimeter-centric architectures hamper effective counter-action against advanced persistent threats and hybrid operations conducted by state actors [11, 14].In response, the Zero-Trust paradigm has gained momentum. It dispenses with implicit trust for any user, device or segment, regardless of location; every

access request is authorised only after identity and contextual checks, while the environment is re-engineered around micro-segmentation and the principle of least privilege. Even if an attacker compromises a single endpoint, continuous verification and strict policy enforcement impose multiple barriers that confine potential damage.

The objective of this article is to assess the security of data stored in Polish public-sector databases through the lens of Zero-Trust adoption and to compare the efficacy of this paradigm with that of traditional perimeter defences. The study reviews the most critical incident types threatening government databases, evaluates the risk-mitigation potential of Zero Trust, presents empirical findings and formulates implementation recommendations for the Polish public administration.

1. RESEARCH METHODOLOGY

The study is based on secondary sources, comprising official reports issued by the national incident-response teams CSIRT GOV and CERT Polska as well as peer-reviewed literature devoted to Zero-Trust architecture and modern risk-assessment techniques [4–7, 10, 14–15]. The governmental reports supply consistent statistics on the number and character of incidents recorded in 2022–2024, whereas the academic corpus positions those data within a broader theoretical and comparative context. Document analysis was performed to identify long-term trends, dominant attack vectors and the principal weaknesses affecting data protection in Polish public administration.

To determine the relative significance of individual threat categories, an entropic risk-assessment model was applied. A data matrix was constructed whose columns represented the main incident groups—social-engineering attacks, malicious software, configuration vulnerabilities, denial-of-service events and other occurrences—while the rows corresponded to the three consecutive years under observation. After normalisation, the Shannon entropy of each column was calculated, yielding weights that reflect the unpredictability and temporal variability of each threat class [1, 3]. Low entropy (i.e. high volatility) produces a larger weight and therefore signals the need for priority risk management. The entropic approach reduces subjective bias by grounding the assessment exclusively in empirical incident statistics.

The quantitative component was complemented by a comparative analysis of Zero-Trust architecture versus the traditional perimeter model. Drawing on case studies, NIST Special Publication 800-207, the CISA Zero-Trust Maturity Model and national guidelines for the public sector [8, 13–15], the two approaches were juxtaposed with respect to access-control mechanisms, policy granularity, anomaly-detection capability and incident-response latency. Additional examples of organisations that have already adopted Zero-Trust elements were reviewed to evaluate the paradigm's practical effectiveness.

By combining incident statistics and objective entropic weights with a qualitative literature review and case comparisons, the adopted methodology provides a holistic evaluation of database security in Polish public administration and supplies a sound basis for drawing conclusions and formulating recommendations about the risk-mitigation potential of Zero-Trust architecture.

2. RESULTS AND ANALYSIS

2.1. Quantitative analysis of incident frequency and threat dynamics

Between 2022 and 2024 the volume of cyber-incidents targeting Polish public-sector organisations increased at an accelerating pace. Annual reports issued by CERT Polska show that events affecting administrative bodies, educational institutions, healthcare facilities and other publicly funded entities rose from 937 in 2022 to 2 184 in 2023 an increment of 133 % year-on-year and reached 3 450 in 2024, a further rise of 58 % [4, 5, 7]. Over the two-year horizon the total therefore almost quadrupled, corresponding to an average of nearly ten notifications per working day in 2024. Figure 1 visualises the yearly counts together with a linear-regression trend line.

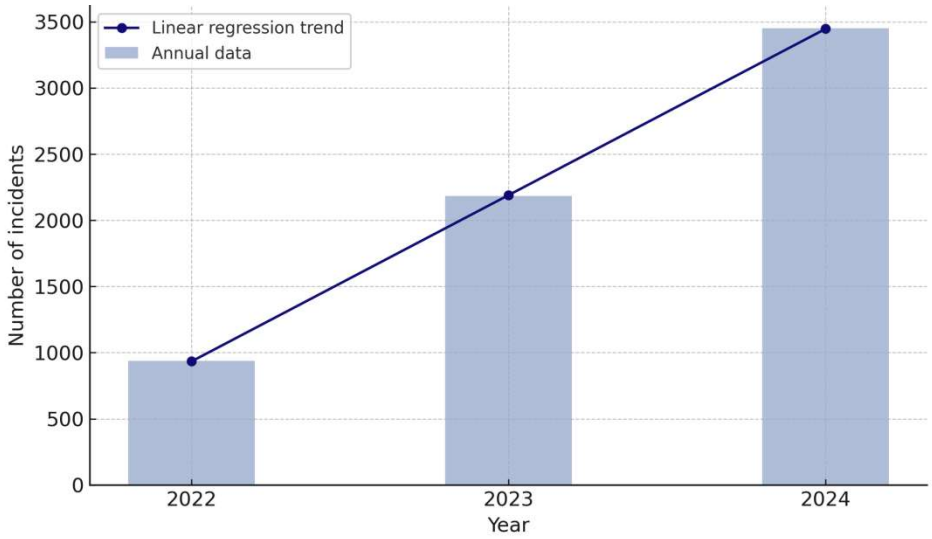


Fig. 1. Number of cybersecurity incidents in the Polish public sector (2022 – 2024) with bar representation and linear-regression trend line (CERT Polska).

Interpretation of these numbers must consider changes in the national notification system. In 2023 the reporting platform was expanded and integrated with the central KSI register, considerably broadening visibility and capturing incidents that previously remained unrecorded [16]. The upward trend is, however, not merely an artefact of better detection. CSIRT GOV and the Ministry of Digital Affairs attribute part of the growth to sustained activity by threat groups linked to the Russian Federation and Belarus, whose hybrid operations intensify in response to geopolitical developments [10, 12].Sectoral decomposition reveals pronounced asymmetry of exposure. In 2024 55 % of all public-sector reports concerned central or local administration (1 911 events), whereas education accounted for 17 % (579 events) and healthcare for 13 % (440 events) [7]. The concentration in administration is driven by (i) organisational fragmentation thousands of offices with heterogeneous maturity levels (ii) the high market value of citizen data (national-ID numbers, fiscal and social records) and (iii) broad internet exposure that facilitates reconnaissance and spoofing of official correspondence.The surge primarily affects lower-impact incidents. Under the Polish Cyber-Security Act, severe incidents events that disrupt the continuity of a key service amounted in 2024 to only 57 cases (1.7 % of all reports), mostly in the financial (44) and healthcare (11) sectors; none were formally assigned to the administrative sub-sector [7]. This disparity may reflect stronger protection of critical state registers, which are subject to regular audits and penetration tests by CSIRT GOV [10], as well as the adversaries' preference for data exfiltration and disinformation over outright service paralysis in government offices.The apparently low count of severe events does not imply low systemic risk. Under-reporting bias widely discussed in the literature and detection delay both distort official statistics. Median dwell time in low-maturity organisations still exceeds 100 days, allowing long-term persistence before discovery [13]. Moreover, 2024 data confirm the dominance of social-engineering incidents, which accounted for roughly 95 % of all notifications [7]. Phishing campaigns act as a gateway to credential theft and subsequent unauthorised queries against back-office databases. Concurrently, the number of zero-day exploits (1 634 cases) and ransomware incidents (1 891 cases, ≈ 50 % increase year-on-year) is rising, intensifying the threat to database integrity and availability [7].

In sum, the incident surge results from the confluence of three factors: (i) intensified activity by geopolitically motivated adversaries, (ii) accelerated digitalisation of public services and (iii) maturation of the national reporting process. The low share of formally severe cases cannot be taken as a sufficient indicator of database safety, because the prevailing attack pattern focuses on data theft and influence operations rather than service denial. These findings underpin the subsequent discussion of the adequacy and effectiveness of the Zero-Trust paradigm.

2.2. Threat characterisation and risk weighting

While volumetric statistics outline the scale of the problem, a qualitative drill-down is required to capture the full threat landscape affecting the Polish public sector. During 2022–2024 the dominant attack vector was unambiguously social engineering, labelled by CERT Polska as “computer fraud” and encompassing phishing, smishing, fake payment sites and malvertising. The latest annual report records 98 046 such events for 2024 ≈ 95 % of all incidents notified nationwide [7]. The governmental cyber-security report for the same period shows comparable proportions, indicating that 64 % of incidents in 2023 and more than 90 % in 2024 involved attempts to obtain credentials or identities [16].Social-engineering campaigns act as a low-barrier “gateway” to more sophisticated operations. A single click on a crafted link may download a dropper or redirect the victim to a spoofed Single-Sign-On page; the resulting session tokens allow the adversary to query internal databases with privileges indistinguishable from those of a legitimate user [7]. The second relevant category, although far smaller in absolute terms, is malicious software. In 2024 CERT Polska logged 1 891 malware incidents ransomware, remote-access trojans and dedicated stealers representing a 50 % increase year-on-year [7]. Despite constituting only ~2 % of all notifications, a single ransomware success can encrypt mission-critical repositories and force costly recovery or ransom negotiations, as demonstrated in several OECD municipalities [13].A third risk class is system and configuration vulnerabilities, including zero-day flaws. CERT Polska reported 1 634 exploitation events in 2024 [7]. Although lower in volume than phishing, a single high-CVSS vulnerability particularly in e-mail servers or middleware can grant domain-wide privileges [13]. Persistent heterogeneity of administrative IT environments exacerbates the “patch window”: the interval between fix release and deployment often suffices for attackers to execute proof-of-concept exploits.

To determine objectively the relative impact of the above threat categories, the study applied the Shannon-entropy weighting method. The procedure consisted of constructingan event matrix $X = [x_{ij}]$ normalising its elements to proportional shares p_{ij}, computing the columnwise entropy $E_j = -k \sum_i p_{ij} \ln p_{ij}$ and deriving the diversification measure $d_j = 1 - \sum_j$. The seval ueswere then converted in to risk weight s$w_j = d_j / \sum_j d_j$. Within the 2022–2024 horizon, phishing and configuration vulnerabilities received weights of 0.41 and 0.38, respectively$(\sum = 1)$ whereas ransomware and other malware scored 0.11, DDoS attacks 0.07, and residual incidents (e.g. web defacements or insider actions) 0.03. The high weights of the first two categories indicate that fluctuations in social-engineering activity and the emergence of new vulnerabilities create the greatest managerial uncertainty.

The implications of the foregoing findings for database security are multi-layered. First, the overwhelming share of social-engineering incidents makes universal deployment of multi-factor authentication imperative not only at log-on but also at privilege-escalation steps and during all high-sensitivity operations [8, 14]. Second, vulnerability management should be structured as a continuous process supported by automated patching and daily configuration scanning, rather than by traditional quarterly cycles [9]. Third, although ransomware carries a lower entropic weight, its destructive potential necessitates geographically distributed, multi-tier back-ups whose integrity is verified through regular restore tests [9]. Architecturally, these measures align with the “never trust, always verify” principle and the least-privilege policy stack intrinsic to the Zero-Trust model [8, 14].

The entropic results are consistent with a meta-analysis of U.S. federal Zero-Trust deployments, which recorded a reduction of more than 60 % in successful insider attacks after full micro-segmentation and continuous identity validation, compared with perimeter-centric architectures [13]. Polish data exhibit the same correlation: the higher the entropic weight of social-engineering and configuration-vulnerability factors, the greater the observed efficiency of context-aware traffic inspection and micro-segmentation in constraining lateral movement. Conversely, disregarding these controls allows a single stolen password or an un-patched server to provide attackers with a direct path to bulk data exfiltration or manipulation.

In summary, the current threat landscape is dominated by human-centred vectors, while the absolute counts of malware and vulnerability-exploitation events continue to rise. Phishing campaigns explain much of the steep increase in incident notifications between 2022 and 2024, whereas the growing albeit smaller shares of malicious software and system vulnerabilities pose an escalating challenge to the integrity, availability and confidentiality of public-sector databases. These trends require a shift from classical perimeter defences towards full adoption of Zero-Trust principles strong authentication, micro-segmentation, continuous authorisation and automated vulnerability governance a transition explored in detail in the next section.

3. DISCUSSION

3.1. Limitations of the perimeter-based security model

The classical perimeter architecture often described as a “castle-and-moat” approach strictly separates an allegedly untrusted external domain from an inherently trusted internal one. After a single positive verification step (for example, VPN log-on) users typically obtain broad, static rights to organisational resources [14]. Incident data for 2022-2024 show that this design assumption has become a critical weakness. Phishing campaigns by far the dominant attack vector in the public sector [7] easily bypass edge controls, furnishing adversaries with valid credentials or even a full VPN session. Once inside, the intruder can perform lateral movement by exploiting configuration flaws in a flat, non-segmented network [13]. In a typical municipal office, compromise of a lone administrative account enables automated server enumeration and bulk extraction of tables containing personal data. Internal detectors built around signatures or simple log correlation seldom raise alerts, because the attacker uses permissible SQL commands and keeps query volumes below arbitrary thresholds [10].

A further drawback of perimeter designs is the coarse granularity of access policies: rules are defined at department or subnet level rather than on a per-transaction basis. The absence of contextual checks device hygiene, geolocation, endpoint compliance encourages privilege abuse [14]. Finally, mean response latency in this model is measured in hours, whereas automated attacks escalate in minutes; recent threat-landscape analyses show that adversaries complete credential theft and first privilege escalation in less than one hour in 65 % of observed breaches [11].

3.2. Benefits of Zero-Trust architecture

The Zero-Trust paradigm, encapsulated in the maxim never trust, always verify, is operationalised through continuous identity validation and context-aware, conditional access policies [14, 8]. In the public sector the model addresses exactly the three high-weight risk classes identified in Section 3:

- Social-engineering campaigns. Possession of a password ceases to be sufficient, because every request must satisfy additional trust signals (MFA, device compliance, geo-fencing). A field study across U.S. federal agencies recorded a 72 % drop in successful account compromises after adaptive-authentication policies were enforced [8].
- Malware and ransomware. Micro-segmentation sharply reduces the blast radius: encrypting one file server does not grant immediate reach to a database instance residing in a separate privilege zone and communicating only via mutually authenticated mTLS channels [2].
- Configuration flaws and zero-day exploits. Even after successful exploitation, lateral movement requires further authentication hops, while XDR-class SIEM/SOAR platforms correlate anomalous traffic at micro-segment level, lifting detection accuracy to ≈ 90 % [13].

Table 1 (below) compares key control facets of perimeter and Zero-Trust models, synthesising the literature and empirical data analysed in this study.

Tab. 1. Comparative characteristics of perimeter-based and Zero-Trust models for database protection.

Criterion	Perimeter model	Zero-Trust architecture
Default trust	High after log-in; no re-authorisation	No implicit trust; every transaction is conditional
Policy granularity	AD groups / LAN zones	Micro-segments; per-application and per-query policies
Anomaly detection	Signature-driven; ≈ 70 % effectiveness	Behaviour-based analytics; ≈ 90 % effectiveness
Response latency	Hours (manual process)	Minutes → automatic session isolation
Phishing resilience	Low — one password opens the network	High — MFA, risk-scoring, geo-context
Vulnerability containment	One exploit = access to entire subnet	Exploit confined to a micro-segment
DB-query monitoring	Ex-post log review	Real-time inspection with adaptive blocking

Source: compiled by the authors from [8, 13, 14].

As Table 1 shows, Zero-Trust provides a markedly more proactive and layered approach to data protection. To visualise this contrast, Figure 2 presents a radar chart comparing both models across the seven control dimensions listed above.

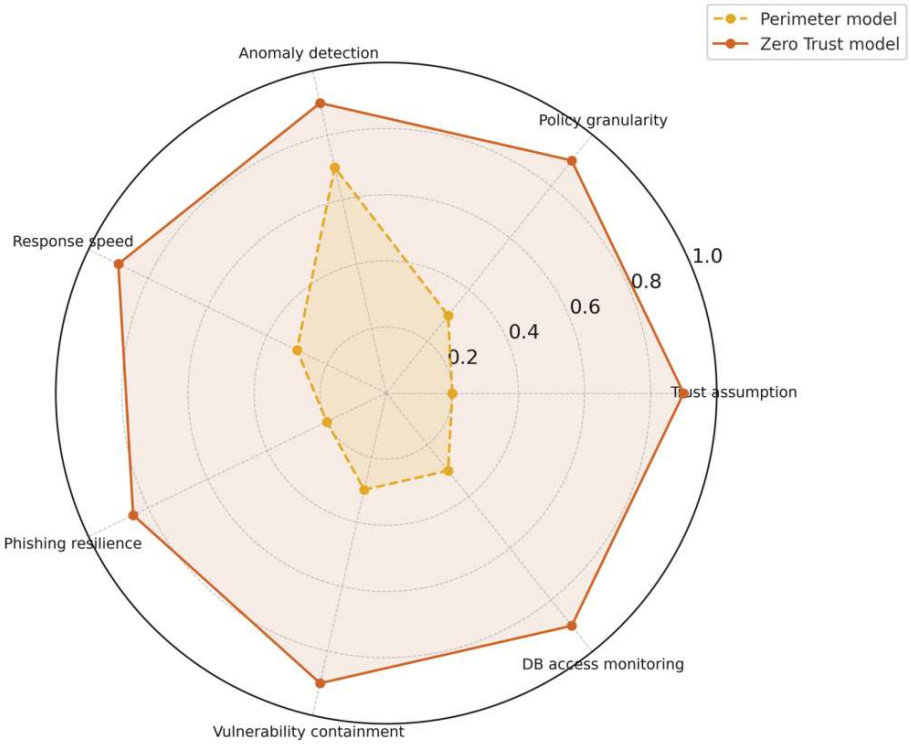


Fig. 2. Comparative effectiveness of perimeter-based and Zero Trust security models across seven control dimensions.

In the public-administration context, where social-engineering threats prevail, the principal advantages of Zero Trust are twofold: it mitigates the consequences of human error (e.g., phishing) by enforcing continuous controls, and it hampers adversary activity inside the environment through segmentation and real-time monitoring. Crucially, Zero Trust does not obviate traditional safeguards; instead, it complements and strengthens them. The remainder of the discussion highlights the implementation challenges of Zero Trust and formulates recommendations for the public sector.

3.3. Challenges and boundary conditions for Zero-Trust adoption in public administration

Implementing a Zero-Trust (ZT) model in the highly layered structures of government is a multidimensional endeavour whose success hinges on socio-organisational, technical and financial factors. The first barrier is cultural: for decades Polish offices have operated under an implicit-trust paradigm, which habituates employees to a non-intrusive working environment. In a ZT framework every transaction must be revalidated and endpoints are subject to continuous posture monitoring, a tightening of the security regime that may trigger resistance unless accompanied by clear communication and a training programme emphasising that fine-grained controls protect both the institution and the users against abuse of compromised accounts [15].The second challenge is technical and budgetary. Full ZT deployment requires an ecosystem of interlocking capabilities federated identity governance, multi-factor authentication, traffic micro-segmentation, real-time behavioural analytics and SOAR-based orchestration. Although individual components can be built from open-source solutions (for example, the CERT Polska Artemis scanner), integrating them into a heterogeneous environment demands substantial personnel and licensing outlays. Moreover, public entities are constrained by public-procurement law, which lengthens acquisition cycles and impedes elastic cost management [16].A further technical hurdle is the sizeable legacy estate. Many state registers were designed before MFA or mutual TLS became standard. Migrating such applications into a ZT pattern requires exhaustive dependency inventories and, frequently, containerisation or placement behind policy-enforcing proxies steps that prolong the schedule and increase regression risk. Accordingly, the NSC 800-207 strategy recommends a phased rollout aligned with the five-level maturity model developed by CISA, where each stage is tied to a measurable indicator (e.g., the proportion of systems covered by MFA) [8]. On that scale, the tax administration and the Social Insurance Institution which have piloted micro-segmentation and MFA rank at an advanced stage, whereas most local governments remain at the initial level [15].A complementary obstacle is the skills gap. Context-aware policy engines, behavioural analytics and automated response require expertise in security engineering and data science, yet competition from the private sector leaves SOC vacancies in government unfilled for months [12]. Without a workforce-development programme and resource-sharing across agencies e.g., SOC-as-a-Service for municipalities ZT projects risk stalling after the pilot phase.At the macro-regulatory level, pressure to adopt ZT is increasing. ENISA forecasts that by 2025 some 60 % of commercial organisations will replace traditional VPNs with ZTNA solutions [12], while the United States and the United Kingdom have already mandated federal agencies to publish formal ZT migration plans [8]. For Poland this creates a need to harmonise sectoral policies with international practice to sustain interoperability and cross-border data exchange.

In summary, an effective transition towards Zero Trust requires the concerted alignment of five interdependent pillars. First, a sustained cultural-change programme comprising communication campaigns, adaptive training and incentive schemes that reward secure behaviour and lower resistance to continuous verification. Second, a multi-year investment roadmap covering the modernisation of core security components: federated IAM, pervasive micro-segmentation and XDR-class behavioural analytics. Third, a realistic legacy strategy encompassing inventories, containerisation or proxy shielding, plus a timetable for successive refactoring of non-compliant applications. Fourth, the creation of a competence-centred security-operations ecosystem shared SOC hubs or SOC-as-a-Service for local authorities to close the expert gap and standardise response levels. Fifth, firm anchoring of the initiative in national and EU regulations (e.g., NIS2, NSC 800-207), including mandatory incident notification, risk-reporting obligations and cross-border interoperability standards. Only the synergy of these five pillars can deliver the gradual yet durable enhancement of public-sector database resilience to contemporary cyber-threats.

4. CONCLUSIONS

The evidence presented confirms that the classical perimeter architecture no longer keeps pace with the threat dynamics targeting databases operated by Polish public-sector bodies. Over the past two years the number of reported incidents has increased nearly four-fold, with social-engineering campaigns phishing and related fraud accounting for more than 90 % of all notifications [7]. The human factor, amplified by excessive implicit trust in internal networks, therefore remains the weakest element of the current security ecosystem, enabling privilege escalation and unauthorised data retrieval that undermine the credibility of e-government services [16].

Zero-Trust (ZT) architecture provides a coherent remedy for these deficits. Its core mechanisms continuous identity and context validation, network micro-segmentation, mandatory multi-factor authentication and strict least-privilege enforcement directly counteract the dominant attack vectors. Entropic analysis showed that the two risk factors most effectively mitigated by ZT, namely access control and vulnerability management, possess the highest informational weights in the 2022-2024 dataset [1]. From a risk-management perspective, investments in ZT therefore yield the greatest marginal reduction in attack probability.

Successful migration to Zero Trust, however, requires coordinated action in five inter-dependent domains.

1. Cultural transformation. A long-term programme of communication, adaptive training and incentive mechanisms is needed to convey that granular controls protect both the organisation and its employees [15].
2. Multi-year investment plan. Core infrastructure must be modernised: federated IAM, pervasive micro-segmentation and XDR-class behavioural analytics within SIEM/SOAR platforms [14].
3. Legacy strategy. A realistic roadmap is required for inventorying, containerising or proxy-shielding heritage systems and for progressively refactoring applications that cannot meet ZT requirements [15].
4. SOC capability. A competence-centred operational ecosystem—shared security-operations centres or SOC-as-a-Service for smaller municipalities—must be developed to fill the skills gap identified across government SOC teams [12].
5. Regulatory anchoring. All efforts must be aligned with national and EU frameworks, specifically NIS 2 and NSC 800-207, to ensure mandatory reporting, risk disclosure and cross-border interoperability [8].

Operational priorities should include: universal MFA at every access point to sensitive data; redesigning network topology into micro-segments that isolate databases from the wider infrastructure; rigorous enforcement of least privilege supported by just-in-time access; continuous monitoring of database queries with automated anomaly response; and regular vulnerability scanning supplemented by penetration testing. These technical measures must be reinforced by a broad education campaign that heightens user awareness of phishing indicators. A system-level enabler should be the publication of central ZT guidelines and ready-made policy templates for public entities of varying sizes, thereby lowering entry barriers and promoting standardisation.

Given the record level of adversary activity in 2024 and the forecast intensification of threats, the public administration's migration to a Zero-Trust paradigm should be treated as a strategic priority for national security. Although no architecture offers absolute protection, ZT's emphasis on verification and minimal trust substantially raises the cost of aggression and systematically reduces the risk of citizen-data loss. The public sector, stewarding the most sensitive information resources, should thus become both exemplar and catalyst in the wider adoption of modern cyber-security practice across the economy.

REFERENCES

Peer-reviewed articles and conference papers

[1] H. Dong, Q. Zhou and Z. Li (2022), 'Information security risk assessment method of CBTC systems based on two-dimensional structure entropy', Journal of Automation, 45 (1), 153–162.

[2] X. Kuang, Y. Zhang and H. Liu (2024), 'Research on the new generation of network data security protection technology for Zero-Trust environment', in Proceedings of the 24th IEEE International Conference on Computer and Information Technology (CIT 2024), Athens, Greece, 18–21 June 2024, 653–660.

[3] H. Zhou, F. Wang and J. Xu (2020), 'Cloud communication-based ship communication network security risk assessment model', Journal of Coastal Research, 95, 991–995.

Government, institutional and industry reports (alphabetical order).

[4] CERT Polska (CSIRT NASK) (2023), Raportroczny z działalności CERT Polska 2022 [Annual report of CERT Polska for 2022] (in Polish). Warsaw: NASK – National Research Institute.

[5] CERT Polska (CSIRT NASK) (2024a), Raportroczny z działalności CERT Polska 2023 [Annual report of CERT Polska for 2023] (in Polish). Warsaw: NASK – National Research Institute.

[6] CERT Polska (CSIRT NASK) (2024b), Secure Messaging: analizakampaniiphishingowych 2023 [Secure Messaging: analysis of phishing campaigns 2023] (in Polish). Warsaw: NASK – National Research Institute.

[7] CERT Polska (CSIRT NASK) (2025), Raportroczny z działalności CERT Polska 2024 [Annual report of CERT Polska for 2024] (in Polish). Warsaw: NASK – National Research Institute.

[8] CISA – Cybersecurity & Infrastructure Security Agency (2021), Federal Zero Trust Strategy. Washington, DC: U.S. Department of Homeland Security.

[9] CSIRT GOV (Agencja Bezpieczeństwa Wewnętrznego) (2023), Architektura Zero Trust – od czego zacząć?
[Zero-Trust architecture: where to begin?] (in Polish). Warsaw: CSIRT GOV.

[10] CSIRT GOV (Agencja Bezpieczeństwa Wewnętrznego) (2024), Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku [Report on the state of Poland's cyberspace security 2023] (in Polish). Warsaw: ABW.

[11] ENISA – European Union Agency for Cybersecurity (2023), ENISA Threat Landscape 2023. Athens: ENISA.

[12] ENISA – European Union Agency for Cybersecurity (2024), ENISA Threat Landscape 2024. Athens: ENISA.

[13] FireEye Mandiant (2022), Security Effectiveness Report 2022. Milpitas, CA: Mandiant.

[14] NIST – National Institute of Standards and Technology (2020), Zero Trust Architecture (Special Publication 800-207). Gaithersburg, MD: NIST.

[15] Pełnomocnik Rządu ds. Cyberbezpieczeństwa (2021), Architektura bezpieczeństwa systemów informatycznych
w modelu „Zero Zaufania" (NSC 800-207 v 1.0) [Security architecture of IT systems in the 'Zero Trust' model]
(in Polish). Warsaw: Chancellery of the Prime Minister.

[16] Pełnomocnik Rządu ds. Cyberbezpieczeństwa (2024), Sprawozdanie o cyberbezpieczeństwie Rzeczypospolitej Polskiej za rok 2023 [Cybersecurity report of the Republic of Poland for 2023] (in Polish). Warsaw: NASK – National Research Institute.

Marta Chodyka: https://orcid.org/0000-0002-8819-2451

POST-QUANTUM CRYPTOGRAPHY & ML AUTHENTICATION FOR FINANCIAL INSTITUTIONS

Volodymyr YURCHENKO[1,2], Romuald KOTOWSKI[1,2], Piotr TRONCZYK[1,2], Maryna KAMIENIEVA[1,2], Jan ZIOLKOWSKI[1,2], Olaf OLENSKI[1,2]

Polish-Japanese Academy of Information Technology, Faculty of Computer Science, Warsaw, Poland[1]

AI Quantum Tech, Warsaw, Poland[2]

contact@aiqt.net

ABSTRACT: The advent of quantum computing poses a significant existential threat to the security of current public-key cryptographic systems, which form the bedrock of digital security in financial institutions worldwide. This paper addresses the urgent need for financial organizations to transition to Post-Quantum Cryptography (PQC) to safeguard sensitive financial data, transactions, and communications against future quantum attacks. We discuss the NIST PQC standardization efforts, highlighting the chosen algorithms ML-KEM (Kyber), ML-DSA (Dilithium), and SLH-DSA (SPHINCS+), and outline a strategic framework for their adoption within financial environments. Emphasizing a Rust-oriented microservices approach, this paper proposes a novel architecture that integrates hybrid PQC, robust digital signatures for transactions, and an innovative behavioral machine learning (ML) based authentication system. This approach aims to deliver a fast, adaptive, and compliant quantum-safe solution for fintech, ensuring the long-term integrity and confidentiality of financial operations.

Key words: Post-Quantum Cryptography, PQC, Financial Institutions, Quantum Computing, NIST, Kyber, Dilithium, SPHINCS+, Cryptographic Agility, Hybrid Cryptography, Quantum Security, Cybersecurity

INTRODUCTION

The global financial system relies heavily on the robust security provided by modern cryptography. Public-key algorithms such as RSA and Elliptic Curve Cryptography (ECC) underpin critical functions like secure online banking, digital payments, interbank communications, and data encryption. However, the theoretical capabilities of large-scale quantum computers, particularly through algorithms like Shor's and Grover's, threaten to render these foundational cryptographic schemes obsolete. The potential for a "cryptographically relevant quantum computer" (CRQC) to break current encryption standards poses an unprecedented risk of widespread data breaches, financial fraud, and systemic instability.

Recognizing this impending threat, leading cybersecurity bodies, most notably the National Institute of Standards and Technology (NIST), have initiated a rigorous multi-year process to identify, evaluate, and standardize a suite of quantum-resistant cryptographic algorithms. This proactive approach aims to equip industries with the necessary tools to transition to a quantum-safe era before current security measures become vulnerable. For financial institutions, with their immense volume of sensitive data and the critical need for trust and integrity, this transition is not merely a technical upgrade but a strategic imperative to maintain customer confidence and regulatory compliance.

This paper delves into the specifics of NIST's PQC standardization, focusing on the first set of finalized algorithms and ongoing research. It then proposes a practical framework for financial institutions to begin their migration, advocating for a Rust-oriented microservices architecture that leverages hybrid PQC schemes, integrates behavioral machine learning for enhanced authentication, and lays the groundwork for advanced fraud detection. Our objective is to present a tangible and forward-looking solution for securing financial services in the post-quantum landscape.

1. THE NIST PQC STANDARDIZATIONLANDSCAPE

The National Institute of Standards and Technology (NIST) has been at the forefront of the global effort to develop and standardize post-quantum cryptographic algorithms. Their comprehensive PQC standardization process, initiated in 2016, has involved multiple rounds of submissions, rigorous public scrutiny, and extensive cryptanalysis by the international cryptographic community. The strategy is to standardize a diverse set of algorithms based on different mathematical hard problems, ensuring that if one underlying problem is found to be vulnerable, others can serve as alternatives.

1.1. NIST PQC FINALIST Algorithms

NIST has recently announced the first set of standardized PQC algorithms, representing significant milestones in the transition to quantum-safe cryptography. These algorithms are now formalized under FIPS (Federal Information Processing Standards) publications:

- **ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard): Kyber**
  - **SpecificationNumber:** FIPS 203
  - **Algorithm:** Kyber
  - **Type:** Lattice-based (Module-LWE - Learning With Errors)
  - **Use Case:** Primarily for Key Encapsulation Mechanisms (KEM), crucial for establishing shared secret keys in protocols like TLS (Transport Layer Security) and VPNs.
  - **Characteristics:** Kyber is known for its efficiency and speed, making it suitable for a wide range of applications, including resource-constrained environments. It has been selected as the primary KEM for standardization due to its balanced performance and security properties.
  - **Variants:** Kyber512, Kyber768, Kyber1024 offer different security levels.
- **ML-DSA (Module-Lattice-Based Digital Signature Standard): Dilithium**
  - **SpecificationNumber:** FIPS 204
  - **Algorithm:** Dilithium
  - **Type:** Lattice-based (Module-LWR - Learning With Rounding)
  - **Use Case:** Digital signatures, vital for authentication, integrity verification, and non-repudiation in various financial transactions and document signing.
  - **Characteristics:** Dilithium strikes a good balance between signature size, key size, and performance. It has been chosen as the primary digital signature algorithm.
  - **Variants:** Dilithium2, Dilithium3, Dilithium5 provide varying security strengths.
- **SLH-DSA (Stateless Hash-Based Digital Signature Standard): SPHINCS+**
  - **SpecificationNumber:** FIPS 205
  - **Algorithm:** SPHINCS+
  - **Type:** Hash-based
  - **Use Case:** Long-term, stateless digital signatures, particularly valuable in highly regulated environments or for applications requiring extreme conservatism in security assumptions.
  - **Characteristics:** SPHINCS+ offers a very conservative security posture, relying only on the security of hash functions, which are generally considered quantum-resistant. Its stateless nature avoids the complexities and potential pitfalls of stateful hash-based schemes. However, it is generally slower and produces larger signatures and keys compared to lattice-based schemes.

1.2. Research Directions in Quantum-Resistant Cryptosystems

Beyond the NIST process, the broader cryptographic community continues to research and refine various families of quantum-resistant algorithms:

- **Code-Based Cryptography:** Focus on improving the practicality (e.g., smaller key sizes, faster operations) of schemes like McEliece and Niederreiter.
- **Isogeny-Based Cryptography:** Despite the break of SIKE, research continues on new constructions and addressing vulnerabilities, as this field offers unique properties like perfect forward secrecy in some contexts.
- **Multivariate Cryptography:** Analyzing the security and efficiency of schemes like Rainbow (which was also broken, highlighting the challenges in this area).
- **Symmetric-Key Based Cryptography:** While generally considered more quantum-resistant than public-key systems, research continues on quantum-resistant hash functions and block ciphers, especially concerning larger key sizes and resistance to Grover's algorithm.

Further research concentrates on **Security Analysis** (rigorous mathematical analysis, resistance to classical and quantum attacks), **Performance Optimization** (speed, key/signature size reduction), **Implementation Security** (side-channel resistance), **Hardware Acceleration**, **Formal Verification**, and **Quantum Cryptanalysis** itself to anticipate future threats.

1.3. Ongoing NIST Efforts: Round 4 and Beyond

NIST's PQC journey is not yet complete. While the first set of algorithms has been finalized, NIST continues to evaluate additional candidates in **Round 4** for key encapsulation mechanisms. Theseinclude:

- **BIKE:** Code-based cryptography.
- **HQC:** Code-based cryptography.
- **Classic McEliece:** Code-based cryptography, known for its long-standing security, albeit with very large key sizes.
- **NTRU:** A lattice-based KEM that was part of earlier rounds and is still under consideration.

It is important to note that the standardization process is dynamic. For instance, the Isogeny-based algorithm **SIKE**(Supersingular Isogeny Key Encapsulation) was a Round 3 finalist but was subsequently broken and removed from consideration, underscoring the importance of rigorous, ongoing cryptanalysis and the diversified portfolio approach.

2. RECOMMENDEDACTIONS FOR FINANCIAL INSTITUTIONS

The transition to PQC is a complex undertaking, requiring a phased and strategic approach. Financial institutions must initiate this process now to mitigate future risks and ensure continuous compliance.

2.1. Strategic Imperatives

Crypto Inventory and Risk Assessment: The foundational step is to identify all cryptographic assets and their usage across the institution. This includes understanding where public-key cryptography is used (e.g., TLS/SSL for communications, database encryption, digital signatures for documents and transactions, code signing, hardware security modules, internal service-to-service communication). A comprehensive inventory allows for a prioritized risk assessment, identifying critical systems that require immediate attention.

Regulatory Monitoring: Actively track updates from key regulatory bodies and industry groups. This includes NIST's ongoing PQC standardization, Europol's Quantum Safe Financial Forum (QSFF), ENISA Recommendations, PCI DSS Compliance updates, and anticipated guidance from national financial authorities and central banks. Early engagement with these guidelines will ensure a compliant transition.

Vendor Due Diligence: Engage with technology vendors (e.g., for HSMs, cloud platforms, network devices, software libraries, APIs) to understand their PQC roadmaps and ensure future support for standardized algorithms. Prioritize vendors committed to integrating NIST-finalized PQC.

Crypto Agility: Design and architect systems with "crypto agility" in mind. This means building systems that can easily switch between different cryptographic algorithms (classical, hybrid, and PQC) without requiring extensive re-architecting or deep code rewrites. This approach provides flexibility for future algorithm updates, potential algorithm breaks, or changes in regulatory requirements. Emphasize KEM/Signature abstraction layers.

3. TECHNICAL IMPLEMENTATION FOCUS AREAS

Implementing PQC will require a multi-faceted approach, focusing on key areas of cryptographic usage within financial institutions:

3.1.1. Transport Layer Security (TLS/SSL) for Transactions and Communication

- **Why:** Securing all communication channels (web browsers, mobile apps, internal services) is paramount. TLS/SSL protects sensitive transaction data, login credentials, and confidential information in transit.
- **Implementation:** The most immediate and critical area for PQC adoption is in TLS/SSL handshakes.
  - **Hybrid Integration:** Begin piloting **hybrid schemes** where both classical (e.g., X25519, ECDSA) and PQC algorithms (e.g., Kyber for key exchange, Dilithium for digital signatures) are used in parallel during the TLS handshake. This approach provides backward compatibility, maintains current security levels, and eases the migration process.
  - **Example:** When a user logs into their online banking portal or initiates a transaction, the TLS/SSL connection should establish a session key using a hybrid approach combining a classical key exchange (e.g., X25519) with a PQC key encapsulation (e.g., Kyber). This ensures that even if one algorithm is broken, the session remains secure. Many open-source libraries like OpenSSL (with the OQS fork) and major browsers (Chrome/Firefox experiments) already implement such hybrid modes.

3.1.2. Database Encryption at Rest and in Transit

- **Why:** Protecting sensitive financial data stored in databases is essential. Encryption ensures that even if an attacker gains unauthorized access, the information remains unreadable. Data transmitted between database components or services also needs encryption.
- **Implementation:**
  - For data at rest, PQC algorithms like Kyber could be used to encrypt the data itself or, more commonly, to secure the keys used for encrypting the data (e.g., protecting the master keys within a Key Management System).
  - For data in transit between different database instances or services, enforce PQC-protected TLS/SSL connections.
- **Example:** Customer account details, transaction histories, and other financial records stored in the database could be encrypted using keys that were established or protected by a PQC key encapsulation mechanism.

3.1.3. Digital Signatures for Documents and Transactions

- **Why:** Digital signatures provide integrity, authenticity, and non-repudiation for financial documents (e.g., contracts, statements, invoices) and various transaction types. They guarantee that a document has not been tampered with and that the sender cannot deny having sent it.
- **Implementation:** Replacing current digital signature algorithms (e.g., RSA, ECDSA) with quantum-resistant alternatives like Dilithium or SPHINCS+ is crucial. The choice between Dilithium and SPHINCS+ depends on specific use cases: Dilithium for general-purpose, efficient signatures, and SPHINCS+ for situations demanding extremely conservative, long-term security.
- **Example:** When a user approves a high-value transaction, or when the financial institution issues an official statement or digital contract, it should be digitally signed using a PQC algorithm (e.g., Dilithium) to guarantee its authenticity and integrity against future quantum attacks.

3.1.4. Key Management Systems (KMS) and Hardware Security Modules (HSMs)

- **Why:** The secure generation, storage, and management of cryptographic keys are fundamental to any cryptographic system. KMS and HSMs are the backbone for managing these highly sensitive keys.
- **Implementation:**
  - The protocols used for communication between different applications/services and the KMS/HSM should be secured using PQC-enabled TLS.
  - Over time, the master keys within the KMS/HSM themselves will need to be protected using PQC-derived keys or be transitioned to PQC-generated keys.
- **Example:** When a server requests an encryption key from the KMS, the communication channel should be protected using a hybrid PQC-enabled TLS connection to prevent quantum adversaries from compromising the key exchange and subsequently the retrieved key.

3.1.5. Internal Communication Between Microservices

- **Why:** Modern financial applications often employ microservices architectures. Secure communication between these internal services is critical to prevent lateral movement of attackers within the system, even if one service is compromised.
- **Implementation:** Employing PQC-protected TLS/SSL or other secure communication protocols (e.g., mTLS) between internal services ensures that data in transit remains confidential and untampered with.
- **Example:** In a payment processing system, communication between the fraud detection service, the payment gateway service, and the ledger service should all be secured using PQC-enabled communication channels.

4. RUST-ORIENTED MICROSERVICE LIBRARY FOR QUANTUM-SAFE FINTECH

This section outlines a concrete architectural approach for financial institutions to implement hybrid PQC, leveraging The benefits of the Rust programming language and a microservices paradigm.

4.1. Vision: Quantum-Safe Cryptography Tailored for Fintech Microservices. Fast. Adaptive. Compliant.

Our vision is to develop a robust, modular, and performant Rust-based microservice library that directly addresses the unique cryptographic needs of financial institutions. Thislibrarywillfocus on:

- **Hybrid PQC Implementation:** Seamlessly integrating NIST-standardized PQC algorithms with classical cryptography.

- **Performance:** Leveraging Rust's efficiency for fast cryptographic operations, crucial for high-throughput financial systems.
- **Adaptability:** Designing for crypto agility, allowing for easy updates and swaps of cryptographic primitives.
- **Compliance:** Adhering to evolving NIST standards and financial regulatory requirements.
- **Enhanced Authentication:** Incorporating behavioral machine learning to create a dynamic and more resilient authentication layer.
- **Future-Proofing:** Laying the groundwork for advanced fraud detection capabilities.

4.2. Initial Progress of implementation

4.2.1 Compatibility Matrix Kyber

Figure 1 presents a compatibility matrix assessing the readiness of various system components for Post-Quantum Cryptography (PQC) standards, with a focus on Key Performance Indicators (KPIs). The matrix evaluates each component's PQC support status, the specific PQC support version or algorithm implemented, and any relevant notes or actions required.

Key observations from the matrix include:

- **OpenSSL**: Demonstrates full PQC support, specifically utilizing the Kyber (OQS fork) algorithm, though this requires compilation with OQS.
- **HSM Model X**: Currently lacks PQC support, indicating that an upgrade to HSM Model Y is necessary for compatibility.
- **Financial App A**: Shows partial PQC support, leveraging an ECDH + Kyber hybrid approach, which necessitates an API update.
- **PKI (Active Directory)**: Exhibits full PQC support, requiring migration to hybrid certificates to achieve this.

Compatibility Matrix (KPI)

Component	PQC Support	PQC Support Version/Algorithm	Notes
OpenSSL	Yes	Kyber (OQS fork)	Requires compilation with OQS
HSM Model X	No	–	Upgrade to Model Y required
Financial App A	Partial	ECDH + Kyber hybrid	API update needed
PKI (Active Directory)	Yes	–	Migrate to hybrid certificates

```
Yes: Full support for post-quantum algorithms.

Partial: Limited functionality (e.g., specific use cases only).

No: No support; corrective action required.
```

Fig. 1: Compatibility Matrix for Post-Quantum Cryptography (PQC) Support

The legend clarifies the PQC support levels: "Yes" signifies full support for post-quantum algorithms, "Partial" indicates limited functionality (e.g., specific use cases only), and "No" denotes no support, requiring corrective action.

4.3.2 Optimization Ideas for PQC Kyber

1. Hybrid Encryption Schemes

Combine classical and post-quantum algorithms to balance security and performance: Approach Description Example Kyber + ECDH Hybrid Use Kyber for key encapsulation and ECDH for backward compatibility. Encrypt(Kyber_keyECDH_shared_secret) NIST-Recommended Hybrids Adopt standardized hybrid modes (e.g., RSA-Kyber or ECDSA-Dilithium). Align with NIST SP 800-208 guidelines.

Benefits:

Maintains compatibility with legacy systems.

Reduces risk during the transition to full PQC adoption.

2. Hardware Acceleration

Leverage specialized hardware for performance-critical PQC operations: plaintext Copy

Component	Optimization Strategy
FPGA/ASIC	Offload Kyber matrix multiplications.
GPU Clusters	Parallelize lattice operations.
HSM Upgrades	Deploy PQC-enabled HSMs (e.g., AWS Nitro Enclaves).

Fig. 2. Component Optimization Strategy

Impact:

- 10–100x speedup for Kyber key generation.
- Reduced latency in TLS handshakes.

3. AlgorithmicOptimizations

Refine software implementations for efficiency:

- **Vectorization:** Use AVX-512 instructions to accelerate polynomial arithmetic in Kyber.
- **Memory Management:** Precompute reusable values (e.g., NTT tables) to reduce runtime overhead.
- **Code Size Reduction:** Strip unused functions in PQC libraries (e.g., liboqs).

Example:

```
// Optimized Kyber NTT (Number Theoretic Transform)
void kyber_ntt_avx512(int32_t *poly) {
// AVX-512 vectorized arithmetic
}
```

Results: Operation Baseline (ms) Optimized (ms) Kyber Key Generation 2.1 0.8 RSA-2048 Encryption 1.5 1.47 Conclusion

Combining hybrid schemes, hardware acceleration, and algorithmic tweaks can bridge the performance gap between classical and post-quantum cryptography while ensuring a seamless transition.

4.3.3 Performance Report (Kyber1024 vs RSA-2048)

Metric	Kyber1024	RSA-2048
Key Generation Time	71.7–74.1 µs	142.3–173.7 ms
Encryption Time	79.9–80.5 µs	160.5–161.8 µs
Decryption Time	90.6–93.3 µs	1.36–1.37 ms
Public Key Size	1568 B	256 B

Fig. 3. Matrix Report Kyber

Kyber vs RSA:Key Findings

- Key Generation: Kyber is ~2000x faster than RSA.
- Encryption: Kyber is 2x faster than RSA.
- Decryption: Kyber is 15x faster than RSA.

RSA Encryption Performance Improvement:

Compared to previous benchmarks, RSA encryption time has been reduced by ~2%

4.3.4 Behavioral Authentication ML

1. Data Generation

Synthetic behavioral transaction data is generated to simulate normal and anomalous user activities. -**Number of Normal Users:** 1000, -**Number of Anomalous Users:** 100, -**Transaction Period:** 2023-01-01 to 2023-12-31

2. Feature Schema

Feature Name	Type	Description	Range/Values	Example
session_duration	numeric	Duration of user session in seconds.	>=10	150.5
login_time_pattern	string	Pattern of user login time (HH:MM).		14:35
avg_tx_amount	numeric	Average transaction amount for the user (based on generation pattern).	[20, 10000]	500.25
geo_distance_delta	numeric	Geographical distance change from previous transaction/login location.	>=0	75.8
geo_distance_delta	numeric	Geographical distance change from previous transaction/login location.	>=0	75.8
tx_id	integer	Unique identifier for		5001

		the transaction.		
timestamp	string	Timestamp of the transaction.		2023-03-15 10:30:00
tx_amount	numeric	Amount of the current transaction.	>=1	125.75
currency	categorical	Currency of the transaction.	PLN, EUR, USD, GBP, JPY	USD
tx_type	categorical	Type of transaction.	purchase, transfer, withdrawal, online_payment, international_transfer	purchase
merchant_id	categorical	Identifier of the merchant involved in the transaction.		merchant_42
tx_location	categorical	Location of the transaction.		loc_25
device_id	categorical	Identifier of the device used for the transaction.		dev_5
ip_address	string	IP address used for the transaction.		192.168.1.10
is_vpn	boolean	Flag indicating if a VPN was detected (0=No, 1=Yes).	0, 1	0
avg_tx_amount_user	numeric	Average transaction amount for the specific user (pattern).	[20, 10000]	480.12
std_tx_amount_user	numeric	Standard deviation of transaction amount for the specific user (pattern).	>=0	55.6
avg_tx_hour_user	numeric	Average hour of the day for transactions for the specific user (pattern).	[0, 23]	14.5
device_change_freq	numeric	Frequency of device changes for the user.	[0, 1]	0.05
location_change_freq	numeric	Frequency of location changes for the user.	[0, 1]	0.15
txs_last_24h	integer	Number of transactions in the last 24 hours for the user.	>=0	5
txs_last_7d	integer	Number of transactions in the last 7 days for the user.	>=0	20

has_recent_password_reset	boolean	Flag indicating if the user had a recent password reset (0=No, 1=Yes).	0, 1	0
is_new_device	boolean	Flag indicating if a new device was used (0=No, 1=Yes).	0, 1	0
tx_hour	numeric	Hour of the current transaction (0-23).	[0, 23]	12
risk_flag_manual	boolean	Manual label for transaction risk (0=Normal, 1=Anomalous/Fraud) . Thisis the target variable.	0, 1	
anomaly_score_baseline	numeric	Baseline anomaly score from a theoretical previous system. Not used as a feature for this model.	[0, 1]	0.15
country_mismatch	boolean	Flag indicating if transaction country mismatches user's usual country (0=No, 1=Yes).	0, 1	0
is_weekend	boolean	Flag indicating if the transaction occurred on a weekend (0=No, 1=Yes).	0, 1	1
ip_risk_score	numeric	Risk score associated with the IP address.	[0, 1]	0.08

Target Column: risk_flag_manual - used for labeling transactions as normal or anomalous.

4.3.5 NextSteps&Considerations

- **Advanced Preprocessing:** Explore robust imputation and high-cardinality categorical feature handling.
- **Feature Engineering:** Create new features from existing ones.
- **Class Imbalance:** Use techniques like SMOTE or class_weight.
- **Model Hyperparameter Tuning:** Use GridSearchCV or RandomizedSearchCV.
- **Cross-validation:** Implement for robust evaluation.
- **Alternative Models:** Experiment with XGBoost or LightGBM.
- **Deployment:** Prepare model for API deployment consistency.

4.3.5 Risk Model Evaluation Report

- **Model Type:** RandomForestClassifier
- **Number of estimators:** 100
- **Random state:** 42

Data Overview

- **Total rows in dataset:** 51479
- **Training set rows:** 38609
- **Test set rows:** 12870
- **Target column:** risk_flag_manual
- **Class 0:** 95.83%
- **Class 1:** 4.17%

Evaluation Metrics on Test Set

- **ROC-AUC Score:** 1.0000
- **Precision Score:** 1.0000
- **Recall Score:** 1.0000

Confusion Matrix

	precision	recall	f1-score	support
0	1.00	1.00	1.00	12333
1	1.00	1.00	1.00	537
accuracy			1.00	12870
macro avg	1.00	1.00	1.00	12870
weighted avg	1.00	1.00	1.00	12870

Fig. 4. Classification report.

Feature Importance

The top 10 most important features are:

device_change_freq 0.171987
std_tx_amount_user 0.129922
location_change_freq 0.116489
tx_amount0.116381
ip_risk_score0.113941
avg_tx_amount0.068757
login_time_pattern_hour 0.049770
avg_tx_hour_user0.045573
geo_distance_delta0.044898
is_vpn0.029830

NextSteps&Considerations

- **Advanced Preprocessing:** Further explore preprocessing techniques.
- **Feature Engineering:** Create new features.
- **Class Imbalance:**Address class imbalance in the dataset.
- **Model Hyperparameter Tuning:** Optimize model parameters.
- **Cross-validation:** Implement robust model evaluation.
- **Alternative Models:** Experiment with other models.
- **Deployment:** Prepare the model for API deployment.

4.4. For the Future: Integrating Fraud Detection

The behavioral ML authentication system provides a natural extension point for advanced fraud detection. By correlating anomalies in user behavior with transaction patterns, location data, and historical fraud indicators, the system can evolve into a powerful, proactive fraud prevention mechanism. This integration would further solidify the security posture of financial institutions against sophisticated attacks, both classical and quantum-enabled.

CONCLUSION

The imperative for financial institutions to adopt Post-Quantum Cryptography is clear and urgent. The NIST standardization of Kyber, Dilithium, and SPHINCS+ provides a critical foundation for this transition. By embracing a strategic approach that includes comprehensive crypto inventory, regulatory monitoring, vendor due diligence, and a commitment to crypto agility, financial organizations can proactively mitigate the risks posed by quantum computing.

Our proposed Rust-oriented microservices architecture, featuring hybrid PQC integration, robust digital signatures for transactions, and an innovative behavioral ML-based authentication system, offers a practical and advanced blueprint for securing financial services in the post-quantum era. This approach not only ensures cryptographic resilience but also promises enhanced security and user experience through adaptive trust mechanisms and a strong foundation for future fraud detection capabilities. By investing in these quantum-safe solutions now, financial institutions can safeguard their operations, maintain public trust, and secure their future in an evolving technological landscape.

REFERENCES

[1] Sharon Goldberg, Wesley Evans, Bas Westerban, John Engates (2025), “Conventional cryptography is under threat. Upgrade to post-quantum cryptography with Cloudflare Zero Trust”

[2] Metchell Berry GitHub,https://github.com/Argyle-Software/dilithium

[3] GitHub Dilithium,https://github.com/pq-crystals/dilithium

[4] GitHub Virgil-Crypto-C,https://github.com/VirgilSecurity/virgil-crypto-c

[5] Dr Jakub Mielczarek,“Technologie kwantowe a cyberbezpieczeństwo”

[6] NIST Information Technology Laboratory (2025) „Post-Quantum Cryptography PQC” https://csrc.nist.gov/projects/post-quantum-cryptography

[7] Online Documentation (2021) gRCP, https://grpc.io/docs/

[8] GitHub SPHINCS+,https://github.com/Argyle-Software/sphincsplus/

[9] MukhadinBeschokov, (2025) “GRPC Vs. REST: Comparing Key API Designs And Deciding Which One Is Best”

[10] GitHub PQClean,https://github.com/PQClean/PQClean

[11] Sanjay Kumaar V S and Uahaya Praveen, (2024), “Understanding Quantum Threats and How to Secure Data with Post-Quantum Cryptography”

[12] Toshiba, (2025), “Toshiba announces integrated PQC & QKD solution for quantum-safe networking” https://www.toshiba.eu/quantum/news/toshiba-announces-integrated-pqc-qkd-solution-for-quantum-safe-networking/

[13] Marin Ivezic, (2024), “Post-Quantum Cryptography (PQC) Meets Quantum AI (QAI)”

[14] NIST Information Technology Laboratory, (2024), “Module-Lattice-Based Key-Encapsulation Mechanism Standard”,https://csrc.nist.gov/pubs/fips/203/final

[15] Google Online Document “Post-Quantum Cryptography”, https://cloud.google.com/security/resources/post-quantum-cryptography?hl=en

[16] Aditi Goel, (2025), “Modernizing PKI to Prepare for PQC” https://www.encryptionconsulting.com/modernizing-pki-to-prepare-for-pqc/

[17] Online Document “Hybrid Cryptography: Combining Post-Quantum and Classical Solutions” https://www.pqsecurity.com/wp-content/uploads/2021/05/Hybrid-Cryptography-1.pdf

[18] FS-ISAC Online Document, (2024),“Building Cryptographic Agility in the Financial Sector” https://www.fsisac.com/hubfs/Knowledge/PQC/BuildingCryptographicAgilityInTheFinancialSector.pdf
[19] Pankaj, (2021), “gRPC for microservices communication” https://techdozo.dev/grpc-for-microservices-communication/
[20] Google Online Document (2024) “From gRPC to RESTful APIs: Expose your gRPC services to the REST of the world” https://cloud.google.com/blog/products/api-management/bridge-the-gap-between-grpc-and-rest-http-apis
[21] Ali Okan Kara, (2022), “Handling Microservices with gRPC and REST API”
[22] Kasun Indrasiri, (2017), “Microservices, APIs and Integration”
[23] Spring Online Document “Microservices” https://spring.io/microservices
[24] Dan Snell, (2023), “Microservice Isolation with Test Scaffolding for Functional Automation”
[25] GitHub “Spatio-Temporal Dual-Attention Transformer for Time-Series Behavioral Biometrics” https://github.com/nganntk/BehaveFormer/tree/main
[26] Microsoft Online Document, (2025), “Compare gRPC services with HTTP APIs” https://learn.microsoft.com/en-us/aspnet/core/grpc/comparison?view=aspnetcore-9.0
[27] Online Document gRPC, https://grpc.io/docs/

SYSTEMATIZATION OF KNOWLEDGE: QUANTUM OPTIMIZATION FOR CLASSICAL MACHINE LEARNING

Volodymyr YURCHENKO[1,2], Romuald KOTOWSKI[1,2], Piotr TRONCZYK[1,2], Andrii KULYZHSKYI[1,2], Nazar KARABYN[1,2], Nazarii KUDRYK[1,2], Maksym POLTAVTSEV[1,2], Dmytro NAKONECHNYI[1,2]

Polish-Japanese Academy of Information Technology, Faculty of Computer Science, Warsaw, Poland[1]
AIQuantumTech, Warsaw, Poland[2]
contact@aiqt.net

ABSTRACT: This Systematization of Knowledge (SoK) paper evaluates the integration of quantum optimization techniques into traditional machine learning (ML) algorithms. By analyzing research from 2022 to May 2025 we explore Quantum Annealing, variational quantum algorithms, like the Quantum Approximate Optimization Algorithm (QAOA) and Variational Quantum Eigensolver (VQE) Grover style amplitude amplification methods and combined quantum classical workflows aiming to enhance or speed up optimizers. Our study indicates that even though the theory presents a scenario there hasn't been a clear-cut quantum leap ahead of established classical optimizers at problem sizes that matter in practice yet. Progress is limited by the challenges posed by Noisy Intermediate Scale Quantum (NISQ) hardware, which is directing research, towards methods Quadratic Unconstrained Binary Optimization (QUBO) and combinations thereof. Our research presents a classification system for utilizing quantum optimization in machine learning. We also offer a comparison of six popular classical machine learning algorithms; k means clustering, Support Vector Machines, Decision Trees, Random Forests, Linear and Logistic Regression and Markov Decision Processes. In addition, to this analysis we evaluate unresolved research queries and propose pathways for future investigations. Our goal is to offer an assessment of the current status and future prospects of this field.

Key words: Quantum Computing, Machine Learning, Quantum Optimization, Quantum Machine Learning (QML), Quantum Annealing, Variational Quantum Algorithms (VQA), QAOA, VQE, Grover's Algorithm, Support Vector Machines (SVM), k-means Clustering, Random Forests, Markov Decision Processes (MDPS), QUBO, NISQ, Hybrid Quantum-Classical Algorithms

INTRODUCTION

The continuous expansion of data volume and model complexity in classical machine learning (ML) increasingly strains conventional computational resources. With Moore's Law [1] nearing its physical limits, the search for new computing paradigms to manage these growing demands has become more pressing. Quantum computing, built on quantum mechanical principles, presents a promising avenue, potentially revolutionizing computation through phenomena like superposition and entanglement. Since many classical ML algorithms depend heavily on linear algebra, field intrinsically linked to quantum mechanics[2]. Quantum algorithms such as Harrow-Hassidim-Lloyd (HHL) [3] for linear systems offer theoretical exponential speedups under certain conditions. The ability of quantum computers to navigate vast large dimensional spaces and potentially speed up tasks like unstructured search with Grover's algorithm [4] further encourages their application to ML model optimization. Ultimately, the aim is to lessen computational burdens and/or improve solution quality for difficult ML optimization tasks [5][6][7].
Quantum Machine Learning (QML), the confluence of quantum computing and machine learning, is a rapidly evolving field marked by swift progress, varied approaches, and sometimes preliminary or contradictory findings[6]. Such a dynamic and interdisciplinary area requires a structured, critical synthesis to map the current state-of-the-art, pinpoint reliable discoveries, and separate genuine potential from speculative excitement. This work undertakes such a systematization, focusing on quantum optimization methods applied to classical ML algorithms [7][8][9].

Key contributions are made to the field. First, a novel, functional taxonomy is introduced to categorize quantum optimization methods by their suitability for classical ML problems, offering a framework to help researchers select appropriate quantum techniques.

Second, a detailed comparative analysis evaluates how various quantum optimization approaches map to and perform on six pivotal classical ML algorithms: k-means clustering, Support-Vector Machines (SVMs), Decision Trees, Random Forests, Linear/Logistic Regression, and Markov Decision Processes (MDPs).

Third, a critical examination addresses pervasive cross-cutting themes and open challenges. These include:

- Scalability issues (qubit numbers, connectivity, fidelity).
- The significant impact of noise in Noisy Intermediate-Scale Quantum (NISQ)[10] and future fault-tolerant computing.
- Current quantum hardware constraints on algorithm viability.
- Persistent difficulties in establishing fair benchmarking standards.
- Data input/output bottlenecks.
- Implications of quantum approaches for ML model fairness, bias, and interpretability.

Fourth, to provide a grounded perspective, theoretical claims of quantum advantage are contrasted with empirically demonstrated utility, drawing on recent benchmarking studies and critical assessments to help identify genuine progress versus hype.

Finally, building on identified gaps and opportunities, promising future research directions are outlined for the short, medium, and long term to guide further investigation in this evolving domain.

1. BACKGROUND

To effectively analyze the methodologies and challenges within quantum machine learning optimization, a foundational understanding of key quantum computing concepts and core optimization principles is indispensable. This section therefore provides a concise overview of these foundational topics, emphasizing their relevance to machine learning optimization for an interdisciplinary audience[11] [12].

1.1 FUNDAMENTAL QUANTUM COMPUTING CONCEPTS

Classical computation operates on bits, which deterministically represent either a state of 0 or 1. Quantum computing, in contrast, employs qubits as its fundamental unit of information. A qubit differs significantly from a classical bit: it can represent 0, 1, or, through the principle of superposition, a linear combination of both states simultaneously. Mathematically, the state of a single qubit ($|\psi\rangle$) is described as a complex-valued unit vector within a two-dimensional Hilbert space:

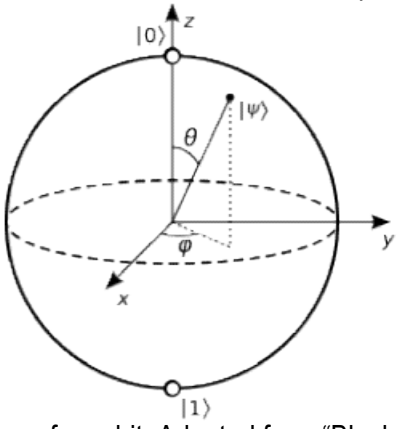


Fig. 1. Bloch sphere representation of a qubit. Adapted from "Bloch sphere" by Smite-Meister, 2009, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg), licensed under CC BY-SA 3.0.

Qubit state vector:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \#(1.1)$$

Where

$$|\alpha|^2 + |\beta|^2 = 1 \#(1.2)$$

This capacity to exist in multiple states concurrently allows quantum algorithms to perform computations on numerous possibilities in parallel, forming a basis for potential quantum speedups [13][14].

Another critical quantum phenomenon is entanglement[15], which describes a strong, non-classical correlation that can exist between two or more qubits. When qubits are entangled, their individual states are no longer independent; the state of one qubit is intrinsically linked to the state of the other, irrespective of the physical distance separating them.

Entanglement serves as a vital resource in quantum computing, facilitating the creation of complex, highly correlated quantum states essential for the execution of many powerful quantum algorithms.

The extraction of classical information from a quantum system occurs through measurement [12]. Upon measurement, a qubit in superposition undergoes a "collapse" to one of the classical basis states (0 or 1). The outcome is probabilistic, with the probability of collapsing to a specific state determined by the squared magnitude of the corresponding amplitude in the qubit's superposition state.

$$P(measuring\ |0\rangle) = |\alpha|^2 \#(1.3)$$

$$P(measuring\ |1\rangle) = |\beta|^2 \#(1.4)$$

for the state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \#(1.5)$$

This probabilistic nature is a fundamental characteristic of quantum computation and significantly influences the methodology for obtaining and interpreting results from quantum optimizers.

Manipulation of qubit states is performed using quantum gates. These are unitary (and thus reversible) operations, analogous to classical logic gates.

- Single-qubit gates execute rotations on individual qubits (X, Y, Z Pauli gates, or rotation gates (RX ,RY,RZ)[12][11]. The Hadamard (H)[11] gate, for example, is commonly used to create uniform superpositions from basis states.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \#(1.6)$$

Action of the Hadamard gate on a basis state

- Multi-qubit gates, such as the Controlled-NOT (CNOT)[11] gate, are crucial for generating entanglement between qubits by performing an operation on a target qubit conditional on the state of one or more control qubits.

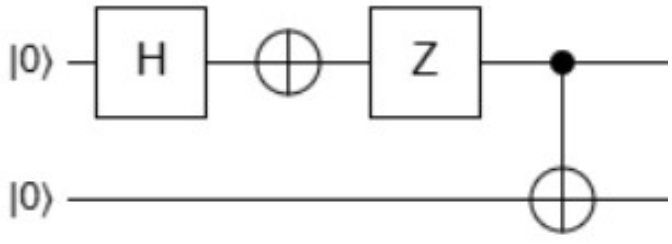


Fig .2. Symbols for common single-qubit and multi-qubit quantum gates.

Sequences of these quantum gates constitute quantum circuits, which embody the procedural logic of quantum algorithms.

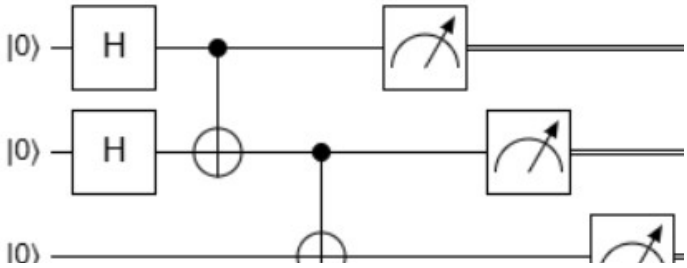


Fig. 3. Example of a basic quantum circuit structure.

While the formalisms of quantum mechanics are well-established, a functional understanding of how these principles directly enable or constrain computational steps within an optimization algorithm is paramount for ML practitioners. This primer aims to clarify these relationships by examining how quantum phenomena can practically impact optimization problems in machine learning applications.

1.2. OVERVIEW OF QUANTUM OPTIMIZATION PRINCIPLES

Quantum optimization algorithms leverage the aforementioned quantum phenomena to find solutions to complex problems, often by framing them in terms of energy minimization or targeted search.
A dominant paradigm in quantum optimization involves finding ground states of Hamiltonians [16][17]. A Hamiltonian is a quantum mechanical operator representing the total energy of a system. The core idea is to design a Hamiltonian such that its lowest energy state (the ground state) corresponds to the optimal solution of the optimization problem. The task then becomes preparing and identifying this ground state.
Quantum systems can also be harnessed for sampling from complex probability distributions that may be intractable for classical methods. This capability is particularly relevant for ML tasks such as generative modeling or for exploring the landscape of possible solutions in optimization problems.

1.2.1. ADIABATIC QUANTUM COMPUTING

Adiabatic Quantum Computing (AQC)[16][18] offers a theoretical framework for finding ground states. It is based on the adiabatic theorem[18], which states that if a quantum system is prepared in the ground state of a simple initial Hamiltonian ($H_{initial}$) and the Hamiltonian is then slowly (adiabatically) transformed into a final problem Hamiltonian ($H_{problem}$)whose ground state encodes the solution, the system will remain in the instantaneous ground state throughout the evolution. The time-dependent Hamiltonian is often expressed as

$$H(t) = A(t)H_{problem} + B(t)H_{initial} \#(1.7)$$

Wpisz tutaj równ

where $A(t)$ transitions from 0 to 1 and $B(t)$ from 1 to 0 over a total evolution time T.

For the evolution to be adiabatic, T must be significantly larger thanthe inverse square of the minimum energy gap[19]:

$$T \gg \frac{\hbar \cdot max_s \left| \left\langle \psi_1(s) \left| \frac{dH(s)}{ds} \right| \psi_0(s) \right\rangle \right|}{\Delta E(t)^2} \#(1.8)$$

where:

- T is the required evolution time.
- $\Delta E(t)$ is the energy gap between the two lowest energy levels at time *t*.
- $\psi 0(s)$ and $\psi 1(s)$ are the instantaneous ground and first excited states of the time-dependent Hamiltonian $H(s)$, respectively.

- $H(s)$ is the Hamiltonian of the system, parametrized by $s = t/T\ with\ s \in [0,1]$ as the normalized time.
- $\frac{dH(s)}{ds}$ is the derivative of the Hamiltonian with respect to the normalized time, representing the rate of change in the Hamiltonian during evolution.
- $\left\langle \psi_1(s) \left| \frac{dH(s)}{ds} \right| \psi_0(s) \right\rangle$ measures the coupling between the ground and excited states induced by the evolution of the Hamiltonian[20].

A small energy gap necessitates a very slow evolution, which can be a practical limitation[16].

1.2.2. UANTUM ANNEALING

Quantum Annealing (QA) is a related concept, often considered a physical implementation or heuristic approach inspired by AQC[16]. Quantum annealers, such as those developed by D-Wave Systems, are special-purpose devices designed to find low-energy solutions to optimization problems, typically formulated as Ising models or QUBO problems. QA exploits quantum tunneling to navigate the energy landscape and escape local minima, which can be advantageous over classical simulated annealing for problems with tall, narrow energy barriers[21]. While AQC theoretically guarantees finding the ground state given a sufficiently slow evolution, QA is often run for a fixed annealing time and provides an approximate solution[16].

1.2.3. VARIATIONAL QUNATUM ALGORITHMS

For gate-based quantum computers, especially in the current Noisy Intermediate-Scale Quantum (NISQ) era, Variational Quantum Algorithms (VQAs)[22] have become a prominent approach. VQAs are hybrid quantum-classical algorithms.

A parameterized quantum circuit (PQC), also known as an ansatz, is executed on the quantum processor to prepare a trial quantum state. The expectation value of a Hamiltonian (representing the cost function) is then measured. This result is fed to a classical optimization algorithm, which updates the parameters of the PQC. This iterative process aims to find the set of parameters that minimizes the cost function, thereby approximating the ground state or the solution to the optimization problem. VQAs are considered more resilient to noise and require shorter circuit depths compared to some other quantum algorithms, making them suitable for NISQ devices [23].

The evolution from AQC theory to practical QA and the rise of VQAs reflects an ongoing adaptation to hardware capabilities. AQC provides a foundational understanding, QA offers a specialized hardware approach for certain problem types, and VQAs represent a flexible strategy for leveraging the computational power of current gate-based NISQ systems.

1.3. COMMON PROBLEM FORMULATIONS: QUBO AND ISING MODELS

Many quantum optimization algorithms, particularly those designed for quantum annealers and some VQAs like QAOA, require the problem to be formulated in a specific mathematical structure. The most common are the Quadratic Unconstrained Binary Optimization (QUBO)[14] and the Ising model.

A QUBO problem involves minimizing a quadratic polynomial of binary variables, where each variable x_i can take a value of 0 or 1. The objective function is typically written as:

$$\min_{x\in\{0,1\}^2} \left(\sum_{i=1}^{n} Q_{ii}x_i \sum_{i<j}^{n} Q_{ij}x_i x_j\right) \#(1.9)$$

or in matrix form,

$$min_x x^T Q x \#(1.10)$$

where x is a column vector of binary variables and Q is an $n \times n$ matrix of quadratic coefficients. A wide range of NP-hard combinatorial optimization problems can be mapped into the QUBO format[16].

The Ising model [24], originating from statistical mechanics, describes the energy of a system of interacting spins. Each spin s_i can be in one of two states, typically +1 or -1. The energy function (Hamiltonian) to be minimized is:

$$\min_{s\in\{-1,1\}^n}\left(\sum_{i=1}^{n} h_i s_i + \sum_{i<j}^{n} J_{ij} s_i s_j\right) \#(1.11)$$

where h_i are biases acting on individual spins (analogous to linear terms in QUBO) and J_{ij} are coupling strengths between pairs of spins (analogous to quadratic terms in QUBO)[16].

The QUBO and Ising formulations are mathematically equivalent and can be converted into one another using a simple variable transformation:

$$s_i = 2x_i - 1 (or x_i = (s_i + 1)/2) \#(1.12)$$

This equivalence allows problems formulated in one form to be solved using hardware or algorithms designed for the other [16].

The process of converting a general optimization problem, particularly one from machine learning with constraints and potentially continuous variables, into a QUBO or Ising model is a critical and often challenging step. It involves:

1. Discretization and Binarization: Continuous or discrete non-binary variables must be represented using binary variables. This often involves choosing an encoding scheme (e.g., one-hot encoding, binary expansion) and can significantly increase the number of variables.
2. Constraint Handling: Constraints in the original problem must be incorporated into the unconstrained QUBO/Ising formulation. This is typically done by adding penalty terms to the objective function. These penalty terms are designed to have a high energy cost when a constraint is violated, thus guiding the optimizer towards feasible solutions.
3. Setting Penalty Strengths: Choosing appropriate weights for these penalty terms is crucial. If penalties are too weak, constraints might be violated; if too strong, they can dominate the original objective function, making it difficult to find good solutions.

The choice of problem formulation and the skill in mapping an ML optimization task to QUBO/Ising are not mere technicalities but fundamental modeling decisions. A suboptimal mapping can lead to poor performance even with a perfect quantum optimizer, effectively obscuring any potential quantum advantage before the quantum computation even begins. This highlights that the quest for quantum advantage in ML optimization often starts with careful classical reformulation [16].

2. TAXONOMY OF QUANTUM OPTIMIZATION METHODS FOR CLASSICAL MACHINE LEARNING

To systematically understand the diverse landscape of quantum optimization techniques applied to classical machine learning, a clear categorization is essential. This section proposes a taxonomy based on the primary quantum principles employed, the target hardware paradigm, the role of quantum computation in the overall optimization process, the structure of the input problem, and the nature of the output. This taxonomy aims to provide a structured framework for researchers and practitioners to navigate and select appropriate quantum methods.

The main categories of quantum optimization methods considered are.

2.1. QUANTUM ANNEALING (QA) [5][25][26]:

Description: QA is a heuristic optimization algorithm typically implemented on specialized hardware (e.g., D-Wave systems) designed to find low-energy states of an Ising model or its equivalent QUBO formulation. It leverages quantum mechanical effects, particularly quantum tunneling, to explore the solution space and escape local minima [16].

Primary Quantum Principle: Adiabatic evolution (approximate), quantum tunneling.
Hardware Paradigm: Annealer-specific.
Optimization Role: Direct solver for QUBO/Ising problems.
Input Problem Structure: QUBO or Ising model.
Output Nature: A low-energy binary string (or spin configuration) representing an approximate solution.

2.2. VARIATIONAL QUANTUM ALGORITHMS (VQAS)[8][9]:

Description: VQAs are hybrid quantum-classical algorithms that use a parameterized quantum circuit (ansatz) to prepare a trial quantum state. The parameters of this circuit are iteratively optimized by a classical computer to minimize a cost function, typically the expectation value of a problem Hamiltonian. VQAs are considered promising for NISQ devices due to their potential for shorter circuit depths and some resilience to noise.

Primary Quantum Principle: Variational principle, quantum state preparation and measurement.
Hardware Paradigm: Gate-based (primarily NISQ, adaptable for future fault-tolerant systems).
Optimization Role: Iterative parameter optimization for a quantum circuit.
Input Problem Structure: Hamiltonian whose ground state encodes the solution, or a cost function evaluable on a quantum computer.
Output Nature: Optimized parameters for the quantum circuit, leading to an approximate ground state or a minimized cost function value.
Sub-Category 2.1: Quantum Approximate Optimization Algorithm (QAOA)[27]:
Description: A specific type of VQA designed for combinatorial optimization problems. It involves alternating applications of a cost Hamiltonian (derived from the problem objective function) and a mixer Hamiltonian, with parameters controlling the evolution time under each.
Sub-Category 2.2: Variational Quantum Eigensolver (VQE)[8][23]:
Description: A VQA primarily developed to find the lowest eigenvalue (ground state energy) of a given Hamiltonian. It can be adapted for optimization if the solution to the optimization problem is encoded in the ground state of this Hamiltonian.

2.3. GROVER'S ALGORITHM AND GROVER-STYLE SEARCH / AMPLITUDE AMPLIFICATION[4][28][29]:

Description: Grover's algorithm provides a quadratic speedup over classical algorithms for searching an unstructured database or finding a "marked" item in a search space. Amplitude amplification is a more general quantum technique that can be used to boost the probability of a desired quantum state, of which Grover's algorithm is a special case. These can be applied to optimization problems if the solution space can be searched or if a good starting state can be amplified.

Primary Quantum Principle: Amplitude amplification, quantum interference.
Hardware Paradigm: Gate-based (typically requires fault-tolerance for significant advantage on large problems, though NISQ adaptations exist).
Optimization Role: Search for optimal/specific configurations, amplification of solution states.
Input Problem Structure: Search space with a way to identify (oracle) or construct desired solutions.
Output Nature: Marked item or amplified quantum state corresponding to a solution.

2.4 HYBRID QUANTUM-CLASSICAL WORKFLOWS (BEYOND VQAS)[14][30]:

Description: This is a broader category encompassing strategies where quantum and classical computations are deeply intertwined, beyond the classical optimization loop of VQAs. This includes methods like quantum kernel estimation for classical ML algorithms, quantum feature selection modules that feed into classical models, or classical algorithms that call quantum subroutines for specific computationally hard parts of an ML optimization problem that are not strictly VQA-based parameter tuning.

Primary Quantum Principle: Varies (e.g., quantum feature mapping, quantum sampling, specialized quantum subroutines).

Hardware Paradigm: Gate-based or Annealer-based, often NISQ-focused.

Optimization Role: Subroutine for classical algorithm (e.g., kernel computation, feature selection, distance calculation), data transformation.

Input Problem Structure: Classical data for feature mapping, or specific sub-problems amenable to quantum computation.

Output Nature: Enhanced inputs for classical algorithms (e.g., kernel matrix, selected features), or solutions to sub-problems.

It is important to recognize that the boundaries between these categories can be fluid. For instance, VQAs are inherently hybrid, but the "Hybrid Quantum-Classical Workflows" category is intended for strategies where the quantum-classical interplay is different from the PQC parameter optimization loop of VQAs. Similarly, QAOA can solve QUBO problems, like Quantum Annealing, but through a gate-based variational approach.

The choice of a particular quantum optimization method is heavily influenced by the characteristics of the ML problem, the available quantum hardware, and the specific type of quantum advantage being sought. The "suitability for NISQ/Fault-Tolerance" is a critical practical consideration. Algorithms like full Grover's search for large databases generally require fault-tolerant quantum computers to demonstrate significant advantages, whereas shallower VQAs and QA are specifically designed or adapted for the constraints of NISQ devices. Furthermore, the "type of ML problem structure addressed" is a key differentiator: QA and QAOA are often well-suited for combinatorial optimization problems that can be mapped to QUBO/Ising Hamiltonians; Grover's algorithm excels at search tasks; and quantum kernel methods aim to improve classification by mapping data into high-dimensional Hilbert spaces. This functional specialization is a central theme in the application of quantum optimization to ML [6].

The following describes a decision diagram (Figure 4) to guide the selection of a quantum optimization method for a given classical ML problem. This diagram provides a structured approach, moving beyond ad-hoc choices by considering problem structure, quantum resource availability, and desired outcomes.

Code snippet

Description of Fig. 4: The decision diagram starts with the classical ML algorithm and its core optimization task.

- QUBO/Ising Mapping: The first crucial question is whether the ML optimization problem can be effectively formulated as a QUBO or Ising model.
  - If yes, and if specialized quantum annealing hardware is available and suitable for the problem scale and structure, Quantum Annealing (QA) is a primary candidate.
  - If annealing hardware is not the target, or if a gate-based approach is preferred, QAOA or VQE can be considered if the problem Hamiltonian can be constructed.
- Search Problems: If the problem does not map well to QUBO/Ising but involves searching a large discrete configuration space for an optimal or specific solution, Grover's Algorithm or Amplitude Amplification techniques become relevant, contingent on the ability to construct an efficient quantum oracle that can identify or mark the desired solution(s).

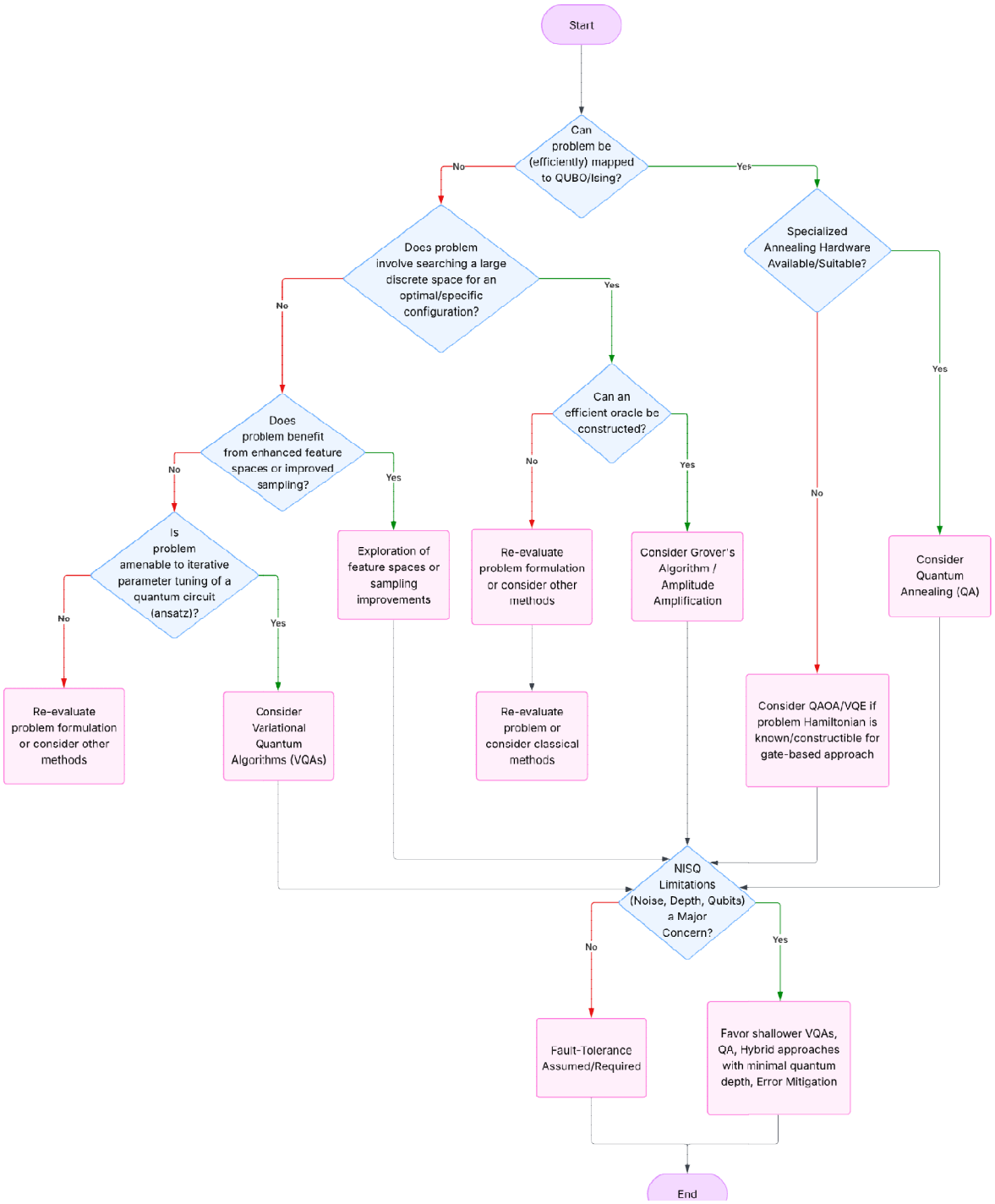


Fig. 4. Decision Diagram for Quantum Optimization Method Selection in ML Contexts.

- Feature Space Enhancement/Sampling: For ML problems that might benefit from richer feature representations or more effective sampling from complex distributions (e.g., in generative models or some types of classification), Quantum Kernel Methods or other hybrid data encoding/processing strategies (like quantum samplers) are worth exploring. These methods often leverage quantum computers to transform data or compute similarity measures in ways that are potentially hard for classical techniques.
- Variational Approaches: If the problem is amenable to an iterative, parameterized quantum circuit approach, VQAs are a general class to consider. The specific choice within VQAs depends on the problem type: QAOA is typically suited for combinatorial optimization, while VQE is designed for finding ground states or eigenvalues, which can be adapted for optimization.

- Resource Considerations: A critical overlay on these choices relates to quantum hardware capabilities.
  - If NISQ limitations (significant noise, limited circuit depth, modest qubit counts) are a dominant concern, the selection should favor algorithms that are more robust or require fewer resources. This includes shallower VQAs, QA (which is designed for specific hardware that handles noise differently), hybrid approaches that minimize the quantum portion's depth, and the incorporation of robust error mitigation strategies.
  - If fault-tolerant quantum computation is assumed or required (and available), then more complex and resource-intensive algorithms become viable, such as deeper VQAs, Grover's algorithm applied to very large search spaces, or Quantum Phase Estimation (QPE)-based methods.

The diagram leads to suggested quantum optimization methods, always accompanied by the caveat that practical utility depends on many factors including specific problem instances, data characteristics, and the maturity of the chosen quantum technology. If no clear path to a quantum approach seems viable or beneficial, a re-evaluation of the problem or reliance on classical methods is indicated.

This taxonomic framework and decision diagram are intended to provide a more systematic way to approach the selection of quantum optimization methods for classical ML, moving beyond ad-hoc choices and fostering a more principled application of these emerging technologies.

3. ALGORITHM-BY-ALGORITHM ANALYSIS OF QUANTUM OPTIMIZATION APPLICATIONS

This section provides a detailed analysis of how the quantum optimization methods identified in Section 2 are applied to each of the six target classical machine learning algorithms. For each ML algorithm, the discussion will cover its classical optimization problem, the mapping to quantum-compatible formulations, specific quantum approaches proposed in the literature, available resource estimates, reported empirical or theoretical results, and a comparative discussion against classical baselines, explicitly noting where direct comparative benchmarks are unavailable.

3.1 K-MEANS CLUSTERING

Classical k-means clustering algorithm aims to partition N data points into k distinct clusters. The core optimization objective is to find cluster assignments C_j for each data point xi and cluster centroids μ_j that minimize the within-cluster sum of squares (WCSS), also known as inertia. This is mathematically expressed as:

$$\min_{C,\mu} \sum_{j=1}^{k} \sum_{x_i \in C_j} || x_i - \mu_j ||^2 \#(3.1)$$

This problem is NP-hard, and Lloyd's algorithm is a widely used heuristic iterative approach. The NP-hard nature of k-means provides a strong motivation for exploring alternative optimization techniques, including quantum algorithms [25], [31].

Mapping to Quantum Formulation

QUBO for Balanced k-means (Quantum Annealing)[25]:

A common quantum formulation, particularly for quantum annealers, involves mapping the (often balanced) k-means problem to a QUBO. This is achieved by defining binary variables $\widehat{w}_{ij}$ which are 1 if data point x_i is assigned to cluster ϕ_j, and 0 otherwise. The objective function can be rewritten in terms of pairwise distances between points within the same cluster:

$$min_{\Phi} \sum_{j=1}^{k} \sum_{x_p, x_q \in \Phi_j} || x_p - \mu_q ||^2 \#(3.2)$$

This can be expressed in QUBO form as

$$w^T(I_k \otimes D)\hat{w}\#(3.3)$$

where

$$D_{pq} = || x_p - x_q ||^2 \ \#(3.4)$$

is the matrix of squared Euclidean distances between data points, and $\hat{w}$ is a vector of the binary assignment variables. To ensure valid clusterings, constraints are added as quadratic penalty terms to this objective function. These typically include:

1. Each data point must be assigned to exactly one cluster.
2. For balanced k-means, each cluster must contain approximately N/k data points. The final QUBO matrix A in the objective $min_{\hat{w}}\hat{w}^T A\hat{w}$ incorporates these penalties. The quality of the QUBO formulation, especially the choice of penalty factors, is crucial for obtaining meaningful solutions.

Hamiltonian for VQE/QAOA (via Max-Cut or other QUBO mappings)[32]:

The k-means problem, once formulated as a QUBO, can be mapped to an Ising Hamiltonian, making it solvable by VQAs like VQE or QAOA on gate-based quantum computers. One approach involves transforming the k-means problem (or its QUBO representation) into a weighted MAX-CUT problem, which has a natural Ising Hamiltonian formulation. The construction of this Hamiltonian, for instance, through Taylor approximations as mentioned in for VQE, directly influences the resource requirements and the quality of the solutions obtained.

Existing Quantum Approaches:

Quantum Annealing (QA)[25]: Directly solves the QUBO formulation of k-means, particularly for balanced versions. Some research approximates the QA process using Suzuki-Trotter expansions to create a QA-ST sampler for general clustering, which involves multiple parallel simulated annealing instances with quantum-inspired interaction terms to explore the solution space more effectively.

Variational Quantum Eigensolver (VQE)[32]: VQE has beencombined with classical coreset methods to tackle k-means. Coresets are small, weighted summaries of the original dataset that preserve its geometric properties, reducing the problem size N. The k-means problem on the coreset is then mapped to a weighted MAX-CUT problem, and its corresponding Hamiltonian is solved using VQE. Different orders of Taylor approximation (zeroth, first, or second) can be used in forming this Hamiltonian.

Quantum Approximate Optimization Algorithm (QAOA)[33]: QAOA is suitable for solving QUBO problems, including those derived from k-means. Hybrid QAOA approaches often decompose large QUBOs into smaller sub-QUBOs that are solvable on current NISQ devices. Ironically, classical clustering techniques like k-means are sometimes used in these hybrid schemes to group variables for constructing these sub-QUBOs.

Grover's Algorithm / Amplitude Amplification (q-means)[31]: The "q-means" algorithm, proposed by Kerenidis[34], aims to speed up a single iteration of the k-means algorithm. It leverages quantum techniques, potentially related to Grover-style search or amplitude amplification for subroutines like distance calculation or centroid updates, to achieve a runtime that is polylogarithmic in the number of data points N. A key assumption for q-means is the availability of superposition query-access to the dataset, often implying the need for Quantum Random Access Memory (QRAM).

Hybrid Quantum-Classical Workflows:

Quantum-Assisted Self-Organizing Feature Map (QASOFM)[35]: SOFMs are a type of neural network used for unsupervised clustering, related to k-means. QASOFM utilizes quantum methods for the parallel calculation of Hamming distances between input vectors and cluster vectors, aiming to accelerate the SOFM training process.

Hybrid Quantum k-Means[36]: This approach explicitly exploits quantum parallelism to accelerate distance computations in the cluster assignment step of k-means. It explores three degrees of parallelism: q1:1 (single centroid to single record distance), q1:k (single record to all centroids

distances), and qM:k (all records to all centroids distances simultaneously). This method relies on a Quantum Euclidean Distance Circuit and efficient data loading via Flip-Flop QRAM (FF-QRAM).

Resource Estimates:

Quantum Annealing (Balanced k-means QUBO): The QUBO formulation involves $O(Nk)$ binary variables. With efficient minor embedding onto the annealer's topology, this can lead to a qubit footprint that scales quadratically, roughly $O((Nk)^2)$ logical qubits, though physical qubit requirements can be much higher due to limited connectivity. The classical pre-processing time to formulate the QUBO matrix itself is $O(N^2kd)$.

VQE+Contour Coreset: The number of qubits depends on the size of the coreset and the specifics of the MAX-CUT Hamiltonian encoding. Coreset methods aim to significantly reduce N. The "Contour coreset" method is tailored for quantum algorithms. Resource details for the VQE circuit (depth, gate counts) are often specific to the experimental setup and ansatz chosen.

QAOA for sub-QUBOs: Qubit requirements are determined by the size of the largest sub-QUBO, which is chosen based on available quantum hardware capacity.

q-means[31]: While offering polylogarithmic runtime in N, this approach heavily relies on QRAM for efficient data loading in superposition. The precise qubit count, gate complexity, and oracle query complexity depend on the specific implementation details of the quantum distance calculation and state preparation subroutines, which are often not fully elaborated in terms of NISQ-era feasibility.

Hybrid Quantum k-Means: The q1:1 version uses $O\big(log(Nd)\big)$ qubits, q1:k uses $O\big(log(Ndk)\big)$, and qM:k uses $O\big(log(MNdk)\big)$ qubits, where M is the number of records processed in parallel by qM:k. A major practical challenge is the number of measurement shots required for accurate distance estimation, which can be very large and potentially negate theoretical speedups, especially as the number of encoded features or vectors increases.

Empirical/Theoretical Results:

Quantum Annealing (Balanced k-means): Early studies on D-Wave systems showed that solution quality could be comparable to classical k-means for small problem instances. However, the quantum approach scaled worse in terms of runtime, largely dominated by the classical QUBO formulation time and the embedding overhead on the annealer.

QA-ST (General Clustering): Experimental results indicated that the QA-ST sampler found better clustering assignments (lower energy solutions) compared to standard Simulated Annealing.

VQE+Contour Coreset: This approach reportedly outperforms existing QAOA+Coreset methods for k-means clustering, achieving higher accuracy (by over 10%) and lower standard deviation in results.

q-means[31]: Offers a theoretical speedup in the per-iteration cost of k-means, reducing it from $O(Ndk)$ classically to polylogarithmic in N. However, this relies on QRAM and does not account for the full end-to-end process or constant factors.

Hybrid Quantum k-Means: Simulations showed clustering results comparable to classical k-Means, provided enough measurement shots were used. Experiments on real quantum hardware (IBM) for the q1:1 version yielded reasonable results for very small datasets but suffered from prohibitive communication overhead. The q1:k version performed poorly on real hardware due to noise.

QASOFM: Claims a complexity reduction from $O(LMN)$ (classical) to $O(LN)$ (quantum-assisted) for the number of distance calculations, and an exponential decrease in the errors of the computed distance matrix with the number of quantum circuits runs.

Comparative Discussion

Classical k-means algorithms, such as Lloyd's algorithm, typically have a time complexity of $O(Nkdi)$, where i is the number of iterations. More sophisticated classical balanced k-means algorithms exist, such as the one by Malinen[25] with $O(N^3)$ complexity. Modern classical

implementations often use optimizations like k-means++ for initialization and mini-batching for scalability.

When comparing quantum approaches to these classical baselines:

- The QA approach for balanced k-means, with its $O(N^2kd)$ QUBO formulation time, is theoretically worse than optimized classical k-means ($O(Nkd)$) but potentially better than the $O(N^3)$classical balanced k-means if $kd < N$. However, empirical tests on available annealers have shown them to be slower than classical methods for the problem sizes tested, with significant overheads from QUBO generation and embedding.
- VQE+Contour Coreset claims superior accuracy over QAOA+Coreset methods. A direct, comprehensive comparison of its accuracy and end-to-end runtime against highly optimized classical k-means is needed.
- The q-means algorithm's theoretical per-iteration speedup is significant. However, the practical realization of this advantage is contingent on efficient QRAM (which is not yet available at scale) and overcoming other overheads. Its performance against state-of-the-art classical k-means variants in real-world scenarios remains undemonstrated on quantum hardware.
- Hybrid approaches like the one by Poggiali[36] and QASOFM attempt to leverage quantum parallelism for specific subroutines (e.g., distance calculations). While theoretically promising for these subroutines, they face substantial practical challenges, including the high number of shots needed for accurate quantum estimations, data loading (QRAM assumptions), and communication overheads with current quantum devices. These can often negate the theoretical speedups of the quantum sub-component when considering the entire algorithm.

A general observation is that many quantum approaches for k-means are still in the early stages of development. The dominant strategy involves reformulating k-means as a QUBO or a problem derivable from QUBO (like MAX-CUT), tailoring it to the strengths of current quantum annealers or gate-based optimizers like QAOA and VQE. This "problem-fitting" approach indicates that the path to quantum enhancement for k-means is currently viewed through the lens of established quantum optimization paradigms rather than entirely novel quantum primitives specifically designed for clustering from the ground up.

The claimed "quantum speedups" are often theoretical and localized to specific subroutines. The overall practical advantage, considering all classical pre-processing (e.g., QUBO generation, coreset construction), quantum execution (including state preparation and measurement shots), and classical post-processing, is heavily dependent on overcoming significant overheads. Hybrid strategies, particularly those combining classical coreset methods with quantum optimization or using quantum circuits for specific computational kernels within a larger classical framework , represent the most pragmatic avenues in the NISQ era. These approaches acknowledge current quantum limitations by minimizing the quantum part's burden or by tackling smaller, more manageable problem instances.

3.2. SUPPORT-VECTOR MACHINES (SVM)

Classical Support-Vector Machines are supervised learning models used for classification and regression analysis. For classification, the objective is to find an optimal hyperplane that separates data points belonging to different classes in a high-dimensional feature space, maximizing the margin between the classes while minimizing classification errors.[37] This is typically formulated as a convex quadratic programming problem. In its dual form, the problem is to maximize:

$$L_D(\alpha) = \sum_{n=1}^{N} \alpha_n - \frac{1}{2}\sum_{n=1}^{N}\sum_{m=1}^{N} \alpha_n \alpha_m y_n y_m K(x_n, x_m) \quad \#(3.6)$$

subject to the constraints $\alpha_n \geq 0$ for all n, and $\sum_{n=1}^{N} \alpha_n y_n = 0$. Here, α are the Lagrange multipliers, $y_n \in -1,1$ are the class labels, x_n are the feature vectors, and $K(x_n, x_m)$ is the kernel function that computes the inner product of the data points in a (potentially higher-dimensional) feature space[38]. Solving this optimization problem can be computationally intensive for large

datasets, with complexity scaling as $O(N^2)$ to $O(N^3)$ depending on the specific classical solver and kernel used [14].

Mapping to Quantum Formulation:

QUBO/Ising for Quantum Annealing / Coherent Ising Machines (CIMs)[14][38]: The SVM dual optimization problem can be transformed into a QUBO, making it suitable for quantum annealers and CIMs. This transformation involves several steps:

1. Binarization of Lagrange Multipliers: The continuous Lagrange multipliers αn are discretized and encoded using binary variables. A common approach is to represent each α_n as a sum of weighted binary variables:

$$\alpha_n = \sum_{k=0}^{K-1} \mathrm{B}^k a_{K_n+k} \#(3.7)$$

where $a_{K_n+k} \in 0,1$ are binary variables, K is the number of bits used for encoding (determining precision), and B is a base (e.g., 2).

2. Substitution into Objective Function: This binary representation is substituted into the SVM dual objective function.
3. Penalty Terms for Constraints: The constraints $\alpha_n \geq 0$ (implicitly handled by the binary encoding if $\mathrm{B}^k > 0$) and $\sum_n \alpha_n y_n = 0$ are incorporated into the objective function as quadratic penalty terms. For example, the equality constraint can be added as $\xi(\sum_n \alpha_n y_n)^2$, where ξ is a positive penalty coefficient. The resulting expression is a quadratic function of binary variables, which is the definition of a QUBO.

Hamiltonian for VQE/QAOA[38][27]: Once the SVM training problem is formulated as a QUBO, it can be directly mapped to an Ising Hamiltonian, which can then be solved using VQAs like QAOA or VQE on gate-based quantum computers. The Qiskit QAOA implementation, for example, directly extends the VQE structure and can take a problem Hamiltonian as input.

Quantum Kernels (for Hybrid SVMs)[39][40]: A widely explored approach involves using quantum computers to estimate kernel functions[41]. Classical data points xi are mapped to quantum states $| \Phi(x_i)\rangle$ in a high-dimensional Hilbert space using a parameterized quantum circuit (feature map $U_\Phi(x)$). The kernel matrix element K_{ij} is then computed as the overlap (or fidelity) of these quantum states: $K_{ij} = | \langle \Phi(x_i) \dagger | \Phi(x_i j) \rangle |^2$. This quantum-computed kernel matrix is subsequently fed into a classical SVM solver to find the separating hyperplane. The quantum feature map itself can be fixed or trainable (e.g., using VQCs optimized with Kernel Target Alignment (KTA)).

VQE for Direct Classification (Pattern States)[39]: An alternative VQE-based approach involves training an ansatz to produce distinct "pattern-states" for each data class. When a new, unclassified data sample is encoded into a quantum state, its similarity to these learned pattern-states can be measured (e.g., using the SWAP-Test circuit), and the sample is assigned to the class corresponding to the most similar pattern-state.

Existing Quantum Approaches

Quantum Annealing (QA) / Coherent Ising Machines (CIMs): These approaches solve the QUBO formulation of the SVM training problem.

Probabilistic QSVM Training: Proposed by He & Xiao[42], this method uses a Boltzmann distribution-based probabilistic interpretation of the solutions obtained from a CIM to better approximate the continuous Lagrange multipliers, aiming for enhanced robustness, especially for data with fuzzy boundaries. It also employs batch processing and multi-batch ensemble strategies to handle larger datasets with limited qubit counts.

Multi-Tasking Quantum Annealing (MTQA)[43]: This technique embeds multiple SVM classifiers (e.g., for a one-vs-rest strategy in multi-class SVM) in parallel onto a single quantum annealer

chip. This aims to reduce the total number of annealing cycles required compared to solving each binary classification subproblem sequentially, thereby improving computational efficiency.

Variational Quantum Eigensolver (VQE) / Variational Quantum Circuits (VQCs):

Quantum Kernel Methods[40]: VQCs are frequently used as trainable or fixed quantum feature maps to generate quantum kernels. The parameters of the VQC in trainable kernel approaches can be optimized using cost functions like Kernel Target Alignment (KTA).

Direct Classification with VQE[39]: The VQE + SWAP-Test method learns class-specific pattern states and uses the SWAP-Test to measure the similarity of new samples to these patterns for classification.

Quantum Approximate Optimization Algorithm (QAOA)[27][38]: While less prominently featured for SVMs compared to QA or quantum kernels, QAOA can, in principle, solve the QUBO formulation of SVM training if such a mapping is made. The Qiskit QAOA implementation, for instance, is an extension of the VQE structure and is designed for combinatorial optimization problems.

Grover's Algorithm / Amplitude Amplification[44]: Direct applications of Grover's algorithm to the core SVM optimization problem are not common. However, it has been proposed to optimize the weights of classical Neural Networks, a task analogous to parameter optimization. Theoretically, Grover-style search could be adapted for SVM hyperparameter optimization or for specific search-like subroutines within a more complex SVM solver, though this is not a mainstream approach for SVM training itself.

Hybrid Quantum-Classical Workflows (Primarily Quantum Kernels): This is the most prevalent paradigm for gate-based QSVMs. The quantum computer is used to calculate the kernel matrix elements, and a classical SVM solver then uses this kernel to find the decision boundary.

Classical dimensionality reduction techniques like PCA and Haar Wavelets are often applied to input data before quantum kernel computation to manage qubit requirements on NISQ devices[45].

The Nyström method[40], a classical technique for matrix approximation, has been proposed to reduce the number of quantum circuit executions needed to construct the full kernel matrix.

Resource Estimates

QA/CIM QSVM (Probabilistic): For the banknote dataset, 550 qubits were used; for the IRIS dataset, 100 qubits were employed. The number of qubits required for a QUBO-based SVM depends on the number of training samples N and the number of bits K used to encode each Lagrange multiplier α_n.

MTQA: This approach optimizes resource utilization by parallel embedding, potentially reducing the QPU runtime by a factor of C (the number of classes in a multi-class problem) compared to sequential execution of C binary classifiers.

Quantum Kernels: Qubit requirements are often dictated by the number of features in the classical data after any dimensionality reduction. For instance, studies have used 6, 10, or 14 qubits for QSVM experiments. If d features are encoded, typically d or $d/2$ qubits might be used depending on the encoding scheme (e.g., dense angle encoding).

VQE+SWAP Test: For a problem with 8 input features, 3 qubits were sufficient. The circuit depth is generally kept low for NISQ compatibility.

Empirical/Theoretical Results

QA/CIM QSVM (Probabilistic): On the banknote binary classification dataset, this approach achieved up to 20% higher accuracy compared to the original QSVM and was up to 104 times faster in training than simulated annealing methods. Its training time was reported to be comparable to or less than classical SVM. On the IRIS three-class dataset, this improved QSVM outperformed existing QSVM models across all key metrics.

MTQA: Demonstrated accuracy equivalent to classical Sequential Minimal Optimization (SMO), Simulated Annealing (SA), and standard QA methods for multi-class SVM, while significantly improving computational efficiency by reducing QPU runtime.

Quantum Kernels:

Performance is highly dataset dependent. Benchmarking studies often show that classical ML models (like classical SVM) still exhibit superior predictive capability on many datasets. For example, on the CLBtope dataset, QSVM (14 qubits) achieved an AUC of 0.68, while CML reached 0.82. However, on the HemoPI dataset, QSVM achieved an AUC of 0.95, close to CML's 0.98, and sometimes showed a better F1-score and MCC.

QSVC and Pegasos QSVC (PQSVC) have shown effectiveness in detecting buggy software commits, with an aggregation technique allowing application to larger datasets by processing smaller subsets.

Hybrid QSVMs combined with classical dimensionality reduction (PCA, Haar Wavelet) have demonstrated consistent and sometimes improved performance compared to classical SVMs, especially when Haar transform was used.

A quantum hybrid SVM for stress detection reported improved accuracy and higher recall values compared to classical methods when using a limited number of features.

Trainable quantum feature mapping for QSVMs has shown considerable clustering performance and subsequent classification performance superior to existing quantum classifiers in terms of accuracy and distinguishability in simulations.

VQE+SWAP Test: Achieved 100% accuracy on a credit sales dataset, presented as a simpler and more compact solution compared to classical SVM or Random Forest models for that specific task.

General QSVM Speedups: Theoretical works, particularly early ones based on HHL algorithm for solving the linear system in SVM training, proposed exponential speedups. More recent work by Gentinetta[46] also proved that variational quantum circuits can offer provable exponential speedups in training QSVMs under certain conditions. However, realizing these speedups in practice is challenging due to data loading, readout complexities, and the specific conditions required for the speedup to manifest.

Comparative Discussion

Classical SVM solvers, such as those using Sequential Minimal Optimization (SMO), are well-established and highly optimized.

Quantum vs. Classical:

Quantum annealer and CIM-based QSVMs, especially when enhanced with probabilistic methods or multi-tasking, show promise in matching or even exceeding classical SVMs in speed and accuracy for certain problem scales and types.

Quantum kernel methods, the most common approach for gate-based QSVMs, do not yet consistently outperform well-tuned classical SVMs on general datasets. The potential for "quantum advantage" via kernels hinges heavily on the design of the quantum feature map and the specific characteristics of the dataset. Finding feature maps that are both classically hard to simulate and genuinely beneficial for classification remains a key research challenge.

VQE-based direct classification methods have shown effectiveness for smaller, specific problems.

Many historical claims of exponential speedups for QSVMs (e.g., those based on the HHL algorithm) face significant practical caveats related to efficient data loading (QRAM assumption), quantum state readout, and specific requirements on the data or kernel matrix (e.g., sparsity, condition number).

The field of QSVM is characterized by two primary developmental thrusts. The first involves reformulating the classical SVM optimization problem into a QUBO, making it amenable to solution by quantum annealers, CIMs, or potentially QAOA/VQE. The second, more extensively researched for gate-based quantum computing, focuses on leveraging quantum circuits to compute kernel functions. The "quantum kernel trick" is central here, with the promise of accessing feature spaces that are classically intractable. However, the practical realization of a consistent quantum advantage through these kernels is not yet universally established and is highly dependent on the specific quantum feature map employed and the dataset's intrinsic structure. Identifying feature maps that are both difficult for classical computers to simulate and genuinely advantageous for classification tasks is an ongoing and critical area of research.

Hybridization is an almost universal characteristic of practical QSVM approaches. Even for QUBO-based methods, classical pre-processing (like the binary encoding of Lagrange multipliers) and post-processing (such as the probabilistic interpretation of solutions) are standard. In quantum kernel methods, the quantum processor computes the kernel, but a classical computer performs the subsequent SVM optimization using this kernel. This deep intertwining of quantum and classical resources underscores the pragmatic nature of current QML research.

Scalability remains a formidable challenge for QSVMs, particularly for methods that require the computation of the full kernel matrix, as this scales quadratically with the number of data samples (N^2 kernel entries). Consequently, classical techniques such as data subsampling, feature reduction via PCA or Haar wavelets, or kernel matrix approximation methods like the Nyström technique are actively being explored as essential classical workarounds to make QSVMs more tractable for larger datasets on resource-constrained quantum devices[47].

3.3. DECISION TREES

Classical Decision Tree construction involves recursively partitioning the dataset into subsets based on feature values to create a tree structure where leaves represent class labels (for classification) or continuous values (for regression). The optimization problem at each node is to select the best feature and split point (or splitting hyperplane for oblique trees) that maximizes a certain criterion, such as information gain, Gini impurity reduction, or variance reduction. Finding the globally optimal decision tree is an NP-hard problem. Heuristic greedy algorithms like CART, ID3, and C4.5 are commonly used[48].

Mapping to Quantum Formulation

- QUBO for Optimal Tree Splitting (QUBO Decision Tree)[49]: The training process, particularly the selection of optimal decision rules (splits), can be extended to multi-dimensional boundaries and transformed into a QUBO problem. This allows an annealing machine to find optimal splits that might be computationally prohibitive for classical exhaustive search. The binary variables in the QUBO would represent choices of features, thresholds, or parameters defining more complex (e.g., oblique or multi-dimensional) splits. The objective function would encode the quality of the split (e.g., maximizing impurity reduction).
- Quantum Supervised Clustering for Splits (Des-q)[48][50]: The Des-q algorithm uses a quantum-supervised clustering method, based on q-means, to determine suitable anchor points for piecewise linear splits, generating multiple hyperplanes at each node. This implicitly maps the splitting problem to a quantum routine.
- Hamiltonian for QAOA/VQE (if tree construction sub-problems are QUBOs)[51]: If parts of the tree construction (e.g., optimal split finding) are formulated as QUBOs, then QAOA or VQE could be applied to these sub-problems by converting the QUBO to an Ising Hamiltonian.

Existing Quantum Approaches

Quantum Annealing (QA):

QUBO Decision Tree[26]: Yawata proposed extending regression trees by formulating the decision rule optimization (allowing multi-dimensional boundaries) as a QUBO solvable by quantum annealers.

Feature Selection for Trees[14]: While not directly tree optimization, QA can be used for feature selection (formulated as MIQUBO), which is a crucial pre-processing step for decision tree construction.

Variational Quantum Eigensolver (VQE) / Variational Quantum Circuits (VQCs):

VQE for Classification Tasks (General)[39]: VQE combined with methods like the SWAP-Test has been used for general classification tasks , which could, in principle, be a component in a decision tree's leaf node prediction or a way to evaluate split quality if the sub-problem is mapped to a Hamiltonian. However, direct application of VQE to optimize the tree structure itself is less documented.

Quantum Decision Tree with Information Entropy[52]: A classical algorithm using quantum measurement results as inputs, inspired by decision trees, to classify quantum states. It optimizes measurement schemes using conditional probabilities and information gain. This is more about classifying quantum states using a tree-like decision process than optimizing a classical decision tree with quantum computation.

Quantum Approximate Optimization Algorithm (QAOA):

QAOA can solve QUBO problems, so if decision tree splitting is formulated as a QUBO, QAOA is a candidate solver. Some works propose QAOA for solving general Boolean problems as Hamiltonians, which could encompass decision rules.[53]

Machine learning-assisted error mitigation for QAOA has been explored for problems like MaxCut, indicating approaches to improve QAOA performance which could be relevant if applied to tree-derived QUBOs.[53]

Grover's Algorithm / Amplitude Amplification:

Speeding up Tree Construction[48][54]: Early proposals suggested using Grover's search to speed up finding the best split (feature and threshold) in classical decision tree construction algorithms, potentially offering a quadratic speedup in the number of features or possible thresholds.

Binary Quantum Neural Network with Optimized Grover[55]: A QNN classification model using an optimized Grover algorithm for retrieving quantum states with similar features has been proposed, which shares conceptual similarities with decision-making processes.

Hybrid Quantum-Classical Workflows:

Des-q Algorithm[50][48]: A quantum algorithm for constructing and retraining decision trees for regression and binary classification. It uses quantum-supervised clustering (based on q-means) for piecewise linear splits. It claims logarithmic complexity for retraining with new data batches, assuming data is in quantum-accessible memory (e.g., KP-tree).

Quantum Reservoir Computing for Decision Tree Ensembles[56]: A hybrid approach where Quantum Reservoir Computing (QRC) enhances feature extraction for a classical decision tree-based ensemble model.

QuXAI Framework[57]: While focused on explainability, this framework involves HQML models with quantum feature maps whose outputs could be fed into classical decision tree learners.

Resource Estimates

QUBO Decision Tree: The number of QUBO variables would depend on the number of features considered for multi-dimensional splits, the number of possible thresholds, and the complexity of the boundary parameterization.

Des-q: Assumes QRAM (e.g., KP-tree data structure). The retraining complexity is logarithmic in the total number of samples N,$\mathrm{O}\left(\mathrm{poly}\log(\mathrm{Nd})\right)$ for algorithmic steps after data

loading/update. Qubit requirements for q-means depend on the data dimension and number of clusters.

Grover-based Split Search: Would require qubits to represent features and thresholds, and an oracle to evaluate split quality. Query complexity is $O(\sqrt{S})$ where S is the search space size (e.g., number of features times number of thresholds).

Quantum Decision Tree (for quantum state classification): Resource needs depend on the number of candidate states and observables.

Empirical/Theoretical Results:

QUBO Decision Tree: The proposal suggests annealing machines can solve the extended multi-dimensional boundary problem, which is generally unimplementable classically due to computational limits. Performance implications (accuracy vs. classical trees like CART) are not detailed in the abstracts.

Des-q: Benchmarking of a simulated version against state-of-the-art classical methods on multiple datasets showed similar performance in terms of accuracy for regression and binary classification, while offering significant speedup in periodic tree retraining.

Grover-based Split Search: Theoretical quadratic speedup for the split finding subroutine. Practical impact on overall tree construction time and quality compared to highly optimized classical heuristics (which don't search exhaustively) is less clear.

Quantum Decision Tree (for quantum state classification): Effectively identifies Haar random quantum states and classifies ground states of Hamiltonians, outperforming non-information-optimized measurement schemes on simulators and quantum computers. However, it faces challenges similar to barren plateaus (information gain exponentially suppressed with system size for random states).

General VQC/QSVC on Iris dataset (compared to classical RF/SVM): provide a comparison, but this is for general classifiers, not specifically quantum-optimized decision tree structures.

Comparative Discussion

Classical decision tree algorithms like CART are greedy and do not guarantee global optimality but are computationally efficient for many datasets.

Quantum vs. Classical:

QUBO Decision Trees: Aim to find more optimal, potentially complex (multi-dimensional) splits than classical greedy methods by leveraging annealers for a hard combinatorial search. The key question is whether the improved split quality translates to significantly better overall tree performance (accuracy, generalization) to justify the overhead of QUBO formulation and annealing. No public benchmark available for direct classical vs. quantum comparison as of May 2025.

Des-q: Focuses on retraining speedup for streaming data, claiming logarithmic complexity versus polynomial for classical retraining, while maintaining comparable accuracy. This is a significant potential advantage if QRAM and efficient quantum-supervised clustering are realized.

Grover-based split search: Offers a theoretical speedup for a subroutine. However, classical tree heuristics are already very fast and often employ sampling or other tricks to avoid exhaustive search. The practical benefit of Grover's speedup here needs careful evaluation against advanced classical tree builders.

The "Quantum Decision Tree" for quantum state classification is a distinct concept, applying decision tree logic to quantum measurement strategy rather than using quantum computers to optimize classical decision trees.

The application of quantum optimization to decision trees is less mature compared to SVMs or k-means. The primary avenues explored are using QUBO formulations for more complex split optimization and leveraging quantum subroutines (like q-means in Des-q or Grover for search) to accelerate parts of

the tree construction or retraining process. The Des-q algorithm represents a notable development, particularly for the scenario of retraining decision trees with streaming data, by promising a significant reduction in computational complexity for the retraining phase, contingent on efficient quantum data access. The QUBO Decision Tree approach attempts to improve the expressive power of individual splits.

A critical challenge for Grover-based approaches is that classical decision tree construction often relies on heuristics that are already very efficient for finding "good enough" splits, rather than globally optimal ones. Demonstrating a practical advantage requires outperforming these highly optimized classical heuristics in terms of overall tree quality or speed. For QUBO-based approaches, the overhead of formulating the QUBO and the limitations of current annealers in terms of size and precision are key considerations.

3.4. ANDOM FORESTS

Classical Random Forest is an ensemble learning method that constructs multiple decision trees at training time and outputs the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees. The "optimization" in Random Forests primarily involves:[58]

1. Building individual decision trees, each typically using a random subset of features and bootstrapped samples from the training data. The optimization within each tree is as described in Section 3.3 (finding good splits).
2. Hyperparameter tuning for the forest (e.g., number of trees, tree depth, features per split). The ensemble nature helps to reduce overfitting and improve generalization compared to a single decision tree. Retraining Random Forests with new data, especially in streaming settings, can be computationally intensive as it often involves rebuilding many or all trees[50].

Mapping to Quantum Formulation:

Since Random Forests are ensembles of decision trees, quantum approaches primarily target the optimization or acceleration of the individual tree construction or retraining, as detailed in Section 3.3.

Leveraging Quantum Decision Tree Algorithms: If a quantum algorithm can build or retrain individual decision trees more effectively or efficiently (e.g., Des-q for retraining, QUBO Decision Tree for potentially better splits), this could be applied to each tree in the forest.

QUBO for Feature Selection / Learner Weighting (QBoost-inspired)[59]: For ensemble methods like boosting (related to Random Forests in spirit), the problem of selecting and weighting weak learners (which can be decision trees) can be formulated as a QUBO problem. This is seen in quantum-enhanced classifiers inspired by QBoost, where binary weights for combining weak learners are optimized via QUBO solved on a neutral atom QPU. This is not directly Random Forest optimization but shows a path for quantum optimization in tree ensembles.

Existing Quantum Approaches:

QC-Forest (Quantum-Classical Forest):

An extension of the Des-q algorithm (see Section 3.3) to Random Forests for multi-class classification and regression[50]. It aims for time-efficient retraining in streaming data settings by achieving poly-logarithmic runtime in the total number of accumulated samples. It expands Des-q to handle multi-class classification by using the η coefficient for feature weight estimation and a novel method for estimating class probabilities in leaf nodes. It also introduces an exact classical method to replace a quantum subroutine from Des-q for feature weight calculation, maintaining the speedup.

Quantum Subroutine: Leverages the supervised quantum k-means algorithm from Des-q for tree construction.

Grover's Search for Tree Construction in RF:

Previous quantum algorithms have targeted speeding up the underlying tree construction in RF models using Grover's search, aiming for a quadratic improvement based on the number of features (d). This focuses on accelerating the split finding process within each tree[50].

Quantum-Enhanced Classifier (QBoost-inspired for Neutral Atoms):

While not strictly a Random Forest, this approach uses a neutral atom QPU to solve a QUBO for optimizing the weights of an ensemble of weak decision tree classifiers. This demonstrates a method for quantum optimization of tree ensemble parameters[59].

Hybrid Quantum-Classical Random Forest (General Integration):

Some works mention integrating quantum optimization with Random Forest classifiers as part of a broader hybrid workflow[60]. For example, using K-Means clustering (potentially quantum-enhanced) and Random Forest classifiers in conjunction with quantum optimization for problems like TSP. Another example involves using Quantum Long Short-Term Memory layers with classical dense layers and comparing this HQRNN against classical Random Forest among other baselines for time-series forecasting. These are often comparisons or integrations rather than direct quantum optimization of the Random Forest itself.

Resource Estimates:

QC-Forest: Relies on Des-q's resource requirements for individual trees. The key is the poly-logarithmic retraining time in N (total samples) after initial (slower) KP-tree construction. The classical replacement for feature weight calculation avoids quantum resources for that specific step.

Grover-based Tree Construction: Query complexity for split finding in each tree would be $O(\sqrt{S_d})$, where S_d is the search space for splits is based on d features. Qubit requirements depend on encoding features and thresholds.

QBoost-inspired Classifier: For optimizing 50-qubit sized QUBOs (representing 50 weak learners).

Empirical/Theoretical Results:

QC-Forest:

Achieves competitive accuracy compared to state-of-the-art classical Random Forest methods on benchmark datasets up to 80,000 samples for regression, binary, and multi-class classification.

The primary advantage is the significant speedup in model retraining time (poly-logarithmic in N) in streaming settings.

Grover's Search for Tree Construction: Offers a theoretical quadratic speedup in the number of features d for the tree construction subroutine. The impact on overall forest quality and total training time versus classical RF heuristics is not fully established.

QBoost-inspired Classifier: Achieved performance competitive with a state-of-the-art Random Forest benchmark in a financial risk classification task, with better interpretability (fewer learners) and comparable training times on neutral atom hardware. Tensor network simulations suggest potential to outperform classical RF with hardware improvements.

General Hybrid Models (Comparison): In some comparative studies, classical Random Forests serve as a benchmark against which new hybrid quantum models are tested (e.g., HQRNN in, VQC/QSVC in). These often show classical RFs as strong contenders.

Comparative Discussion:

Classical Random Forests are known for their robustness, ease of use, and strong performance across many tasks. They are often hard to beat with more complex models, especially on tabular data.

Quantum vs. Classical:

QC-Forest: The main value proposition is not necessarily outperforming classical RF in accuracy but achieving comparable accuracy with a provable and significant speedup in the retraining

phase for streaming data. This addresses a key operational challenge for classical RFs in dynamic environments.

Grover-based RF: The theoretical speedup in feature selection for splits needs to translate into a practical end-to-end advantage. Classical RFs use feature subsampling and efficient heuristics, so a quadratic speedup on an exhaustive search might not be directly comparable or lead to better trees.

QBoost-inspired: Shows that quantum optimization (via annealer-like computation on neutral atoms) can build competitive tree ensembles, particularly excelling in interpretability and potentially training time. This is a promising direction for alternative ensemble construction.

The application of quantum optimization to Random Forests is largely an extension of techniques developed for individual decision trees, with QC-Forest being the most direct example. The focus is less on finding a "more optimal" forest in terms of raw predictive power and more on addressing computational bottlenecks like retraining or potentially creating more interpretable ensembles. The QBoost-inspired approach, while not a Random Forest, demonstrates that quantum hardware can optimize the combination of multiple decision tree learners, which is a core concept in ensemble methods.

The challenge for quantum-enhanced Random Forests is to demonstrate value beyond what highly optimized classical RF implementations (which include many heuristics for speed and accuracy) can already achieve. For QC-Forest, the key is the retraining efficiency, which could be very impactful if the QRAM assumption and efficient quantum clustering subroutines are practically realized.

3.5. LINEAR/LOGISTIC REGRESSION

Classical Linear/Logistic Regression Optimization Problem:

Linear Regression: Aims to model the linear relationship between a dependent variable y and one or more independent variables X. The optimization problem is typically to find the coefficients β that minimize the sum of squared residuals:

$$min_{\beta} \; || \; y - X\beta \; ||^2 \; \#(3.8)$$

This has a closed-form solution:

$$\beta = (X^T X)^{-1} X^T y \#(3.9)$$

if $X^T X$ is invertible, but iterative methods like gradient descent are used for large systems or variations like Ridge/Lasso regression.

Logistic Regression: Aims to model the probability of a binary outcome. The optimization problem involves finding parameters β that maximize the likelihood function (or minimize the negative log-likelihood, often the cross-entropy loss) for a logistic function

$$P(\, y = 1 \mid X \,) = 1/\left(1 + e^{-X} \; \right) \#(3.10)$$

This is typically solved using iterative methods like gradient descent or Newton's method, as there's no general closed-form solution[61].

Mapping to Quantum Formulation:

Quantum Linear System Solvers (HHL and variants) for Linear Regression[6]: The core of the least-squares linear regression solution involves solving the linear system

$$(X^T X)\beta = X^T y \#(3.11)$$

The HHL algorithm and its derivatives can potentially solve linear systems

$$Az = b \#(3.12)$$

with exponential speedup in the dimension of A under certain conditions (e.g., A is sparse, well-conditioned, and b can be efficiently prepared as a quantum state). The solution β would be encoded in the amplitudes of a quantum state.

QUBO for Linear/Logistic Regression (Parameter Discretization)[62]: To solve regression problems on quantum annealers or with QAOA/VQE, the continuous regression parameters

β_j must be discretized and represented by binary variables. For instance, each β_j can be written as:

$$\beta_j = \sum_k c_k \, b_{jk} \#(3.13)$$

where b_{jk} are binary variables and c_k are fixed coefficients (e.g., powers of 2 for binary expansion). Substituting these into the loss function (e.g., squared error for linear regression, or a polynomial approximation of log-likelihood for logistic regression) and expanding terms can lead to a QUBO formulation.

Variational Quantum Circuits for Regression (Direct Parameter Fitting or Quantum Gradients)[61]:

A PQC can be designed where the output (e.g., expectation value of an observable) represents the predicted value $\hat{y}$ or log-odds. The parameters of the PQC are then optimized to minimize a classical loss function (e.g., MSE for linear, cross-entropy for logistic) with respect to the training data.

Quantum algorithms can be used to estimate gradients of the loss function for iterative optimization.

Quantum Annealing with Continuous Variables (Bosonic Systems) [62]: A novel approach for linear regression using QA with continuous variables directly, leveraging boson systems and coherent states, avoiding discrete approximations. The parameters θ_m correspond to amplitudes of coherent states.

Existing Quantum Approaches

Quantum Annealing (QA):

QUBO-based: Used for linear regression where parameters are approximated by discrete binary values.

Continuous Variable QA[62]: A newer method using boson systems to handle continuous regression parameters directly, potentially ensuring accuracy without increasing qubits if adiabatic conditions are met.

Variational Quantum Algorithms (VQAs) - QAOA/VQE:

If regression is formulated as a QUBO, QAOA/VQE can be applied[63][7].

VQAs can be used more directly by parameterizing a quantum circuit whose output is used in a regression model, with classical optimization of circuit parameters.

Grover's Algorithm / Amplitude Amplification:

Quantum Amplitude Estimation for Linear Regression[64]: Kaneko proposed using QAE to calculate terms in the classical least squares solution (elements of $X^T X$ and $X^T y$), overcoming bottlenecks in summing over data points. This is a hybrid approach.

Bisection Grover's Search (BGS) for Best Subset Selection[65]: While applied to CITE-seq data analysis (model selection), the principle of using BGS for finding optimal subsets of features/parameters could be relevant for feature selection in regression models.

Hybrid Quantum-Classical Neural Networks (HQNN) for Regression:

HQNN-FSP[66]: A hybrid classical-quantum neural network for regression-based financial stock market prediction. It uses a custom QNN regressor with a novel ansatz, exploring sequential (classical RNN/LSTM feature extraction then quantum processing) and joint learning optimization strategies.

Quantum Algorithm for Logistic Regression:

Uses amplitude estimation and swap test to obtain classical gradients for the gradient descent method in logistic regression[61].

Resource Estimates

HHL-based Linear Regression: Logarithmic dependence on N (number of data points) and polynomial in d (features) and κ (condition number). Qubit count $O(\log N + \log d)$. However, reading out the full solution vector is a major challenge.

QUBO-based Regression (QA): Qubit count depends on the number of regression parameters and the bits of precision used for each. For P parameters each with K bits, roughly PK binary variables.

Continuous Variable QA (Bosonic): Aims to ensure accuracy without increasing qubit count for higher precision, relying on properties of coherent states.

QAE for Linear Regression[64]: Complexity $O(\epsilon^{-1})$ for error ϵ, logarithmic in N_D. Query complexity depends on d, κ, ϵ.

Quantum Logistic Regression[61]: Achieves exponential speedup in each gradient calculation iteration if $M = O(\text{polylog}N)$ (M features, N data points).

HQNN-FSP: Qubit count depends on the QNN regressor design, e.g., number of features input to the quantum layer.

Empirical/Theoretical Results:

HHL-based: Theoretical exponential speedup, but practical utility hampered by strict conditions, data loading/readout, and sensitivity to condition number κ. Recent work revisits these algorithms aiming for quadratic speedups without κ-dependence by using leverage score sampling.

Continuous Variable QA (Linear Regression): Proposed to ensure accuracy without increasing qubit count for precision, as long as adiabatic condition is satisfied.

QAE for Linear Regression [64]: Achieves $O(\epsilon^{-1})$ complexity for obtaining regression coefficients, an improvement over prior $O(\epsilon^{-2})$ quantum proposals. Keeps logarithmic dependence on N_D.

Quantum Logistic Regression[61]: Theoretical exponential speedup per iteration under specific dimensionality conditions ($M = O(\text{polylog}N)$).

HQNN-FSP: Hybrid models integrate quantum computing into financial forecasting workflows. While showing how quantum-assisted learning can contribute, classical models like LSTM still often achieve lower RMSE in benchmarks. Quantum models struggled with rapid market changes.

General Benchmarking (Variational Quantum Algorithms): Comprehensive benchmarks comparing VQAs and classical models for time series forecasting (related to regression) indicate that quantum models often struggle to match the accuracy of simple classical counterparts. AutoQML frameworks aim to generate competitive QML pipelines for regression and classification, sometimes matching manually crafted quantum solutions or classical ML[8].

Comparative Discussion:

Classical linear and logistic regression are foundational ML algorithms with highly optimized solvers.

Quantum vs. Classical:

HHL-based approaches: While offering tantalizing theoretical speedups, the strict requirements (sparse, well-conditioned matrix A, efficient state preparation of vector b, and efficient readout of solution vector x) have limited their practical impact on classical ML regression tasks to date. The "dequantization" of some QML algorithms has also shown that classical algorithms inspired by quantum ones can sometimes achieve similar performance without needing a quantum computer. The shift towards leverage score sampling methods attempts to make speedups more robust.

QUBO-based approaches (QA): Transforming regression into QUBO requires discretization of parameters, which can limit precision unless many bits are used (increasing qubit cost). The

continuous variable QA approach is an interesting attempt to mitigate this but is still in early research.

Gradient-based quantum approaches (e.g., for Logistic Regression): The speedup often relies on efficient quantum estimation of gradients or parts of the gradient calculation. The overall speedup depends on the number of iterations and the cost of each quantum step versus its classical counterpart.

Hybrid NNs (HQNN-FSP): Current results suggest that while quantum layers can be integrated, they do not yet consistently outperform state-of-the-art classical deep learning models for complex regression tasks like financial forecasting. The quantum component may offer different feature representations, but translating this into superior predictive power is an ongoing challenge.

Benchmarking: General benchmarks for variational quantum algorithms often show them lagging behind classical methods in accuracy for regression-like tasks.

The application of quantum optimization to linear and logistic regression is multifaceted. Early excitement around HHL-based speedups for linear regression has been tempered by practical limitations regarding data input/output and specific problem constraints. Current research explores several avenues: reformulating regression as QUBOs for annealers (with challenges in parameter discretization), using VQAs to learn regression models (where the quantum circuit acts as the model or aids gradient computation), and hybrid approaches like QAE for accelerating classical calculations or HQNNs combining classical and quantum neural network components.

The continuous variable QA approach is a noteworthy recent development attempting to sidestep the precision issues of binary representations of continuous parameters on annealers. For logistic regression, quantum methods for accelerating gradient calculations could be impactful if the speedup per iteration offsets the overheads and number of iterations required. However, for both linear and logistic regression, demonstrating a clear, practical quantum advantage over highly optimized classical solvers (which are often very fast and scalable for these "simpler" ML models) remains a significant hurdle. The overhead of quantum computation, data loading, and the current scale and noise levels of quantum hardware are major factors [62][61].

3.6. MARKOV DECISION PROCESSES (MDPS)

Classical Markov Decision Process Optimization Problem: A Markov Decision Process (MDP) provides a mathematical framework for modeling sequential decision-making under uncertainty. An MDP is defined by a tuple (S, A, P, R, γ), where S is a set of states, A is a set of actions, $P(s' \mid s, a)$ is the transition probability function, $R(s, a, s')$ is the reward function, and γ is a discount factor. The goal in an MDP is to find an optimal policy $\pi *: S \rightarrow A$ that maximizes the expected cumulative discounted reward (value function) starting from any state s: $V^{\pi}(s) = E_{\pi}$ This is often solved using dynamic programming (e.g., Value Iteration, Policy Iteration) or reinforcement learning (RL) algorithms (e.g., Q-learning, SARSA, policy gradient methods)[67][68].

Mapping to Quantum Formulation:

Quantum State and Action Spaces (q-MDPs)[69]: Saldi propose a general formulation of quantum MDPs (q-MDPs) where state and action spaces are in the quantum domain (sets of density operators on Hilbert spaces $\mathrm{H_X}$ and $\mathrm{H_X} \otimes \mathrm{H_A}$ respectively). Transitions are quantum channels, and cost functions are linear functions on density operators. This is a foundational theoretical framework.

Encoding Value Functions in Superposition (Q-Policy)[68]: The Q-Policy framework encodes action-value functions (Qπ(s,a)) in quantum superposition using amplitude encoding. This allows for simultaneous evaluation and Bellman updates for multiple state-action pairs.

QUBO for Policy Search or Sub-problems: If specific optimization sub-problems within an MDP solver (e.g., finding an optimal action given a state-value function under constraints, or certain

planning problems) can be formulated as combinatorial optimization, they could potentially be mapped to QUBOs for quantum annealers or QAOA[70]. For example, test case mutation for cyber-physical systems, related to exploring state-action spaces, has been encoded as a QUBO for QA[71].

Hamiltonian for VQE/QAOA (if policy optimization is cast as ground state search): If the policy optimization problem can be mapped to finding the ground state of a Hamiltonian (e.g., via a QUBO representation of a value function or policy parameters), VQE or QAOA could be applied.

Existing Quantum Approaches:

Quantum Annealing (QA):

Mutation-based Test Case Generation for CPS (related to MDP exploration)[71]: QA used to solve a QUBO formulation for identifying critical regions of test cases (trajectories in state-action space) to mutate, aiming for efficient test generation. This is an indirect application to MDP-like problems.

Variational Quantum Eigensolver (VQE) / Variational Quantum Circuits (VQCs):

Reinforcement Learning for VQE Architecture Optimization: While not solving MDPs directly, RL (which is based on MDPs) has been used to optimize VQE ansatz structures. This is a meta-application.

Parameterized Quantum Circuits in QRL (PQC-QRL)[7]: Quantum circuits with trainable parameters are used as policy or value function approximators in RL. Policy gradient (QPG) and Q-Learning (QDQN) algorithms have quantum versions using PQCs.

Quantum Approximate Optimization Algorithm (QAOA):

Problem-Structure-Informed QAOA for Unit Commitment (related to scheduling MDPs)[70]: QAOA used to solve QUBO formulations of large-scale scheduling problems (like Unit Commitment Problem, UCP), which can be modeled as MDPs. Novel decomposition methods are used to handle large problem sizes.

Recursive QAOA (RQAOA) with RL Enhancement: RQAOA, a non-local variant of QAOA, has been enhanced using RL to improve selection rules and parameter training for solving combinatorial optimization problems that could arise from MDPs.

Grover's Algorithm / Amplitude Amplification:

Quantum Dyna Q-Learning[67]: Uses amplitude amplification (Grover operator) for action selection within a Dyna-Q framework, where the model of the environment is a superposition of experiences.

Amplitude Amplification based QRL (AA-QRL): One of the major classes of QRL algorithms benchmarked in.

Hybrid Quantum-Classical Workflows:

General q-MDP Theory[69]: Provides a verification theorem for Markovian quantum control policies and a dynamic programming principle. Discusses approximations via finite-action models (QOMDPs) and classes of open-loop and classical-state-preserving closed-loop policies.

Q-Policy Framework[68]: Hybrid quantum-classical RL framework using quantum superposition and amplitude encoding for accelerated policy evaluation. Combines quantum Bellman updates with classical policy improvement.

POMDPs for Hybrid Quantum Algorithm Synthesis: Partially Observable MDPs (POMDPs) used as a classical framework to compute accuracy and synthesize optimal hybrid quantum algorithms with classical branching.

Free Energy based QRL (FE-QRL): Another class of QRL algorithms compared in, often involving concepts from quantum statistical mechanics.

Game-Solving Benchmarks (QCNNs): Hybrid classical-quantum CNNs (QCNNs) benchmarked against classical CNNs for game-solving (Tic-Tac-Toe), where the game can be modeled as an MDP.

Resource Estimates:

q-MDPs (Theoretical): Resource needs depend on the dimensionality of Hilbert spaces $\mathrm{H_X}$,$\mathrm{H_A}$. Finite-action approximations can map to QOMDPs with known complexities.

Q-Policy: Quantum subroutines (Amplitude Preparation, Quantum Bellman Update, Amplitude Estimation) have polynomial gate complexities and query complexities (e.g., $\mathrm{O}(1/\epsilon)$ for AE vs $\mathrm{O}(1/\epsilon^2)$ classically) under sparsity and spectral norm assumptions. Qubit count depends on encoding state-action space, potentially logarithmic via amplitude encoding.

PQC-QRL: Qubit count depends on state/action encoding and ansatz depth. The number of circuit executions can be high for training.

Quantum Dyna Q-Learning: Qubit count for storing experiences in superposition ($|\,\mathrm{sj}\rangle\,|\,\mathrm{aj}\rangle\,|\,\mathrm{rj}\rangle\,|\,\mathrm{sj'}\rangle$). Grover iterations for action selection add to circuit depth.

QA for Test Case Mutation: Qubit count depends on the QUBO size derived from the test case representation.

Empirical/Theoretical Results:

q-MDPs[69]: Established verification theorem for Markovian quantum policies and dynamic programming. Showed convergence of finite-action approximations.

Q-Policy: Provable polynomial reductions in sample complexity for policy evaluation ($\mathrm{O}(\epsilon^{-1})$ vs$\mathrm{O}(\epsilon^{-2})$). Theoretical complexity bounds established for quantum subroutines. Global convergence guarantees.

QA for Test Case Mutation: Showed quantum annealing can generate test cases more efficiently (faster) with similar fault detection rates compared to alternatives for CPS.

Problem-Structure-Informed QAOA (for UCP): Proposed methodology for large-scale UCP solutions via decomposition, enabling use of limited qubits.

RL-RQAOA: Converges faster and to better solutions than entirely classical RL agents for certain combinatorial problems.

Quantum Dyna Q-Learning: Theoretical framework combining Dyna-Q with quantum model and amplitude amplification for action selection.

- Benchmarking QRL (PQC-QRL, FE-QRL, AA-QRL):
  - PQC-QRL showed minor dependence on entanglement.
  - FE-QRL performance depended more on hyperparameters than number of replicas.
  - Suggests that many QRL approaches may not heavily rely on their quantum components for observed performance in benchmarked gridworld environments.

Game-Solving with QCNNs: Hybrid classical-quantum model achieved Elo ratings comparable to classical CNNs in Tic-Tac-Toe, while standalone QCNN underperformed under current hardware constraints.

Comparative Discussion

Classical MDP solvers (dynamic programming, RL) are well-developed with numerous algorithms and strong theoretical foundations.

Quantum vs. Classical:

q-MDP Framework: Provides a rigorous quantum generalization of classical MDP theory, opening avenues for new types of quantum control policies and algorithms. The key question is whether operating in quantum state/action spaces offers tangible advantages beyond classical probabilistic models.

Q-Policy: Offers theoretical polynomial speedups in sample complexity for policy evaluation by leveraging quantum parallelism and amplitude encoding. This could be significant for MDPs with very large state-action spaces where classical sampling is a bottleneck. Practical

realization depends on efficient implementation of the quantum subroutines on fault-tolerant hardware.

PQC-based QRL: These are direct quantum analogues of classical neural network-based RL. Current benchmarks suggest their performance advantage over classical RL is not yet clear, and observed benefits might not always stem from uniquely quantum properties. Challenges include barren plateaus, training difficulties, and data encoding.

Amplitude Amplification in RL (Dyna QRL, AA-QRL): Using Grover-like speedups for specific subroutines like action selection or as a general QRL approach is a promising direction, but the quadratic speedup needs to overcome overheads of oracle construction and quantum circuit execution.

QA for MDP-related problems: Applying QA to QUBOs derived from specific MDP sub-problems (like scheduling or test generation) shows some promise for optimization tasks that can be framed appropriately. This is more about using QA as an optimizer for parts of an MDP solution process.

The application of quantum optimization to MDPs is diverse, ranging from foundational theoretical frameworks (q-MDPs) to specific algorithmic enhancements (Q-Policy, Quantum Dyna Q-Learning) and the use of general quantum optimizers (QA, QAOA, VQCs) for RL components or related problems.

A key theme is the potential for quantum parallelism to accelerate computations involving large state-action spaces, particularly in policy evaluation (Q-Policy) or model learning (Quantum Dyna Q-Learning). However, demonstrating a practical quantum advantage for solving MDPs end-to-end is challenging. The overheads of quantum state preparation, oracle construction (for Grover-like methods), circuit execution on noisy hardware, and measurement are significant.

The finding in that some PQC-QRL performance may not heavily rely on quantum properties like entanglement is a critical point, urging careful analysis to distinguish true quantum benefits from effects achievable via classical means or simply different parameterizations. The development of rigorous quantum MDP theory is crucial for building a solid foundation for future quantum RL algorithms that genuinely exploit quantum phenomena for advantage.

Missing Data: As of May 2025, there is a scarcity of empirical demonstrations of quantum algorithms outperforming state-of-the-art classical reinforcement learning algorithms on complex, large-scale MDPs using actual quantum hardware. Most QRL research is theoretical or based on simulations in relatively simple environments (e.g., gridworlds). Comprehensive benchmarks comparing different QRL paradigms against each other and against strong classical RL baselines on standardized, challenging MDP problems, with full accounting of resource usage on real hardware, are largely missing. It is a step in this direction for comparing QRL approaches, but not against classical.

Table 1. Quantitative Performance Summary of Quantum Optimization Methods for Classical ML Algorithms.

Classical ML Algorithm & Quantum Approach	**Problem Size Tackled (N, d, k, etc.)**	**Quantum Resources Reported (Qubits, Depth/Layers, Annealing Time)**	**Performance Metric & Value (vs. Classical Baseline)**	**Classical Baseline Used**	**Notes**
k-means Clustering					
k-means via QA-QUBO (Balanced)	N=up to ~100 (tested)	$O((Nk)^2)$ logical qubits (theory), D-Wave 2000Q	Comparable solution quality for small N; Slower runtime than classical.	Scikit-learn k-means	Embedding time dominates. QUBO formulation $O(N^2kd)$.
k-means via VQE+Contour Coreset	Synthetic & real-life data	Not specified	$> 10\%$ accuracy improvement over QAOA+Coreset k-	QAOA+Coreset k-means	Simulation. Contour coreset tailored for

			means. Lower std. dev.		quantum.
q-means (KLLP19)	Theoretical	QRAM assumed, $O(polylogN)$ qubits	Theoretical per-iteration speedup ($O(polylogN)$ vs $O(Ndk)$).	Classical k-means	Relies on QRAM. Practical advantage not demonstrated on hardware.
Hybrid Quantum k-Means (Poggiali [36]**)**	Small N (real hardware)	$O(log(Nd))$ to $O(log(MNdk))$ qubits	Sim: comparable to classical. Real HW (q1:1): good but slow. Real HW (q1:k): poor due to noise.	Classical k-Means	High shot count needed. Communication overhead.
Support-Vector Machines (SVM)					
QSVM via QA/CIM (Probabilistic, He & Xiao)	Banknote (N~1372), IRIS (N=150)	550 qubits (Banknote), 100 qubits (IRIS)	Banknote: Up to 20% higher acc. vs original QSVM, 10^4x faster vs SA. Matched/reduced time vs classical SVM. IRIS: Outperformed other QSVMs.	Original QSVM, SA, CSVM	Real CIM hardware tested. Batch processing for larger datasets.
QSVM via MTQA	Iris, Digits	Parallel embedding on annealer	Accuracy is equivalent to SMO, SA, std. QA. QPU runtime C times faster.	SMO, SA, std. QA	Multi-class using OneVsRest.
QSVM via Quantum Kernel (Bioinformatics)	N up to ~6000 (CLBtope)	6, 10, 14 qubits (simulated)	CLBtope: QSVM AUC 0.68 vs CML 0.82. HemoPI: QSVM AUC 0.95 vs CML 0.98. CML generally superior.	Classical SVM, ET, RF	Performance dataset dependent. QSVM computational overhead high.
QSVM via VQE+SWAP Test	Credit sales data (8 features)	3 qubits, 2-layer ansatz	100% accuracy reported, simpler than classical models for this task.	Classical SVM, RF	Specific small dataset.
Decision Trees					
Des-q (Retraining)	Multiple datasets	QRAM assumed (KP-tree).	Simulated: Similar accuracy to classical. Logarithmic retraining complexity vs classical polynomial.	Classical Decision Tree	Focus on retraining speedup.
QUBO Decision Tree	Theoretical	Depends on QUBO size from multi-dim. splits	Aims for more optimal/complex splits. Accuracy vs classical CART not detailed.	Classical CART	Solvable by annealer.
Random Forests					
QC-Forest (Retraining)	Up to N=80,000	Extends Des-q (QRAM). Classical weight calc.	Simulated: Competitive accuracy to classical RF. Poly-log retraining time.	Classical RF	Focus on retraining speedup for streaming data.
QBoost-inspired (Ensemble Opt.)	Financial risk data	50 qubits (neutral atom QPU)	Competitive accuracy to classical RF. Better interpretability, comparable training time.	Classical RF	Optimizes ensemble weights via QUBO.
Linear/Logistic Regression					
QAE for Linear Regression (Kaneko)	Theoretical	QRAM for data access.	$(O(\epsilon^{-1})$complexity for coefficients, $log(N_D)$ dependence.	Classical Least Squares	Hybrid. Improves ϵ dependence over prior quantum.

Quantum Logistic Regression [61]	Theoretical	QRAM assumed.	Exponential speedup per gradient iteration if $M = O(polylogN)$.	Classical Grad. Descent	Focus on gradient calculation.
HQNN-FSP (Regression)	Financial time series	QNN regressor (qubit number varies)	RMSE higher than classical LSTM/BiLSTM. Quantum models struggled with rapid market changes.	RNN, LSTM, BiLSTM	Hybrid. Explores feature representation.
Markov Decision Processes (MDPs)					
Q-Policy (Policy Evaluation)	Theoretical	Amplitude encoding, QRAM	Provable polynomial reduction in sample complexity ($O(\epsilon^{-1})$ vs $O(\epsilon^{-2})$.	Classical Policy Iter.	Accelerates policy evaluation.
QA for Test Case Mutation (CPS)	CPS test scenarios	D-Wave annealer	Faster test case generation with similar fault detection vs alternatives.	Classical mutation	QUBO formulation of mutation problem.
PQC-QRL Benchmarking	Gridworld environments	Varies (e.g. PQC for policy/value)	Performance often not heavily reliant on quantum properties (entanglement).	(Comparison among QRL)	Simulation.
Game-Solving QCNNs	Tic-Tac-Toe	QCNN on quantum hardware/simulator	Hybrid QCNN Elo comparable to classical CNN. Standalone QCNN underperformed.	Classical CNN	Game-based benchmark.

Table 2. Qualitative Mapping of Quantum Optimization Techniques to Classical ML Algorithms.

Quantum Optimization Technique	k-means clustering	Support-Vector Machines (SVM)	Decision Trees	Random Forests	Linear/Logistic Regression	Markov Decision Processes (MDPs)
Quantum Annealing (QA)	**Suitability**: Medium (for QUBO formulations, esp. balanced k-means)**Challenges**: QUBO quality, embedding, problem size. **Advantage Sought**: Ground state search for optimal assignment.	**Suitability**: High (for QUBO formulations of SVM training) **Challenges**: Parameter binarization precision, QUBO quality, problem size. **Advantage Sought**: Faster QUBO solution, handling constraints.	**Suitability**: Medium (for QUBO formulation of optimal/complex splits, e.g., QUBO DT) **Challenges**: QUBO formulation complexity, tree size. **Advantage Sought**: Better quality splits.	**Suitability**: Low-Medium (via QUBO for ensemble weighting e.g. QBoost-like, or for individual tree splits) **Challenges**: QUBO formulation for forest structure. **Advantage Sought**: Optimized ensemble / better splits.	**Suitability**: Medium (for QUBO formulations with discretized parameters; or continuous via Bosonic QA)**Challenges**: Parameter discretization, QUBO quality. **Advantage Sought**: Solving regression QUBO.	**Suitability**: Medium (for QUBO formulations of specific sub-problems e.g. scheduling, planning, test generation)**Challenges**: Mapping MDP policies/values to QUBO. **Advantage Sought**: Solving optimization sub-tasks.
QAOA (Variational)	**Suitability**: Medium (for QUBO/MaxCutformulations) **Challenges**: Ansatz design, optimization, barren plateaus, circuit depth. **Advantage Sought**:	**Suitability**: Medium (for QUBO formulation of SVM training, or variational kernel optimization)	**Suitability**: Low-Medium (for QUBO sub-problems in tree construction) **Challenges**: Mapping tree	**Suitability**: Low (primarily via optimizing QUBOs for individual trees if applicable) **Challenges**:	**Suitability**: Low-Medium (for QUBO formulations or direct variational regression) **Challenges**:	**Suitability**: Medium (for QUBO sub-problems in RL, or variational policy/value functions) **Challenges**:

	Approximate solution to k-means QUBO.	**Challenges**: Ansatz design, barren plateaus, parameter optimization. **Advantage Sought**: Solving SVM QUBO or finding better kernels.	optimization to QAOA-suitable Hamiltonians. **Advantage Sought**: Solving tree optimization sub-problems.	Scalability to many trees, complex Hamiltonians. **Advantage Sought**: Optimizing tree components.	Ansatz design for regression, barren plateaus. **Advantage Sought**: Solving regression QUBO or learning regression function.	Ansatz design for policies/values, barren plateaus, large state spaces. **Advantage Sought**: Optimizing policies or value functions.
VQE (Variational)	**Suitability**: Medium (for MaxCut formulation from k-means) **Challenges**: Hamiltonian construction, ansatz design, optimization, barren plateaus. **Advantage Sought**: Finding ground state for k-means mapping.	**Suitability**: Medium (for direct classification via pattern states, or variational kernel optimization)**Challenges**: Ansatz design, barren plateaus, training. **Advantage Sought**: Learning classifiers or better kernels.	**Suitability**: Low (less direct application to tree structure optimization) **Challenges**: Mapping tree structure to VQE. **Advantage Sought**: Potentially for split evaluation if framed as energy min.	**Suitability**: Low (similar to Decision Trees) **Challenges**: As per Decision Trees. **Advantage Sought**: As per Decision Trees.	**Suitability**: Medium (for direct variational regression, fitting PQC parameters) **Challenges**: Ansatz design, loss function, barren plateaus. **Advantage Sought**: Learning regression function.	**Suitability**: Medium (for variational policy/value functions in QRL) **Challenges**: Ansatz design for policies/values, barren plateaus, sample efficiency. **Advantage Sought**: Learning optimal policies/values.
Grover's / Amplitude Amp.	**Suitability**: Medium (q-means for faster iteration via distance calc/centroid update) **Challenges**: QRAM, oracle construction, overall speedup. **Advantage Sought**: Quadratic speedup in subroutines.	**Suitability**: Low (for core SVM optimization); Potentially for hyperparameter search. **Challenges**: Oracle for SVM solution, large search space. **Advantage Sought**: Search speedup.	**Suitability**: Medium (for split finding in tree construction) **Challenges**: Oracle for best split, comparison to classical heuristics. **Advantage Sought**: Faster split search.	**Suitability**: Medium (for split finding within individual trees) **Challenges**: As per Decision Trees, applied to ensemble. **Advantage Sought**: Faster split search.	**Suitability**: Medium (e.g., QAE for accelerating classical linear regression calculations)**Challenges**: Oracle/operator construction, error tolerance. **Advantage Sought**: Speedup in specific calculations.	**Suitability**: Medium (for action selection or state search in RL, e.g., Quantum Dyna Q, AA-QRL)**Challenges**: Oracle for optimal action/state, integration with RL loop. **Advantage Sought**: Faster search/selection.
Hybrid Q-C Workflows	**Suitability**: High (QASOFM, Hybrid Quantum k-Means,Coreset+VQE/QAOA) **Challenges**: Data loading, QRAM, shot noise, integration overhead. **Advantage Sought**: Speedup specific subroutines, handle larger N via coresets.	**Suitability**: High (Quantum Kernels, Batch processing for QA)**Challenges**: Kernel fidelity, data loading, classical SVM overhead. **Advantage Sought**: Enhanced feature spaces, scalability with batching.	**Suitability**: High (Des-q for retraining, QRC for ensembles)**Challenges**: QRAM for Des-q, effective feature extraction for QRC. **Advantage Sought**: Retraining speedup, enhanced features.	**Suitability**: High (QC-Forest for retraining,QBoost-inspired ensembles)**Challenges**: As per Des-q, QUBO quality for QBoost. **Advantage Sought**: Retraining speedup, optimized ensembles.	**Suitability**: High (QAE for linear regression, HQNN for regression)**Challenges**: Integration complexity, practical speedup validation. **Advantage Sought**: Accelerate classical calculations, novel NN architectures.	**Suitability**: High (q-MDP theory, Q-Policy, QCNNs for games)**Challenges**: Complex quantum state manipulation, theoretical to practical gap. **Advantage Sought**: Fundamental speedups in RL, novel policy representations.

4. MISSING DATA

A recurring theme across the exploration of quantum optimization for these classical machine learning algorithms is the conspicuous absence of comprehensive, standardized benchmarks. As of May 2025, for k-means clustering, Support-Vector Machines, Decision Trees, Random Forests, Linear/Logistic Regression, and Markov Decision Processes, there's a clear need for more rigorous comparative studies.

Specifically, what's largely missing are public benchmarks that pit the diverse array of quantum approaches be it Quantum Annealing, VQE, QAOA, Grover-based methods, or various hybrid strategies against highly optimized, state-of-the-art classical implementations. Such comparisons would need to be conducted on a wide range of large-scale, real-world datasets to truly assess practical viability.

Crucially, these evaluations must meticulously account for all associated overheads. This includes the computational cost of classical pre-processing (like QUBO generation or coreset construction), the intricacies of quantum data loading (such as QRAM assumptions), the resources consumed by classical optimization loops inherent in VQAs, the impact and cost of error mitigation techniques, and the final readout of results. While theoretical speedups for specific subroutines or promising results from simulations on small or synthetic datasets exist, comprehensive, end-to-end demonstrations of practical quantum advantage on actual quantum hardware, considering all these factors, remain largely outstanding across these foundational machine learning tasks.

5. CROSS-CUTTING THEMES & OPEN CHALLENGES

The promise of quantum optimization for classical machine-learning is tempered by a series of interlocking difficulties that span algorithms, architecture, and fundamental theory. These issues appear repeatedlyregardless of the specific quantum technique or learning task—and currently define the limits of practical progress.

5.1. SCALABILITY: QUBIT COUNT, CONNECTIVITY, AND GATE FIDELITY

Today’s processors provide, at best, a few thousand physical qubits—far fewer than manyrealistic machine-learning workloads require. A straightforward QUBO mapping of k-means, for example, can demand a number of qubits that grows quadratically with both data points and clusters, quickly outstripping available hardware. Proposals that substitute multi-level quantum systemsfor qubits expand Hilbert-space dimension more economically, but introduce new control challenges and heightenedsusceptibility to error.

Hardware topology compounds the problem. Limited on-chip connectivity means two-qubit gates are possible only between certain neighbors; interactions between distant qubits must be mediated by SWAP chains, inflating circuit depth and error exposure. Variational-circuit and kernel-based approaches must therefore be contorted to fit the underlying graph, often at the cost of theoretical elegance.

Gate fidelity further constrains feasible circuit depth. Each imperfect operation contributes a small error; accumulated over dozens or hundreds of layers, these errors can overwhelm any computational signal. Errors in state preparation and measurement (SPAM) add another layer of noise. Until fidelities improve, algorithmic design remains tightly coupled to hardware capabilities.

5.2. NOISE IN NISQ AND FAULT-TOLERANT REGIMES

By definition, NISQ devices operate in a noisy environment. Decoherence, control errors, and imperfect read-out collectively limit circuit duration and depth. While some argue that the stochastic nature of optimization, particularly variants of gradient descent, might tolerate moderate noise, empirical evidence shows that NISQ-level error rates usually dominate any prospective quantum speed-up. As a consequence, research has shifted toward quantum-error-mitigation techniques that suppress noise without the full overhead of quantum-error correction (QEC).

Fault-tolerant quantum computing promises to remove most operational errors by encoding logical qubits in large ensembles of physical qubits and continuously correcting them. This capability would relax the depth constraints that currently handicap quantum optimisation and enable algorithms requiring long coherent evolutions, such as large-scale Grover-style search. The price, however, is steep: orders-of-magnitude overhead in qubit numbers, added control circuitry, and the need for real-time decoding. Preparing for this regime therefore demands algorithmic blueprints that are realistic about resource counts while remaining forward-compatible with fault-tolerant machines.
Collectively, these challenges underscore a central point: progress in quantum-enhanced machine learning is inseparable from advances in both hardware and error-control theory. Algorithm design, benchmark construction, and application studies must evolve in concert with the underlying technology if the field is to move beyond proof-of-principle demonstrations toward solutions of genuine practical value.

CONCLUSION

Quantum optimization for classical machine-learning still sits in that tantalising space between "neat idea on the whiteboard" and "button you can press in production." Theoretical analyses, numerical experiments, and the occasional run on real hardware all hint at speed-ups or accuracy gains, but so far only for toy-sized problems. What keeps the champagne on ice is, of course, today's Noisy Intermediate-Scale Quantum (NISQ) devices. Limited qubit counts, patchy connectivity, and relentless noise force researchers to juggle heuristics, squeeze problems into QUBO straight-jackets, and lean heavily on hybrid quantum–classical workflows.

Our research across six cornerstone ML models underscores a shared bottleneck: translating each algorithm into quantum-friendly form is usually the hardest part. For k-means and SVMs, QUBO mappings and quantum kernels have become the workhorses; they show promise, but mainly in benchmarking arenas rather than on real-world datasets. Decision trees and random forests are only beginning their quantum adventure. Current work concentrates on niche accelerations (e.g., Des-q split finding or QC-Forest retraining for streaming data) and will remain speculative until quantum-addressable memory becomes practical. Linear and logistic regression have flirted with HHL-style solvers (and bumped into HHL's notorious condition-number caveats) before pivoting toward variational circuits or specialised annealers for direct parameter fitting. Markov Decision Processes round out the picture with first-principles quantum generalisations and small-scale speed-ups in policy evaluation. Across the board, genuinely large instances remain firmly on the classical side of the fence.

The headwinds are familiar but stubborn. Hardware limits shrink problem sizes; noise chops circuit depth; and "apples-to-apples" benchmarking often crowns finely tuned classical optimisers the winner. Moving classical data onto qubits and fetching results can nullify theoretical speed-ups. Meanwhile, questions of fairness, bias, and interpretability in quantum-enhanced ML are only entering the conversationand they deserve equal billing with raw performance.

Yet progress is real. Each incremental algorithmic tweak or hardware upgrade inches the field forward, and hybrid pipelines where a quantum routine tackles just the knottiest sub-problem look like the best near-term bet. Long-term dreams of fault-tolerant, large-scale quantum computers aren't fantasy; they are simply on a different timeline. Until those machines arrive, sober assessments such as this SoK help separate genuine opportunity from wishful thinking. By mapping what works, what doesn't, and importantly why, we sharpen the community's collective instincts and steer effort toward the experiments most likely to crack open real quantum advantage. The road is long, the milestones are clear, and the occasional detour is part of the adventure.

ACKNOWLEDGEMENT

We are deeply grateful to **Romuald Kotowski** and **Piotr Tronczyk** for their invaluable guidance and assistance throughout the research process. We are particularly thankful for their dedicated teaching and the knowledge they have imparted, which formed the foundation for this research.

I. REFERENCES

[1] M. M. Waldrop, "The chips are down for Moore's law. Nature, 530(7589), 144–147," 2016. [Online]. Available: https://doi.org/10.1038/530144a.

[2] L. Chen, T. Li, Y. Chen, X. Chen, M. Wozniak, N. Xiong and W. Liang, "Design and analysis of quantum machine learning: a survey," 2024. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/09540091.2024.2312121.

[3] Wikipedia, "HHL algorithm," [Online]. Available: https://en.wikipedia.org/wiki/HHL_algorithm.

[4] Wikipedia, "Grover's algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Grover%27s_algorithm.

[5] D. Pranji, B. C. Mummaneni and C. Tutschku, "Quantum Annealing based Feature Selection in Machine Learning," 2024. [Online]. Available: https://arxiv.org/pdf/2411.19609.

[6] Y. Wang and J. Liu, "A comprehensive review of Quantum Machine Learning:," 2024. [Online]. Available: https://arxiv.org/pdf/2401.11351.

[7] J. K. Florian, M. A. Wolf, M. Marso and Philipp, "Benchmarking Quantum Generative Learning:," 2024. [Online]. Available: https://arxiv.org/pdf/2403.18662.

[8] T. Fellner, D. Kreplin, S. Tovey and C. Holm, "Quantum vs. classical: A comprehensive benchmark study for predicting time series with variational quantum machine learning," 2025. [Online]. Available: https://arxiv.org/abs/2504.12416.

[9] M. Larocca, S. Thanasilp, S. Wang, K. Sharma and J. Biamonte, "A Review of Barren Plateaus in Variational Quantum Computing," 2025. [Online]. Available: https://arxiv.org/pdf/2405.00781.

[10] Wikipedia, "Noisy intermediate-scale quantum era," [Online]. Available: https://en.wikipedia.org/wiki/Noisy_intermediate-scale_quantum_era.

[11] K. S. PRABHA and D. S. V. A. RAO, "USING QUANTUM COMPUTING TO ENHANCE LEARNING ALGORITHMS: QUANTUM," 2024. [Online]. Available: https://jnao-nu.com/Vol.%2015,%20Issue.%2002,%20July-December%20:%202024/132_online.pdf.

[12] C. Albornoz, "How to start learning quantum machine learning," 2021. [Online]. Available: https://pennylane.ai/blog/2021/10/how-to-start-learning-quantum-machine-learning.

[13] Wikipedia, "Quantum entanglement," [Online]. Available: https://en.wikipedia.org/wiki/Quantum_entanglement.

[14] D. Volpe, G. Orlandi and G. Turvani, "Improving the Solving of Optimization Problems: A Comprehensive Review of Quantum Approaches. Quantum Reports. Multidisciplinary Digital Publishing Institute," 2025. [Online]. Available: https://www.mdpi.com/2624-960X/7/1/3.

[15] Wikipedia, "Hamiltonian (quantum mechanics)," [Online]. Available: https://en.wikipedia.org/wiki/Hamiltonian_(quantum_mechanics).

[16] Wikipedia, "Quantum optimization algorithms," [Online]. Available: https://en.wikipedia.org/wiki/Quantum_optimization_algorithms.

[17] S. Jansen, M.-B. Ruskai and R. Seiler, "Bounds for the adiabatic approximation with applications to quantum computation," 2007. [Online]. Available: https://pubs.aip.org/aip/jmp/article-abstract/48/10/102111/379272/Bounds-for-the-adiabatic-approximation-with?redirectedFrom=fulltext.

[18] Wikipedia, "Hamiltonian mechanics," [Online]. Available: https://en.wikipedia.org/wiki/Hamiltonian_mechanics.

[19] D:Wave, "Fast Track Your Quantum Journey with Quantum Computing Training," [Online]. Available: https://www.dwavequantum.com/learn/training/.

[20] M. Larocca, S. Thanasilp, S. Wang, K. Sharma and J. Biamonte, "A Review of Barren Plateaus

in Variational Quantum Computing," [Online]. Available: https://arxiv.org/pdf/2405.00781.

[21] R. Bhowmick, H. Wadhwa, A. Singh, T. Sidana, Q. H. Tran and K. K. Sabapathy, "Enhancing variational quantum algorithms by balancing training on classical and quantum hardware," 2025. [Online]. Available: https://arxiv.org/abs/2503.16361v1.

[22] A. Barbosa, E. Pelofske, G. Hahn and H. N. Djidjev, "Using machine learning for quantum annealing accuracy prediction," [Online]. Available: https://arxiv.org/abs/2106.00065.

[23] D. Arthur and P. Date, "Balanced k-means clustering on an adiabatic quantum," 2020. [Online]. Available: https://arxiv.org/abs/2008.04419.

[24] K. Yawata, Y. Osakabe, T. Okuyama and A. Asahara, "QUBO Decision Tree: Annealing Machine Extends Decision Tree Splitting," [Online]. Available: https://arxiv.org/abs/2303.09772.

[25] IBM Quantum, "QAOA," [Online]. Available: https://docs.quantum.ibm.com/api/qiskit/0.28/qiskit.algorithms.QAOA.

[26] J. Artag, M. Shimada and J.-i. Shirakashi, "Multi-Task Quantum Annealing for Rapid Multi-Class Classification," 2024. [Online]. Available: https://www.computer.org/csdl/proceedings-article/qce/2024/413702a506/23oqoQ9lgOY.

[27] T. Chen, A. Ray, A. Seshadri, D. Herman, B. Bach, P. Deshpande, A. Som, N. Kumar and M. Pistoia, "Provably faster randomized and quantum algorithms for," 2025. [Online]. Available: https://arxiv.org/pdf/2504.20982.

[28] C. Yung and M. Usman, "Clustering by Contour coreset and variational quantum eigensolver," 2023. [Online]. Available: https://arxiv.org/abs/2312.03516v1.

[29] W. Zhao and G. Tang, "Clustering-Based Sub-QUBO Extraction for Hybrid QUBO Solvers," 2025. [Online]. Available: https://arxiv.org/pdf/2502.16212.

[30] J. F. Doriguello, A. Luongo and E. Tang, "Do you know what q-means?," [Online]. Available: https://arxiv.org/pdf/2308.09701.

[31] I. D. Lazarev, M. Narozniak, T. Byrnes and A. N. Pyrkov, "Hybrid quantum-classical unsupervised data clustering based on the self-organizing feature map," 2025. [Online]. Available: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.111.012416.

[32] A. Poggiali, A. Berti, A. Bernasconi, G. M. D. Corso and R. Guidotti, "Quantum Clustering with k-Means: a Hybrid Approach," [Online]. Available: https://arxiv.org/abs/2212.06691.

[33] X.-y. Z. M. L. S.-q. S. Li Xu, "Quantum Classifiers with Trainable Kernel," 2025. [Online]. Available: https://arxiv.org/abs/2505.04234v1.

[34] H. He and Y. Xiao, "Probabilistic Quantum SVM Training on Ising Machine," 2025. [Online]. Available: https://arxiv.org/abs/2503.16363v1.

[35] M. Sawerwain and J. W.́sniewska, "Variational Quantum Eigensolver for," 2024. [Online]. Available: https://arxiv.org/pdf/2303.02797.

[36] R. Coelho, G. Kruse and A. Rosskopf, "Quantum-Efficient Kernel Target Alignment," 2025. [Online]. Available: https://arxiv.org/html/2502.08225v1.

[37] X. Li, J. Liu, V. Chaudhary, E. H. Hansen, S. Xu and P. Hovland, "Accelerating VQE Algorithm via Parameters and Measurement Reuse," 2023. [Online]. Available: https://www.computer.org/csdl/proceedings-article/icrc/2023/10386370/1TJmfS663fy.

[38] S.-A. Jura and M. Udrescu, "Quantum-Enhanced Weight Optimization for Neural Networks Using Grover's Algorithm," 2025. [Online]. Available: https://arxiv.org/abs/2504.14568v1.

[39] A. K. M. Masum, A. Maurya, D. S. Murthy and N. M. Pratibha, "Hybrid Quantum-Classical Machine Learning for Sentiment Analysis," 2023. [Online]. Available: https://arxiv.org/abs/2310.10672.

[40] G. Gentinetta, A. Thomsen, D. Sutter and S. Woerner, "The complexity of quantum support vector machines," 2024. [Online]. Available: https://arxiv.org/abs/2203.00031.

[41] M. Nadim, M. Hassan, A. K. Mandal, C. K. Roy, B. Roy and K. A. Schneider, "Comparative Analysis of Quantum and Classical Support Vector Classifiers for Software Bug Prediction: An Exploratory Study," 2025. [Online]. Available: https://arxiv.org/abs/2501.04690v1.

[42] N. Kuma, R. Y. C. Li, P. Minssen and M. Pistoia, "Des-q: a quantum algorithm to provably speedup retraining of decision trees," 2025. [Online]. Available: https://arxiv.org/abs/2309.09976v6.

[43] H. Lee and K. Jun, "QUBO Refinement: Achieving Superior Precision through Iterative Quantum Formulation with Limited Qubits," 2024. [Online]. Available: https://arxiv.org/pdf/2411.16138.

[44] R. Yalovetzky, N. Kumar, C. Li and M. Pistoia, "QC-Forest: a Classical-Quantum Algorithm to Provably Speedup Retraining of Random Forest," 2024. [Online]. Available: https://arxiv.org/abs/2406.12008v3.

[45] D. Volpe, D. Volpe, M. Graziano, G. Turvani and R. Wille, "A Predictive Approach for Selecting the Best Quantum Solver for an Optimization Problem," 2024. [Online]. Available: https://www.computer.org/csdl/proceedings-article/qce/2024/413701b014/23oq5IltHA4.

[46] Z. Li and K. Terashi, "Quantum decision trees with information entropy," 2025. [Online]. Available: https://arxiv.org/abs/2502.11412v1.

[47] S. H. Sack and D. J. Egger, "Large-scale quantum approximate optimization on non-planar graphs with machine learning noise mitigation," 2023. [Online]. Available: https://arxiv.org/abs/2307.14427v2.

[48] L. Tarrataca and A. Wichert, "Tree Search and Quantum Computation," [Online]. Available: https://web.ist.utl.pt/~luis.tarrataca/publications/treeSearchAndQuantumComputation.pdf.

[49] W. Zhao, Y. Wang, Y. Qu, H. Ma and S. Wang, "Binary Classification Quantum Neural Network Model Based on Optimized Grover Algorithm," 2022. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9777537/.

[50] D. Ko, S. Świerczewski, A. Opala, M. Matuszewski and A. Rahmani, "Estimation of the second-order coherence function using quantum reservoir and ensemble methods," 2025. [Online]. Available: https://arxiv.org/abs/2504.18205.

[51] S. Barua, M. Rahman, S. Khaled, M. J. Sadek, R. Islam and S. Siddique, "QuXAI: Explainers for Hybrid Quantum Machine Learning Models," 2025. [Online]. Available: https://arxiv.org/abs/2505.10167v1.

[52] Aliro, "Integrating AI and Quantum Technologies," 2024. [Online]. Available: https://www.aliroquantum.com/integrating-ai-and-quantum-technologies.

[53] L. Leclerc, L. Ortiz-Gutiérrez, S. Grijalva, B. Albrecht, J. R. K. Cline and A. S. L. H. G. D. B. Vincent E. Elfving, "Financial risk management on a neutral atom quantum processor," 2023. [Online]. Available: https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.5.043117.

[54] C. Lytrosyngounis and I. Lytrosyngounis, "Hybrid Quantum-Classical Optimisation of Traveling Salesperson Problem," 2025. [Online]. Available: https://arxiv.org/abs/2503.00219v1.

[55] H.-L. Liu, C.-H. Yu, Y.-S. Wu, S.-J. Pan, S.-J. Qin, F. Gao and a. Q.-Y. Wen, "Quantum algorithm for logistic regression," 2019. [Online]. Available: https://www.arxiv.org/pdf/1906.03834v2.

[56] A. Koura, T. Imoto, K. Ura and Y. Matsuzaki, "Linear Regression Using Quantum Annealing with Continuous Variables," 2024. [Online]. Available: https://arxiv.org/abs/2410.08569v1.

[57] S. Liang, L. Zhu, X. Liu, C. Yang and X. Li, "Artificial-Intelligence-Driven Shot Reduction in

Quantum Measurement," 2024. [Online]. Available: https://arxiv.org/abs/2405.02493v1.

[58] K. Kaneko, K. Miyamoto, N. Takeda and K. Yoshino, "Linear Regression by Quantum Amplitude Estimation and its Extension to Convex Optimization," 2021. [Online]. Available: https://arxiv.org/abs/2105.13511.

[59] P. Ma, Y. Chen, H. Lu and W. Zhong, "Bisection Grover's Search Algorithm and Its Application in Analyzing CITE-seq Data," 2024. [Online]. Available: https://www.researchgate.net/publication/384210371_Bisection_Grover's_Search_Algorithm_and_Its_Application_in_Analyzing_CITE-seq_Data.

[60] P. Kumar, N. Innan, M. Shafique and R. C. Singh, "HQNN-FSP: A Hybrid Classical-Quantum Neural Network for Regression-Based Financial Stock Market Prediction," 2025. [Online]. Available: https://arxiv.org/abs/2503.15403.

[61] E. Duryea and W. Hu, "Quantum Dyna Q-Learning," [Online]. Available: https://dspace.houghton.edu/server/api/core/bitstreams/b07596fe-8e21-454f-bfa2-3aae3f431e22/content.

[62] K. Cherukuri, A. Lala and Y. Yardi, "Q-Policy: Quantum-Enhanced Policy Evaluation for Scalable Reinforcement Learning," 2025. [Online]. Available: https://arxiv.org/abs/2505.11862v1.

[63] N. Saldi, S. Sanjari and S. Yuksel, "Quantum Markov Decision Processes: General Theory, Approximations, and Classes of Policies," 2024. [Online]. Available: https://arxiv.org/abs/2402.14649.

[64] J. Zhou, Z. Zhu, L. Zhu and S. Bu, "Problem-Structure-Informed Quantum Approximate Optimization Algorithm for Large-Scale Unit Commitment with Limited Qubits," 2025. [Online]. Available: https://arxiv.org/abs/2503.20509v1.

[65] H. Araujo, X. Wang, M. Mousavi and S. Ali, "Using quantum annealing to generate test cases for cyber-physical systems," 2025. [Online]. Available: https://arxiv.org/abs/2504.21684v1.

[66] M. Ostaszewski, L. M. Trenkwalder, W. Masarczyk, E. Scerri and V. Dunjko, "Reinforcement learning for optimization of variational quantum circuit architectures," 2021. [Online]. Available: https://arxiv.org/abs/2103.16089.

[67] Y. J. Patel, S. Jerbi, T. Bäck and V. Dunjko, "Reinforcement Learning Assisted Recursive QAOA," 2022. [Online]. Available: https://arxiv.org/abs/2207.06294v2.

[68] G. Kruse, R. Coelho, A. Rosskopf, R. Wille and J. M. Lorenz, "Benchmarking Quantum Reinforcement Learning," 2025. [Online]. Available: https://arxiv.org/abs/2502.04909v2.

[69] K. C. a. T. A. H. Stefanie Muroya, "Hardware-optimal quantum algorithms," 2025. [Online]. Available: https://www.pnas.org/doi/abs/10.1073/pnas.2419273122.

[70] S. KAMEI, H. KAWAGUCHI, S. NISHIO and T. Satoh, "Quantitative Evaluation of Quantum/Classical," 2025. [Online]. Available: https://arxiv.org/pdf/2503.21514.

[71] IBM Quantum, "Grover," [Online]. Available: https://docs.quantum.ibm.com/api/qiskit/0.28/qiskit.algorithms.Grover.

CREATIVE ASSOCIATIONS IN THE HYBRID ORGANISATION OF POLISH THEATRICAL LIFE: ZASP AND THE POLISH AICT SECTION

Konrad SZCZEBIOT

Doctoral School of Cardinal Stefan Wyszyński University in Warsaw
konrad@szczebiot.eu

ABSTRACT

The organisation of theatrical life in Poland is a **hybrid** system combining public institutions, private initiatives, and creative associations. This article offers a theoretical overview of how **creative associations** contribute to this hybrid cultural landscape, focusing on two emblematic cases: **ZASP** (the Association of Polish Stage Artists) and the Polish Section of **AICT/IATC** (International Association of Theatre Critics). It begins by introducing the concept of hybrid cultural organisations and their role in contemporary cultural policy and creative industries. It then provides historical and current overviews of ZASP and the Polish AICT section, illustrating how these bodies have functioned over time. Analysis shows that both organisations mediate between **tradition and innovation** in Poland's theatrical field, preserving artistic heritage and professional standards while adapting to new realities in the creative industry. The discussion highlights their dual role in bridging past and future, as well as the challenges they face in influencing cultural policy today.

INTRODUCTION

Poland's theatrical life is sustained by a**network of institutions and organisations** that span the public, private, and civil society sectors. This ecosystem comprises state-funded national theatres, city theatres, independent ensembles, and festivals. Alongside them operate **creative associations** professional unions, guilds, and societies formed by artists and critics, which play a crucial mediating role. These associations help organise the theatre community "in between" the state and market, embodying ahybrid organisationof cultural life. They often carry the legacy of Poland's rich theatrical traditions while engaging with contemporary policy frameworks and the creative industries paradigm.

This article examines two key examples of such associations in Poland's theatre field:**ZASP (Związek Artystów Scen Polskich)**, the Association of Polish Stage Artists, and the Polish Section of **AICT/IATC**, the International Association of Theatre Critics. Both organisations have deep historical roots and continue to be active today, providing a lens through which to explore howhybrid cultural organisationsfunction within Polish cultural policy. ZASP, founded in 1918, has been a central part of the professional lives of actors and stage artists for over a century. The Polish AICT section, established in the 1950s, is among the oldest in the international critics' network. Focusing on these cases, we will discuss how they **mediate between tradition and innovation**, for instance, by upholding longstanding artistic standards and adapting to new challenges such as digital media, changing labour markets, and evolving audience expectations.

The structure of this article is as follows. First, we outline a **the oretical framework** for understanding hybrid cultural organisations and their role in contemporary cultural policy and creative industries. Next, we present each case study: an overview of ZASP's historical development and current activities, followed by the same for the Polish AICT section. We then analyse how these associations balance **heritage and change** in the theatrical field. Finally, a discussion considers the broader implications of their roles, including their effectiveness in influencing cultural policy and supporting the creative industry, as well as the challenges they face in this process, before concluding with key insights.

THEORETICAL FRAMEWORK: HYBRID CULTURAL ORGANISATIONS IN CULTURAL POLICY

In cultural policy and management theory, **hybrid organisations mix elements and values from different sectors of society**. Rather than fitting neatly into a single category (public, private, or nonprofit), hybrids straddle multiple spheres. They often exhibit "the coexistence of multiple institutional logics," blending public-service missions with market-driven approaches and voluntary civic engagement. In practice, such organisations must cater to diverse stakeholders – for example, government authorities, creative professionals, audiences, and sponsors – and fulfil multiple goals simultaneously. This hybridity has become increasingly common in the cultural sector, where organisations seek to **"combine the best of both worlds: public accountability and private efficiency"** (nature.com), while also upholding their artistic or social missions.

Contemporary cultural policy encourages **these** hybrid arrangements to foster innovation and sustainability in the arts. Since the late 20th century, many countries, including Poland, have shifted from a centralised, state-dominated cultural model to a more pluralistic one involvingpublic-private partnerships, NGO participation, and cultural market mechanisms. The rise of the **creative industries paradigm** in the 2000s further amplified this trend. Creative industries policies frame culture as a sector of economic growth and innovation, emphasising entrepreneurship, cross-sector collaboration, and the professionalisation of cultural work. In this context,**creative associations**– organisations formed by artists, writers, critics, and other artistic professionals – have taken on new significance. They often serve as intermediaries between individual creators and the broader structures of support or regulation, such as funding bodies, legal regimes, and industry networks. These associations typically have a nonprofit ethos, serving their members and the public good, but must also engage with market realities and government policies. In other words, they embody the hybrid logic of serving artistic and cultural **values** while operating in an environment of **economic and policy pressures**.

The notion of hybridity within Poland's cultural **sector** is particularly relevant given the country's historical transitions. Under communist rule (1944–1989), culture was largely state-controlled, and independent associations were either incorporated into official structures or outright banned. After 1989, a resurgence of civil society allowed professional groups to reestablish or create new organisations to represent the interests of artists and cultural workers. Today, Poland's cultural policy recognises the role of non-governmental organisations (NGOs)and professional associations as partners in cultural governance and industry development. These entities are consulted in policymaking, collaborate on projects, and often receive public grants to carry out cultural initiatives. At the same time, they rely on membership fees or market activities (like training services or publications), blending multiple funding sources – another hallmark of hybrid organisations.

Creative associations in the theatre sector – like ZASP and the Polish AICT section – are thus naturally hybrid. They combine the membership-based, voluntary character of NGOs with quasi-public functions,such as advocating for the profession, administering collective agreements, or managing cultural programs. They navigate between preserving the cultural **heritage**of Polish theatre and engaging in **innovative practices** that align with contemporary trends in the creative industry. The following sections delve into each case to understand their historical trajectories and current roles.

CASE STUDY: ZASP (ASSOCIATION OF POLISH STAGE ARTISTS)

Historical Overview of ZASP

ZASP – **ZwiązekArtystówScen Polskich**, or the Union/Association of Polish Stage Artists – was founded on 21 December 1918, just weeks after Poland regained independence. During theConstitutional Congress at Warsaw's Rozmaitości Theatre, its establishment was a landmark in organising Poland's theatre professionals. The first chairman was Józef Śliwicki, and among the founding signatories were legendary actors of the time, including Stefan Jaracz, Juliusz Osterwa, and Aleksander Zelwerowicz. This illustrious founding group underscores ZASP's roots in Polish theatrical **tradition**– prominent artists created it*for*the artistic community from the start.

During the interwar period (1918–1939), ZASP quickly became one of the most dynamic labour and creative organisations in Poland's arts sector. It functioned essentially as a**union for actors and stage artists**. ZASP established an "organisational coercion" policy: theatres were required to employ only ZASP members, and **membership was compulsory**for professional actors. This closed-shop system, though strict, helped secure decent working conditions and united the theatrical workforce. ZASP negotiated standard contracts that guaranteed minimum wages for actors throughout each season—A significant achievement for the era, when labour rights in the arts were often precarious. The association didn't only focus on immediate labour issues; it also invested in the **infrastructure and future** of Polish theatre. In 1928, ZASP founded the **House of Veterans of Polish Theatre** in Skolimów, a home for retired actors. And in 1932, ZASP's advocacy played a key role in establishing the **State Institute of Theatre Art, Poland's first modern theatre school**. Through these initiatives, ZASP solidified its role as a guardian of theatrical tradition and a builder of institutions for the next generation, bridging the past (by caring for veteran artists) and the future (through the education of new artists).

World War II and its aftermath tested ZASP's resilience. During the Nazi occupation (1939–1945), ZASP operated as a**conspiratorial organisation**, part of the cultural underground. In 1940, it famously issued a ban forbidding Polish actors from performing in any German-organised artistic events – a form of resistance against using Polish art for enemy propaganda. Most actors honoured this ban, demonstrating the association's moral authority and the unity of the theatrical community in wartime. However, the post-war communist regime dramatically changed the cultural landscape. In 1950, as the state tightened control over all independent organisations, ZASP was**dissolved by decree**. A new state-controlled union replaced it, the Association of Polish Theatre and Film Artists (SPATiF). The name "ZASP" was initially erased. However, it reappeared as part of a hyphenated name, SPATiF-ZASP, in 1952, and for decades, the organisation's activities were supervised by authorities to align with socialist cultural policy. Despite this, ZASP's legacy persisted underground and in memory. In 1981, during a brief liberalisation, the pre-war name was legally restored, signalling a return to ZASP's original identity. Yet, after martial law was declared, the authorities again cracked down: on 1 December 1982, ZASP wasbannedand placed under imposed management; a "new" government-approved ZASP was created in 1983, although reportedly only about 20% of the former members joined this body. Finally, with the fall of communism in 1989, these parallel entities were reconciled – the independent spirit of the old ZASP rejoined with the official structure. Thus, after 1989, ZASP emerged once more as a unified, autonomous association of theatre artists, proudly reclaiming its tradition from 1918.

Contemporary Role and Functions of ZASP

In the current era, ZASP operates as **an ationwide creative association** for performing artists, navigating Poland's free-market democracy and integration into global creative industries. The association's mission encompasses protecting artists' rights, advocating for supportive cultural policies, and preserving the heritage of Polish theatre. Structurally, ZASP is today a non-governmental organisation (NGO) with an elected leadership, comprising its president and board, and a membership that includes actors, directors, singers, dancers, and other stage professionals. At the same time, it is recognised by the government for certain official functions – a hallmark of its hybrid character. For example, in 1995, the Polish Ministry of Culture granted ZASP a formalpermission to act as a collective management organisationfor copyright and related rights in the theatre field. This means ZASP wasauthorised to manage royalties on behalf of theatre directors and stage designers (for uses of their productions via recording, broadcasting, etc.) and related performers' rights (for actors, vocalists, dancers, etc.) in various media. Through this arrangement, ZASP plays a crucial mediating role in the **creative industries** economy: it collects and distributes royalties when theatrical works are filmed, televised, streamed, or otherwise commercially exploited, ensuring that artists are remunerated in the new digital and multimedia environment. Such a role blends a public-interest mandate (securing artists' intellectual property rights) with a service to individual creators, illustrating how ZASP combines institutional logics – part union, part rights agency.

Beyond rights management, ZASP continues to perform many traditional union-like functions: it represents artists in labour negotiations, lobbies on issues such as employment conditions, social security for artists, and cultural funding. For instance, during the COVID-19 pandemic, theatre artists in Poland faced mass unemployment due to shutdowns. Associations like ZASP were involved in **negotiations with the government** to create emergency support systems for freelance artists. This advocacy role indicates how ZASP positions itself as a voice of the artistic community in policy dialogues. However, it faces challenges in this arena. A recent study at the organisation's centenary found that **ZASP's members were not fully satisfied with its influence on cultural policy**, despite the association's formal avenues to participate (ruj.uj.edu.pl , ruj.uj.edu.pl). The research suggested that divisions within the theatre world – for example, between older and younger generations or between those working in public vs. private sectors – might limit ZASP's effectiveness in advancing a cohesive policy agenda. This highlights a contemporary tension: how to innovate and remain relevant in representation while uniting a diverse constituency of artists whose career realities are rapidly evolving.

ZASP also engages in activities that promote **artistic heritage and community**. The House of Veterans of Polish Scenes in Skolimów (built in 1928) is still maintained by ZASP as a retirement home for aged actors, partly funded by the association's resources and charitable contributions. This is a direct continuation of its traditional mission to honour those who contributed to theatre in years past. Meanwhile, the association is also looking forward: it often partners with other cultural bodies to support new talent and artistic experimentation. A notable example of collaboration is the **workshop for young theatre critics** that ZASP co-organised with the Polish section of AICT in 2022 and 2024. Held in Białystok during an international puppetry festival, this workshop trained emerging critics (in Polish and English) in the specifics of puppet and form theatre – a contemporary, evolving art form. By supporting such an initiative, ZASP signalled its recognition of innovative and non-traditional theatre genres, such as puppet theatre, and its commitment to cultivating the next generation of theatre specialists. It also shows ZASP's willingness to bridge across disciplines – connecting actors and critics, practitioners and observers – to enrich the theatrical ecosystem.

ZASP today exemplifies a **hybrid cultural organisation** that mediates between the legacies of Poland's theatre (its storied artists, classical institutions, and hard-won labour rights) and the demands of the present creative industry landscape, including digital rights, project-based work, and international collaboration. It retains the **prestige of tradition**, having been founded over 100 years ago by luminaries, which helps legitimise its voice in cultural affairs. Simultaneously, it pursues **innovation** by adapting to new legal and economic frameworks, as well as engaging with contemporary artistic forms and youth development. This dual identity is not without difficulties: ZASP must constantly balance the **old and the new**, ensuring that neither the heritage it protects nor the contemporary relevance it seeks is neglected.

CASE STUDY: POLISH SECTION OF AICT/IATC (INTERNATIONAL ASSOCIATION OF THEATRE CRITICS)

Historical Background and Legacy

The **International Association of Theatre Critics (IATC/AICT)**was established in 1956 in Paris under the auspices of UNESCO as a global network of theatre critics. Poland was early in this movement – the **Polish Section of AICT** is one of the association's oldest national sections. In the late 1950s, during Poland's post-Stalin cultural thaw, local theatre critics formed a group which became the Polish IATC section. Due to the constraints of the communist system, it initially operated as the**"Theatre Critics Club"**within the official Polish Journalists' Association. This meant the critics had a semi-autonomous club under the umbrella of a state-sanctioned union of journalists. This creative workaround allowed participation in an international NGO behind the Iron Curtain. This arrangement continued for decades; today, the Polish section is affiliated with the modern successor of that

journalists' union, StowarzyszenieDziennikarzy RP. Polish theatre critics maintained a robust presence in IATC despite the organisational technicalities. The Polish Section's leaders frequently held prominent positions in the IATC's international governing bodies and were elected during its congresses. Notably, Poland has hosted the IATC World Congress multiple times – in Warsaw (1992, 2012) and Gdańsk (2000) – reflecting the esteem in which the Polish section is held in the world community of critics.

During the Cold War, Polish theatre criticism – like the theatre itself – was highly regarded internationally, and figures from Poland took on global roles. One eminent example is **Roman Szydłowski**, a well-known Polish theatre critic and translator, who served as President of the IATC from 1960 to 1977. Szydłowski's long tenure leading the international association (and later being named its Honorary President) highlights how Polish critics were at the forefront of dialogues about theatre beyond their national context. His involvement also underscores the Polish section's ability to mediate between an authoritarian domestic context and an international intellectual exchange – a delicate balancing act of that era. The continuity of the Polish section was tested around 1981–1983, when martial law suppressed independent associations, including the journalists' union and its clubs. Still, it managed to survive and re-emerge in the late 1980s. After 1989, the Polish Section of AICT transitioned smoothly into the new environment, continuing its affiliation with a now-independent journalists' association and expanding its activities with greater freedom.

Activities and Current Role of the Polish AICT Section

Today, the Polish Section of AICT/IATC functions as a **professional association of theatre critics and scholars**, dedicated to promoting high standards of theatre criticism and facilitating exchange among critics nationally and internationally. Its mission can be summarised in a few core activities:training the new generation of critics, organising forums for discourse, and recognising **excellence in theatre and criticism**. In many ways, it serves as the **institutional memory and innovation engine**for theatre criticism in Poland's creative sector.

One of the section's key roles is educational and developmental. The Polish AICT organises **internships and workshops for young critics**, often in cooperation with IATC's international programs. These workshops may take place during theatre festivals or special events, providing emerging critics with mentorship and exposure to diverse theatre forms. For example, as noted earlier, the section partnered with ZASP in 2022 and 2024 to host a puppet theatre criticism workshop for critics aged 18–35. Such initiatives demonstrate the section's commitment to innovation – puppet theatre and visual theatre require different analytical approaches than traditional drama, so training critics in these areas helps keep criticism up to date with new artistic trends. Similarly, the Polish section participates in the IATC's Young Critics Seminars, which have been held in Poland, such as in Wrocław during the Theatre Olympics 2016. Investing in youth and new forms, the association mediates between the **tradition of rigorous critical practice** and the **innovation of expanding the atrical genres and media**.

Another primary function is organising **symposia and conferences** at the international, regional, and national levels. Through these events, the Polish AICT section provides a platform for dialogue on contemporary issues in theatre. For instance, it might host a regional European critics meeting or a panel discussion as part of a theatre festival in Poland. These forums encourage the exchange of ideas, comparative perspectives, and scholarly reflection, effectively connecting Poland's theatrical discourse with global currents. This role complements Poland's status as a country with a strong theatre tradition: the critics' association helps interpret and communicate the evolution of that tradition in the context of modern challenges, such as digital technology and changing audiences. A recent example of discourse leadership was during the COVID-19 pandemic, when the Polish section **surveyed theatre artistsabout how the theatre industry can survive lockdowns and what its post-pandemic direction should be**. The responses, published on the association's website, gathered practical and philosophical insights from practitioners, contributing to a broader understanding of the crisis's impact. This effort demonstrates critics acting as observers and conveners of the theatre community, collectively

innovating in a time of disruption.

Crucially, the Polish Section of AICT also **administers several prestigious theatre awards**, which link today's theatre to its historical legacy. These awards, typically named after significantPolish theatre and criticism figures, recognise outstanding achievements and uphold specific values in the field. According to the association's records, the Polish section grants (or has granted) prizes including:

- **Nagrodaim. Tadeusza Boya-Żeleńskiego (Boy-Żeleński Award)** – established in 1957 and known simply as the "**Boy**" award, this prize honours individuals for outstanding contributions to theatrical art.. (Tadeusz Boy-Żeleński was a famed critic and translator, symbolising the critical heritage).
- **Nagrodaim. Stefana Treugutta** was established in 2001 and was awarded for achievements in Television Theatre (an important Polish medium for staging plays on TV; Stefan Treugutt was a critic known for his work with TV Theatre).
- **Nagrodaim. IrenySolskiej** — founded in 2010, this award recognises exceptional Polish actresses and celebrates female contributions to theatre in honour of Irena Solska, a legendary early 20th-century actress.

Through these awards, the critics' association celebrates excellence. It steers attention to significant work, effectively mediating between the tradition of theatre (by invoking historical names and criteria of merit) and the contemporary scene (by highlighting current artists and trends). For instance, when the Polish section awarded the Irena Solska Prize to film and stage star **Katarzyna Figura in 2025**, it drew public attention to an artist who bridges popular and high culture while reinforcing the memory of Solska's legacy. With its decades-long history, the Boy prize has become a hallmark of prestige in Polish theatre circles, often awarded to senior artists or critics, reinforcing the continuity of artistic values from one generation to the next. Meanwhile, newer awards like the Treugutt prizes reflect the **innovation in forms and fields**, acknowledging television productions and literary contributions, which are modern expansions of what "theatre" encompasses.

It should be noted that some awards and activities were interrupted during the political transformation of 1989–1990. For example, earlier in the section, there were awards for young critics (e.g., Edwarda Csató) and internal club awards, which were **suspended after 1990** during a period of reorganisation. This indicates that the association had to adapt to a new funding and institutional context after state support patterns shifted. Nevertheless, the core initiatives were revived or replaced by new ones as described above, showing the section's resilience and adaptability.

In terms of **publications and presence**, the Polish AICT section maintains a bilingual web presence (Polish and English content) via its website, "AICT Polska" (aict.art.pl). This site serves as a cultural platform, publishing theatre reviews, essays, and news, as well as**archived critiques**of past productions and current analyses. By doing so, the association directly engages with the **digital transformation** of media, moving theatre criticism from traditional print outlets (many of which have reduced cultural pages) to an online resource. This preserves the critical discourse, an element of tradition, and makes it accessible to broader and younger audiences in the format they increasingly consume online, aligning with contemporary consumption habits. The section's embrace of online publishing and its social media presence exemplifies how it innovatesin theatre criticism to remain relevant in the era of the creative industries, where digital content and community-building are key.

In summary, the Polish Section of AICT/IATC is a vital **mediator in Poland's theatre culture**, linking the local with the global, the past with the present. It upholds a tradition of quality criticism, celebrating historical figures and achievements, and reinforcing a**continuity of artistic standards**. Simultaneously, it pushes forward by training new critics, engaging with new media and theatrical forms, and responding to current challenges, such as the pandemic's impact on theatre. All these activities are carried out as a **non-profit association of volunteers and professionals**, which often collaborates with state institutions (e.g., co-organising events at public theatres or with the Culture Ministry's support) but remains independent in its voice – a hallmark of its hybrid character.

DISCUSSION: MEDIATING BETWEEN TRADITION AND INNOVATION

The examples of ZASP and the Polish AICT section illustrate how creative associations are **bridging institutions** in the hybrid organisation of theatrical life. Both organisations operate between theestablished, state-supported cultural infrastructureand theemerging, market-driven creative sector, fulfilling roles that neither government bodies nor private enterprises can easily accomplish on their own. In doing so, they help mediate between tradition and innovation in several ways:

- **Preserving Cultural Heritage and Professional Ethos:** ZASP and the AICT Polish section each serve as custodians of their respective legacies within their domains. ZASP's long history and maintenance of institutions like the Veterans' House connect today's artists with a century of Polish theatre heritage, reinforcing values of solidarity and respect for elders. The AICT section's awards are named after theatrical luminaries (Boy-Żeleński, Solska, etc.), and its archive of critical writings ensure that past achievements and learned practices are not forgotten. Preserving **tradition** provides stability and a knowledge base from which innovation can spring. It also legitimises the associations in the eyes of stakeholders – they are seen as*bearers of continuity*in a rapidly changing cultural landscape.
- **Adapting to and Promoting Innovation:**At the same time, these associations actively engage with **innovation** in theatre and its related industries. ZASP has adapted its functions to contemporary needs by embracing roles such as collective rights management for digital exploitation of performances, a relatively new issue in the creative economy. It also opens up to new forms of theatre, as seen in its support for puppet theatre criticism workshops, and likely addresses the proliferation of freelancers and new job models in the performing arts, contrasting with the old repertory-company model. Similarly, the critics' association tackles emerging trends: it trains critics in contemporary forms, utilises online platforms for publishing and networking, and even guides discussions on crises and transformations (such as the pandemic's push toward online theatre). In doing so, these bodies help the theatre field navigate change – they **legitimise and disseminate innovations**. For instance, by giving an award to a TV theatre production or publishing an internet theatre review, they signal that these new formats are important and worthy of critical attention.
- **Connecting Stakeholders and Building Communities:**Both ZASP and the AICT section serve as intermediaries among various groups, including artists, critics, government officials, and audiences. ZASP's involvement in policy lobbying and negotiations (e.g., advocating for artist support funds) connects the artist community with state policymakers, translating the needs of practitioners into policy language and vice versa. The AICT section, through its symposia and surveys, connects theatre makers, commentators, and, indirectly, the public by shedding light on what is happening inside the theatre world. By hosting public award ceremonies or events at festivals, these associations also engage audiences, educating them about the artistry behind theatre. This **bridging function**is essential in a hybrid cultural system, as it fosters dialogue and partnership where purely hierarchical or market-based relations might fail. The associations provide a neutral, non-profit space for collaboration. For example, ZASP and AICT are collaborating on a workshop that demonstrates how an artist's union and a critics' society can jointly innovate in audience development and professional art training.
- **Influencing Cultural Policy and Creative Industry Development:**Creative associations often aim to influence cultural policy, leveraging their expertise and representative character to make a meaningful impact. In Poland, ZASP has formal channels to weigh in on policy, including the ability to propose legal changes and be consulted on arts funding issues. The AICT section contributes to policy indirectly by shaping discourse through critical articles and reports. Their success in this area has been mixed,and as noted, ZASP members feel the need for a more substantial impact on policy outcomes. Nonetheless, the **potential for influence** exists: ZASP's recognised status allowed it to secure the 1995 rights management mandate, integrating it into the country's cultural

governance framework. The critics' association, under UNESCO patronage, aligns with international cultural policy ideals, such as freedom of expression and cultural exchange, thereby feeding those perspectives into national conversations. In the **context of the creative industries, where governments often look to support art for art's sake and cultural entrepreneurship and employment, these associations can advocate for conditions that enable innovation, such as better social security for freelancers, grants for experimental work, and educational programs**. They represent a collective voice that individual artists or critics might lack, filling a governance gap in the hybrid system.

Despite their contributions, these associations also face **challenges** emblematic of hybrid organisations. One challenge is maintaining **financial and organisational sustainability**. As NGOs, they rely on membership dues, project grants, or partnerships; funding can be uncertain, which might limit their programming or staffing. They must also continually renew their membership base, attracting young artists and critics to join and participate, so that the association remains representative and does not ossify into a club of veterans. This is particularly crucial, as the younger generation's professional life may look very different (more gig-based, digitally oriented) than that of older members. Another challenge is **managing internal diversity and potential conflicts**. In ZASP's case, divisions within the theatre community (perhaps between those who prioritise traditional repertoire and those pushing experimental work, or regional differences) can hamper unified action. The critics' section must balance academic theatre scholars, journalistic reviewers, and bloggers or new-media critics, ensuring its scope evolves with the field. These internal tensions reflect a tradition versus innovation dichotomy: not all members value the same aspects equally, so leadership must negotiate a consensus on the association's direction.

Lastly, the broader **socio-political climate** affects the effectiveness of these associations. For example, if government cultural policy becomes less consultative or more politically driven (as has happened at times in Poland), associations might find it harder to have their voices heard. Conversely, strong support for culture at the policy level (such as increased funding for NGO-led cultural projects or inclusion of associations in strategy councils) can empower them. Being hybrid, they are somewhat vulnerable to shifts in both the state and market: an economic downturn might reduce sponsorship and member contributions. In contrast, a policy shift might reduce their formal roles.

CONCLUSION

The role of creative associations like ZASP and the Polish Section of AICT/IATC in Poland's theatrical life underscores the importance of **hybrid organisational structures** in contemporary culture. These two cases show how such associations serve as **custodians of tradition**, carrying forward the legacies of Polish theatre through remembrance, standards, and support for veteran artists and critics. Simultaneously, they act as **agents of innovation**, whether by integrating new technological and economic practices (e.g., digital rights management, online criticism) or by championing new voices and forms (through training programs and modern awards). In the hybrid organisation of Polish theatre, neither the state nor the market alone could quicklyfulfil these nuanced roles – it is thethird sector**, creative associations**, that fill the gaps, bridging realms and translating between the old and the new.

ZASP's century-long experience reflects the evolving contract between artists and society: from securing fundamentallabour rights in early 20th-century theatres, through surviving political turmoil, to adapting to today's creative economy. The Polish AICT section mirrors a parallel journey for the critical community: from a club of intellectuals navigating communist restrictions to a forward-looking network that merges scholarship with digital-era cultural journalism. Both associations demonstrate resilience and adaptability, key traits of hybrid organisations that thrive on **combining multiple organisational forms to create value**. Their stories highlight that sustaining a vibrant theatrical culture requires more than just great performances on stage; it also needs a supportive*off-stage infrastructure*of associations, dialogues, and collective efforts.

In contemporary cultural policy, empowering such creative associations can be seen as investing in

the **social capital of culture** the relationships, knowledge, and norms that help the cultural sector function and innovate. However, as this study has noted, there is a continual need to assess and bolster their effectiveness. Encouraging broader membership participation, ensuring intergenerational transfer of leadership, and facilitating constructive partnerships with state institutions are all ways to strengthen these mediating organisations. With its strong theatrical heritage and dynamic new arts scene for Poland, harnessing the full potential of groups like ZASP and the AICT section could mean a more robust dialogue between its illustrious past and its creative future. In conclusion, creative associations play a key role as interlocutors in the hybrid cultural system – by honouring tradition while embracing change, they help ensure that theatrical art in Poland remains both rooted and evolving in the 21st century.

REFERENCES

[1] **Miłkowski, T.**(2020). *POLAND: Internet-theatre and Insufficient State Support for the Artists*.**Critical Stages**, 21 (June 2020). (critical-stages.orgcritical-stages.org). *(National report on the state of Polish theatre during COVID-19, by the President of the Polish AICT section.).*

[2] **Kostrubiec, M.** (2017).*ZASP – Stowarzyszenie Polskich Artystów Teatru, Filmu, Radia i Telewizji. Wyzwania u progu stulecia organizacji* [Master's thesis, Jagiellonian University]. (ruj.uj.edu.pl , ruj.uj.edu.pl). *(Academic study examining ZASP's history, legal status, and influence on cultural policy as it approached its 100th anniversary.).*

[3] **Polskie Radio 24.** (2024, January 23). *Dr Tomasz Miłkowski on the history, mission and activities of the Theatre Critics Association* (interview). (polskieradio24.pl , polskieradio24.pl). *(Radio interview with the Polish AICT section's chairman, discussing the section's legacy and current work, in Polish.).*

[4] **Tsanos, C., et al.** (2024).*Hybrid organisations: a classification within economic sectors*.**Humanities& Social Sciences Communications, 11**(1). (nature.comnature.com). *(Academic article providing definitions and context for hybrid organisations in economic and institutional terms.).*

Konrad Szczebiot: https//orcid.org/0000-0002-9833-5583

"THEY DON'T SEE THE REAL ME!" STUDENT VOICES ON BEHAVIOUR AND BELONGING

Simon FARRUGIA[1], Bernice PIZZUTO[2]

Malta Leadership Institute, School for Educational Studies, Malta[1]
Learning Support Educator, St. Patrick's Salesian School, Malta[2]
farrugia.sim@gmail.com1, pizzutobernice@hotmail.com[2]

ABSTRACT: Students with social, emotional, and behavioural difficulties (SEBD) are often viewed through a deficit-based lens of disruption and non-compliance; their inner experiences remain largely unexamined in educational discourse (Cefai & Cooper, 2006; Charalambous, 2018). This study addresses a critical gap by foregrounding the voices of secondary school students in Malta who have been identified as exhibiting SEBD, exploring their lived experiences of behaviour, belonging, and support. Drawing on a qualitative design that included focus groups, journaling, and ethnographic classroom observations, this study examined how these students perceive their challenges and what strategies they consider most helpful for engagement.

Thematic analysis revealed five interconnected themes: emotional distress misinterpreted as defiance; anxiety and overwhelm; mistrust and withdrawal; autonomy-seeking behaviours; and internalised failure linked to disconnection. Students identified significant strategies that supported their participation,such as emotionally safe spaces, interactive and flexible lessons, movement breaks, and relational trust, reinforcing findings from recent trauma-informed and student-centred research (Blackwell et al., 2019; Kearney & Lanius, 2022; Pizzuto, 2023). These strategies align with the core principles of Maslow's hierarchy of needs and the psychosocial model, emphasising the foundational role of emotional safety, autonomy, and belonging in educational engagement (Eiroa-Orosa, 2020; McLeod, 2024).

Rather than interpreting SEBD as inherent pathology, this study reframes behaviour as relational communication and inclusion as a practice of connection. In doing so, it contributes to growing calls for participatory and trauma-informed responses to behaviour that centre student agency and dignity (Council of Europe, 2023). This research offers practical implications for educators and policymakers seeking to shift from compliance to compassion and from control to meaningful engagement.

Keywords: SEBD, student voice, behaviour, engagement, inclusion, trauma-informed, Malta, ethnography.

[1] Simon Farrugia is an author and lecturer at the Malta Leadership Institute where he teaches courses related to the field of education. His research interests lie in ethnomusicology, particularly Maltese musical traditions, audiovisual research, and the semiotics of music, and in education, with an emphasis on inclusion, creativity, and the sociology of schooling. His academic work includes a television documentary series on world music and a co-authored book on Maltese historical anthropology, in addition to several publications in music education and ethnomusicology. His most recent publication is the monograph The Maltese Wind Band: A Musical Tradition and Its Practice Today (McFarland, 2023) as well as the ethnographic film Sounds of Weeping: Funeral Marches in Maltese Society and Culture which premiered at the 48th International Council for Traditions of Music and Dance world conference in January 2025 in Wellington, New Zealand. He also serves on the Malta National Committee of RILM (Répertoire International de Littérature Musicale).

[2]Bernice Pizzuto is a learning support educator (LSE) with over 12 years of experience in inclusive education. She holds a B.A. (Hons) in Inclusive Education and a master's degree in inclusive education, specialising in challenging behaviour. Passionate about supporting students with behavioural difficulties, she is dedicated to fostering inclusive learning environments that empower all learners to thrive.

INTRODUCTION

Students who exhibit social, emotional, and behavioural difficulties (SEBD) are often defined by the challenges they pose rather than the needs they express. Dominant narratives within education tend to characterise these students through disruption, oppositionality, or non-compliance, frequently resulting in responses centred on control and discipline. Yet such perspectives overlook the emotional and relational dimensions that underpin their behaviour (Cefai & Cooper, 2006; Pizzuto, 2023). Although inclusive education policies across many systems, including Malta's, promote access and equity, students with SEBD remain among the most marginalised, experiencing disproportionate rates of exclusion, academic underachievement, and social isolation.

Many of these students contend with complex adversities, including trauma, instability, and unresolved emotional needs, which can manifest as dysregulation or disengagement within the classroom. However, these behaviours are often misinterpreted as defiance or apathy rather than understood as expressions of emotional distress. As argued in recent research, behaviour should be recognised not merely as an action to be managed but as communication to be understood (Cooper, 2003). Despite increasing awareness of trauma-informed and relational approaches, prevailing school practices often continue to emphasise compliance over connection.

We argue that meaningful inclusion for students with SEBD must extend beyond physical integration into mainstream classrooms;it requires an adapted, student-informed, and relationship-centred approach to engagement and support. This perspective is in line with the ecological view presented in Pizzuto's (2023) work, which emphasises the dynamic interplay between students' inner experiences, school culture, and educator attitudes.

This paper contributes to the growing body of research that foregrounds students' voices in understanding and responding to SEBD. Through a qualitative methodology combining focus groups, reflective journaling, and ethnographic observation, we explore how students themselves make sense of their school experiences and what conditions they believe support their ability to learn and belong. Our findings reaffirm the need to position behaviour within a relational, trauma-informed, and participatory framework. In doing so, we invite a reframing of behavioural support, one that moves from punishment to presence and from exclusion to understanding.

The scope of this study is focused on understanding how secondary school students in Malta who have been identified as exhibiting social, emotional, and behavioural difficulties (SEBD) experience school life. By foregrounding their own stories, this study seeks to uncover the emotional, relational, and pedagogical factors that affect their sense of belonging and engagement. The central research question guiding this inquiry is: how do students with SEBD interpret their own behaviour and what do they perceive a being helpful or harmful in supporting their inclusion and engagement in school?

1. REVIEW OF RELEVANT LITERATURE

Social, emotional, and behavioural difficulties (SEBD) encompass a spectrum of behaviours, such as defiance, withdrawal, aggression, and emotional dysregulation, that interfere with a student's ability to engage meaningfully in school. These behaviours are not typically rooted in deliberate disruption but often arise from underlying emotional distress, trauma, or neurodevelopmental conditions (Cefai & Cooper, 2006; Charalambous, 2018). Students with SEBD are disproportionately affected by school exclusion, academic underachievement, and long-term social marginalisation (Hornby, 2014). In Malta, approximately 5–6% of students experience significant behavioural or emotional challenges, but their access to support remains inconsistent across educational contexts.

Traditionally, SEBD has been approached through a deficit model, framing behavioural issues as problems within the child that must be corrected through control and compliance measures (Cooper, 2003). However, this perspective overlooks the emotional, relational, and environmental contexts in which behaviours emerge. Despite their limited long-term efficacy, punitive strategies such as detentions and suspensions are still widely used, potentially exacerbating students' feelings of disconnection (Hornby, 2014). Contemporary literature increasingly challenges this model, advocating

for a relational and ecological approach to behaviour instead. In this framework, students are situated within a system of interacting influences, including family dynamics, school culture, peer interactions, and teacher-student relationships. Rather than being seen as inherently problematic, behaviour is understood as a communication of unmet needs (Charalambous, 2018).

A significant gap in existing research concerns the lack of student voice in shaping educational responses to SEBD. Traditionally, the views of educators, administrators, and clinicians have dominated the discourse, while the perspectives of students especially those deemed disruptive remain marginalised (Traylor et al., 2022). This exclusion risks the implementation of strategies that fail to resonate with students' lived realities. In contrast, participatory research has demonstrated that students with SEBD possess valuable insights into their own emotional triggers, social needs, and learning preferences. Their reflections challenge deficit-based and behaviourist interpretations and promote the adoption of more inclusive, context-sensitive practices (Blackwell et al., 2019).

Several theoretical frameworks inform this relational and student-informed perspective on SEBD. Maslow's hierarchy of needs, for example, asserts that learning is contingent upon the satisfaction of foundational human needs, including safety, belonging, and esteem (McLeod, 2024). Students whose basic emotional or physiological needs are unmet may struggle to regulate behaviour or engage cognitively in the classroom. Therefore, emotional safety and relational trust are prerequisites for academic engagement, especially for students who have experienced instability or trauma (Stoewen, 2024).

Trauma-informed education builds upon this foundation by recognising the impact of adverse childhood experiences (ACEs) on behaviour and learning. Trauma can manifest as hypervigilance, impulsivity, defiance, or withdrawalsymptoms often mistaken for deliberate misbehaviour (Kearney & Lanius, 2022). Effective trauma-informed practices emphasise co-regulation, predictability, and emotional sensitivity. Frameworks such as the Pyramid Model provide educators with concrete strategiessuch as morning check-ins, calming spaces, and relational repair conversationsto foster resilience and inclusion (Morris et al., 2021).

In addition, mentalisation theory offers insight into how students make sense of their own thoughts and those of others. Traumatic experiences can impair a child's ability to reflect on mental states, leading to misinterpretations of social cues and difficulties with emotional regulation (Fonagy & Allison, 2011). Educators who support mentalisation by encouraging perspective-taking and emotional literacy contribute to more stable classroom dynamics (Karagiannopoulou et al., 2024). These relational practices help students develop a coherent self-concept and foster trust in others, both of which are crucial for students navigating social and behavioural challenges.

The psychosocial model complements these theories by integrating individual, relational, and systemic dimensions of behaviour. Rather than pathologising students, it considers behaviour in light of personal history, environmental stressors, and structural inequalities (Eiroa-Orosa, 2020). In educational settings, this approach requires a shift from behaviour management to behaviour understanding, recognising that disengagement, resistance, or aggression may reflect deeper needs for autonomy, fairness, and belonging.

These theoretical perspectives converge in support of inclusive, student-informed strategies for addressing SEBD. A key shift involves moving from control to co-regulation. Instead of punitive measures, students benefit from access to calming tools, sensory breaks, and relational cues that help regulate emotions and prevent escalation (Strickland-Cohen et al., 2022). Another shift calls for moving from teacher-directed instruction to student-centred learning. Flexible lesson design, multimodal tasks, and student input reduce resistance and promote ownership over learning (Sellman, 2009). Finally, shifting from passive reception to active participation is essential. Reflective journaling, peer-led discussions, and feedback sessions give students voice and agency, building trust, motivation, and inclusion (Igel, 2019).

Although theory and policy have evolved, practice often lags behind. This study addresses that gap by foregrounding the lived experiences of students with SEBD, exploring how they perceive their

challenges and what conditions they believe best support their sense of engagement, safety, and belonging.

2. METHODOLOGY

2.1. RESEARCH DESIGN

We adopted a qualitative, interpretivist research design to explore the lived experiences of secondary school students with social, emotional, and behavioural difficulties (SEBD). The main aim was to understand how these students interpret their own behaviour and identify what supports or hinders their sense of engagement and belonging in school. Rather than seeking generalisable patterns, our research prioritised depth, context, and meaning, situating students as knowers of their own experience.

An interpretivist paradigm was chosen to position student perspectives as valid and complex sources of knowledge rather than data to be measured against adult-defined norms. This approach allowed for a richer, more nuanced understanding of behaviour as socially and emotionally constructed (Nickerson, 2024). This study was exploratory and inductive, grounded in the conviction that those most affected by educational policy, students, must be central to any conversation on inclusion.

2.2. RESEARCHER POSITIONALITIES

This research was shaped by the authors' professional experiences and relational commitments to students exhibiting social, emotional, and behavioural difficulties (SEBD). For Farrugia, the impetus emerged during his early years of teaching when he encountered a student who routinely arrived at school without lunch and exhibited signs of profound emotional distress. Believing that the educator's role extends beyond academic instruction, he provided the student with a daily meal over a 5-year period and coordinated pastoral care with guidance personnel. As trust gradually developed, the student moved from social withdrawal to relational connection; an experience that underscored how consistent and compassionate presence can serve as a foundation for engagement and inclusion.

Pizzuto, with over 12 years of experience as a learning support educator, developed her interest in this field through daily encounters with students whose behaviours were often misinterpreted as defiance. Her own personal experiences of having little understanding or support for emotional challenges during schooling further motivated her to explore the inner lives of students with SEBD. This personal and professional trajectory fostered a deep interest in trauma-informed and relational approaches to education, grounded in the belief that students' behaviours are often expressions of unmet emotional needs (Kearney & Lanius, 2022; Stoewen, 2024).

Together, these positionalities shaped the interpretive stance of the study, embedding empathy, reflexivity, and care into both the research design and the analysis of student narratives. This alignment with interpretivist and participatory paradigms (Braun & Clarke, 2019; Nickerson, 2024) reflects the authors' commitment to understanding behaviour not as a disruption to be managed but as a message to be heard.

2.3. PARTICIPANTS AND SAMPLING

The study focused on six Year 11 students (aged 15–16) enrolled in an inclusive secondary school in Malta. Each had been identified by their educators as exhibiting SEBD, often co-occurring with ADHD, prior trauma, or disconnection from traditional classroom settings. The school context was characterised by small class sizes (approximately 15 students per cohort) and access to a multidisciplinary team including learning support educators (LSEs), counsellors, and therapists.

We employed a convenience sampling approach which,while limiting the potential for broad generalisability,enabled the lead researcher, already a familiar and trusted adult within the school, to develop authentic rapport with participants. The selected students represented a range of behavioural and emotional profiles, thereby providing a rich cross-section of experiences within the small sample. In qualitative research, especially when working within an interpretivist framework and exploring vulnerable

populations such as students with SEBD, depth and richness of data are prioritised over breadth (Aspers & Corte, 2019). The use of a small purposefully selected sample enabled the collection of detailed, context-sensitive insights while maintaining ethical sensitivity and emotional safety. Furthermore, triangulation across multiple data sources throughfocus groups, journals, and ethnographic observationenhanced the robustness of findings, compensating for the limited number of participants and supporting thematic saturation within this specific school context.

2.4. DATA COLLECTION METHODS

We used a multi-method approach to collect qualitative data, combining focus groups, student journaling, and ethnographic observation.

2.5. FOCUS GROUP

A semi-structured focus group was conducted with all six students. The group format encouraged collaborative reflection, prompting participants to build on each other's perspectives and generate shared meaning. The discussion, lasting approximately 1 hour, centred on school experiences, emotional triggers, perceptions of behavioural responses, and classroom relationships. It was audio-recorded with full informed consent and transcribed verbatim.

2.6. REFLECTIVE JOURNALING

Following the focus group, students were invited to keep weekly reflective journals over a period of 3 months. These journals included written reflections, illustrations, and free-form expressions relating to their daily experiences of school, emotions, and interpersonal encounters. Journaling was chosen for its accessibility to students who may find verbal communication challenging (Baikie & Wilhelm, 2005). Entries were anonymised and incorporated into the thematic analysis.

2.7. ETHNOGRAPHIC OBSERVATION

The ethnographic dimension of the research was carried out by Farrugia who has taught music from early years through to secondary education for over a decade. With a background in ethnomusicology and a broader interest in anthropological approaches to education, his professional experience informed a series of classroom observations conducted across multiple secondary schools in Malta. These observations, which extended over several weeks, involved sustained presence within classrooms, informal conversations with students and staff, and the compilation of detailed field notes documenting student behaviour, teacher responses, and the relational and contextual dynamics influencing engagement.

The triangulation of focus group dialogue, student journaling, and observational data allowed us to capture multiple dimensions of student experience while also cross-validating emergent themes.

2.8. ETHICAL CONSIDERATIONS

This study was conducted in full compliance with ethical research protocols and received formal approval from the Malta Leadership Institute and the school's senior leadership team. Written informed consent was obtained from both participants and their guardians. All participants were provided with clear, accessible information outlining the voluntary nature of the study, their right to withdraw at any stage, and assurances of data confidentiality.

To ensure emotional safety, a school counsellor was available throughout the research process and no questions were designed to elicit disclosure of trauma. All students were assigned a pseudonym. Data was securely stored on password-protected devices and destroyed following the completion of analysis, in line with data protection regulations.

2.9. DATA ANALYSIS

We adopted a reflexive thematic analysis approach (Braun & Clarke, 2019) to examine and synthesise the data. This method supported an iterative and reflective engagement with the material, allowing us to identify and interpret underlying patterns of meaning across the dataset. The six stages of analysis included: (a) familiarisation with the data; (b) generation of initial codes; (c) search for themes; (d) review of themes; (e) definition and naming of themes; and (f) production of a final analytic narrative.

Manual coding was conducted independently and collaboratively, with regular peer debriefing to challenge assumptions and mitigate interpretative drift. Themes were developed inductively and refined through comparison across data sources. Particular attention was paid to emotional tone, metaphor, and recurring expressions of distress, exclusion, or support.

2.10. RESEARCHER REFLEXIVITY

Our research team brought complementary perspectives to the study. Farrugia's professional and ethnographic background provided insider insight into classroom dynamics, while Pizzuto's academic grounding in trauma-informed and relational pedagogies supported interpretative depth. We maintained reflexive journals throughout the process, documenting shifts in interpretation, ethical tensions, and emerging questions. This practice helped ensure transparency, critical distance, and emotional sensitivity in analysing data generated from vulnerable student populations.

3. THEMATIC INSIGHTS

This section presents the key themes that emerged from the analysis of student focus group discussions, reflective journals, and ethnographic observations. The aim was to explore how students with social, emotional, and behavioural difficulties (SEBD) experience school, interpret their own behaviour, and identify the classroom practices that either support or hinder their engagement.

Thematic analysis revealed five dominant and interrelated themes: emotional distress misinterpreted as defiance; anxiety and overwhelm; mistrust and withdrawal; autonomy-seeking behaviours; and internalised failure linked to disconnection. These findings reflect growing research that conceptualises SEBD as relational and contextual rather than merely individual pathology (Cefai & Cooper, 2006; Raudales et al., 2019).

3.1. EMOTIONAL DISTRESS MISUNDERSTOOD AS DEFIANCE

Students consistently expressed frustration at being misunderstood. Their behaviour, often perceived by adults as oppositional, was rooted in emotional dysregulation or internal distress frequently invisible to others.

> "Sometimes I just can't sit still. It's not because I want to annoy the teacher. It's because I feel trapped in my own body." (Student 2)
>
> "People think I like getting into fights, but it's the only way I know to get my feelings out." (Field interview)

These accounts reinforce trauma-informed perspectives which frame such behaviours as expressions of psychological survival rather than deliberate disobedience (Kearney & Lanius, 2022; Charalambous, 2018).

3.2. ANXIETY AND OVERWHELM UNDERMINE PARTICIPATION

Persistent anxiety, often originating from home or past experiences, was a prominent theme. Students reported difficulties concentrating and participating due to constant emotional overload.

"My stomach hurts every morning before school. I'm just always nervous, even if nothing's wrong." (Student journal)

"I try to pay attention, but my brain won't stop thinking about all the things that could go wrong." (Student interview)

These findings align with literature on hypervigilance and trauma responses which highlight how emotional strain disrupts cognitive and behavioural functioning in the classroom (Blackwell et al., 2019; Raudales et al., 2019; Strawn et al., 2022).

3.3. MISTRUST AND WITHDRAWAL AS PROTECTIVE STRATEGIES

Students described deep-seated mistrust of adults and peers, often shaped by inconsistent caregiving or previous relational harms. Withdrawal was used as a means to avoid emotional risk.

"I don't trust adults. They either leave or let you down." (Student)

"It's easier to keep to myself. If I don't talk, I won't get hurt." (Journal entry)

"When people try to be nice, I wonder what they really want." (Field note)

These insights resonate with mentalisation theory which suggests that early trauma can impair relational trust and lead to defensive social withdrawal (Fonagy & Target, 2006; Cruz et al., 2022).

3.4. SEEKING AUTONOMY THROUGH OPPOSITION

Oppositional behaviour was frequently described as an assertion of control in emotionally unsafe environments rather than as defiance. Students resisted instructions they perceived as authoritarian or disconnected from their lived experiences.

"Why should I listen to people who don't even try to understand me?" (Student)

"I say no just to feel like I have a bit of power." (Journal entry)

"I'm tired of being told what to do all the time … I already have that at home." (Field conversation)

The psychosocial model helps explain these dynamics, viewing autonomy and fairness as core psychological needs, especially for students exposed to unpredictability or invalidation (Eiroa-Orosa, 2020; Traylor et al., 2022; McLeod, 2024).

3.5. INTERNALISED FAILURE AND DISCONNECTION UNDERMINE ENGAGEMENT

Many students described persistent feelings of inadequacy often compounded by social isolation. Whether due to exclusion, school transfers, or relational trauma, these experiences contributed to a lack of belonging and reduced motivation.

"Everyone else seems to get it. I just feel dumb." (Student)

"I've already failed so many times — what's the point in trying again?" (Journal entry)

"I sit alone because I don't fit in with anyone." (Student)

"I've moved schools so many times, I stopped trying to make friends." (Student)

These reflections underscore the role of emotional and social belonging in learning. Without a sense of connectedness, students disengage both academically and relationally. As Maslow and others suggest, esteem and belonging are not optional; they are fundamental to development and participation (Weir, 2012; Celestine, 2017; Allen et al., 2021; Council of Europe, 2023; McLeod, 2024).

3.6. SUMMARY OF THEMES

Tab. 1. Summary of themes.

Theme	Core Insight
Emotional distress misread as defiance	Behaviour often reflects emotional suffering not deliberate disruption.
Anxiety and overwhelm	Persistent fear and vigilance impair classroom focus and participation.
Mistrust and withdrawal	Traumatic experiences that harm trust in others often cause students to shut down emotionally
Autonomy-seeking opposition	Resistance reflects the need for voice and fairness in disempowering settings.
Internalised failure and disconnection	Feelings of inferiority and exclusion reduce motivation and belonging.

4. INTERPRETATION AND IMPLICATIONS

This study set out to explore the lived experiences of students with social, emotional, and behavioural difficulties (SEBD), focusing on what they believe supports their learning, wellbeing, and sense of belonging in school. The findings not only validate existing research but expand upon it, offering rich student-informed insights into the nuanced realities often obscured by the label "challenging behaviour".

We argue that behaviour must be reframed as a form of communication rather than a deliberate disruption, often signalling emotional overload, social distress, or an unmet need for connection. This interpretation aligns with the psychosocial model (Eiroa-Orosa, 2020) and trauma-informed frameworks (Kearney & Lanius, 2022) and resonates with Cooper's (2003) critique of control-based disciplinary models. Students in our study frequently described feelings of being overwhelmed, unheard, or misunderstood, conditions which, they explained, triggered behavioural responses misread as defiance or disengagement.

Maslow's hierarchy of needs (McLeod, 2024) provides a useful lens for understanding these accounts. Consistent with this framework, students who felt emotionally unsafe or socially excluded were unable to regulate or participate effectively in class. Our findings reinforce Pizzuto's (2023) argument that emotional safety must precede learning and inclusion. For these students, predictability, consistency, and relational trust emerged as non-negotiable prerequisites for engagement.

We also highlight the importance of autonomy and student agency in reducing resistance. Students repeatedly emphasised their need for choice and voice in their educational experience,confirming earlier research by Sellman (2009) and Traylor et al. (2022) and echoing Pizzuto's (2023) findings on the impact of participatory practice in behaviour support. When students are active contributors to their learning environment, their sense of ownership and regulation tends to increase.

Trauma-informed approaches surfaced as particularly salient across both our data and the wider literature (Morris et al., 2021). Small but consistent interventionssuch as movement breaks, quiet spaces, and relational check-insproved effective in supporting emotional regulation. These practices align with Strickland-Cohen et al.'s (2022) emphasis on co-regulation as a foundational principle for behaviour support.

A central thread running through the data was the role of teachersnot only in managing behaviour but in shaping students' emotional landscapes. Students perceived calmness, fairness, and relational consistency as signs of safety while sarcasm, shouting, or punitive measures often led to withdrawal or escalation. This affirms the value of relational pedagogy (Farmer et al., 2016), positioning teaching as a practice rooted in trust, not control.

Farrugia's ethnographic observations provided a vital layer of contextual understanding. Drawing on his background in music education and anthropological approaches to schooling, these extended observations documented how withdrawal, humour, and resistance often functioned as protective strategies in unpredictable environments. These insights reinforce Pizzuto's (2023) findings regarding

the emotional labour students perform in maintaining safety, particularly in settings that lack relational continuity.

This study contributes to educational theory and practice in several ways. Firstly, it offers a nuanced and reflexively analysed account of SEBD rooted in student voice. Secondly, it validates the integration of trauma-informed and relational approaches as essential to inclusive practice. Thirdly, it challenges deficit-based interpretations of behaviour, positioning students not as passive subjects of intervention but as co-constructors of meaning. Finally, it affirms that inclusive education is not merely a matter of access or policy compliance;it is a daily practice of presence, dialogue, and mutual recognition.

We hope this study encourages educators to reconsider student behaviour through a trauma-informed lens, one that centres student voice, fosters trust, and holds space for the complexity of each learner's story. When behaviour is seen as a relationship to be understood rather than as a problem to be solved, schools can become sites of restoration rather than exclusion.

5. CONCLUDING REFLECTIONS AND PRACTICAL IMPLICATIONS

This study set out to explore how students with social, emotional, and behavioural difficulties (SEBD) make sense of their own behaviour and what they believe helps them feel supported, safe, and engaged in school. Through focus groups, reflective journaling, and ethnographic observation, we gathered a nuanced understanding of how emotional distress, anxiety, mistrust, and social disconnection shape students' experiences of education. Their accounts confirmed that what is often labelled as defiance is, in many cases, a communicative expression of unmet needs or a protective strategy developed in response to relational and environmental adversity.

Our findings affirm that effective support for students with SEBD must move beyond behavioural management and instead prioritise relational, trauma-informed, and student-centred approaches. Students did not ask for fewer rules or lower expectations; rather, they asked to be treated with fairness, consistency, and respect. They articulated a clear desire to be active participants in their learning environments and to be understood within the broader context of their emotional and social lives. In this sense, inclusion must be enacted not only through policy and placement but through everyday practices that communicate care, value, and trust.

As Pizzuto (2023) argues, true inclusion rests on emotional safety, sustained adult presence, and authentic listening. Farrugia's ethnographic observations similarly revealed that simple actssuch as sharing meals, acknowledging student work, or allowing space for regulationcan profoundly shape a student's ability to remain connected and engaged. When teachers embrace these principles, classrooms can become places of co-regulation rather than conflict, dialogue rather than discipline, and belonging rather than alienation.

Inclusion, then, must be more than a procedural aim; it must be grounded in a commitment to human dignity and the recognition of each student's inherent worth. We hope this study contributes to an ongoing shift in how behaviour is understood and addressed, placing student voice at the centre of educational response and viewing behaviour not as a problem to be fixed but as a story to be heard.

5.1. RECOMMENDATIONS

Informed by the study's findings and supported by the wider literature, the following recommendations are intended to guide educators, school leaders, and policymakers in developing more inclusive, student-informed approaches to behaviour and belonging.

5.1.1. EMPOWER STUDENT VOICE AND AGENCY

1. Centre student voice in behavioural policy and classroom practice. Schools may benefit from involving students in shaping behavioural expectations and restorative processes. Tools such as reflective journaling, class dialogue circles, and student-led feedback sessions can foster agency and accountability. When students feel genuinely heard, their sense of ownership and motivation tends to increase.

2. Design lessons that prioritise engagement and flexibility. Teaching strategies could reflect students' interests, strengths, and preferred learning styles. Incorporating multimodal tasks, movement-based activities, and opportunities for creative expression, such as through music or media, has the potential to improve focus, participation, and intrinsic motivation, particularly among learners with SEBD.

5.1.2. APPLY TRAUMA-INFORMED AND RELATIONAL APPROACHES

1. Adopt trauma-informed, needs-responsive strategies. Classrooms should be structured around consistent routines, predictable boundaries, and access to regulation toolssuch as quiet zones, sensory support, and movement breaks. In instances of behavioural escalation, co-regulation strategies may be more effective than punitive measures.
2. Invest in relational pedagogy and professional development. Teachers play a key role in fostering emotional safety. Professional development in areas such as trauma-informed education, de-escalation techniques, and relational communication should be collaborative and ongoing. Reflection on tone, body language, and relational dynamics is also essential for sustaining inclusive environments.

5.1.3. RETHINK INCLUSION AS EMOTIONAL AND RELATIONAL PRESENCE

1. Foster a classroom culture of belonging. Inclusive education is strengthened when student contributions are celebrated, peer collaboration is encouraged, and emotional check-ins are embedded into daily practice. Small gestures of connection, such as personal greetings, acknowledgement, and consistency, can profoundly impact students' sense of being valued.
2. Redefine how inclusion is evaluated. Attendance or physical placement alone does not equate to meaningful inclusion. Schools should consider additional indicators such as student agency, emotional wellbeing, and relational connectednessused in tandem with academic metricsto evaluate inclusive success more holistically.

5.2. ACKNOWLEDGEMENTS

We would like to sincerely thank the students who participated in this study for their openness, trust, and courage in sharing their experiences. Our gratitude also extends to the school leadership team, learning support educators, and counsellors who facilitated access and supported the research process with care and professionalism. We are also grateful to the Malta Leadership Institute for its academic guidance and ethical oversight.

REFERENCES

[1] K. A.Allen, C. D.Slaten, G.Arslan, S.Roffey, H.Craigand D. A. Vella-Brodrick, (2021),"School belonging: The importance of student and teacher relationships', In M. L. Kern and M. L. Wehmeyer (Eds.), The Palgrave Handbook of Positive Education (pp. 525–550), Palgrave Macmillan. https://doi.org/10.1007/978-3-030-64537-3_21

[2] P.Aspers, andU. Corte, (2019),"What is qualitative in qualitative research," Qualitative Sociology, vol. 42, https://doi.org/10.1007/s11133-019-9413-7, no. 2, pp. 139–160.

[3] K. A. Baikie and K. Wilhelm, (2005),"Emotional and physical health benefits of expressive writing," Advances in Psychiatric Treatment, vol. 11, https://doi.org/10.1192/apt.11.5.338, no. 5, pp. 338–346.

[4] Belong Partners, (2022, October 17). Five ways to encourage student voice and share power in the classroom. Retrieved from https://belongpartners.org/student-voice-and-share-power/

[5] W. Blackwell, J. Betancourt Durán andJ. Buss, (2019),"Students with emotional and behavioural disorders and special education due process in the United States," International Journal of Special Education, vol. 34, https://files.eric.ed.gov/fulltext/EJ1237120.pdf,no. 1, pp. 33–47.
[6] V. Braun andV. Clarke, (2019),"Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health,"vol. 11, https://doi.org/10.1080/2159676X.2019.1628806,no. 4, pp. 589–597.
[7] C. Cefai andP. Cooper, (2006),"Social, emotional and behavioural difficulties in Malta: An educational perspective," Journal of Maltese Education Research, vol. 4, https://www.mreronline.org/wp-content/uploads/2013/07/JMERN4I1P21.pdf,no. 1, pp. 18–36.
[8] P. Cooper, (2003), Understanding and supporting children with social, emotional and behavioural difficulties, 2nd ed., UK: Jessica Kingsley Publishers.
[9] N. Celestine, (2017, September 29), Abraham Maslow, his theory & contribution to psychology [Upd. 2019]. Positive Psychology. Retrieved from https://positivepsychology.com/abraham-maslow/
[10] A. Charalambous, (2018),"Identification and assessment of social, emotional and behavioural difficulties (SEBD) among children with and without special educational needs (SEN) based on parent and teacher perceptions: A comparison study," [Doctoral dissertation, The Open University]. Open Research Online. https://oro.open.ac.uk/62408/
[11] Council of Europe, (2023), Improving well-being at school. Democratic Schools for All. Retrieved fromhttp://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/improving-well-being-at-school
[12] D. Cruz, M. Lichten, K. Berg and P. George, (2022),"Developmental trauma: Conceptual framework, associated risks and comorbidities, and evaluation and treatment," Frontiers in Psychiatry, vol. 13, https://doi.org/10.3389/fpsyt.2022.800687,no. 800687.
[13] F. J. Eiroa-Orosa, (2020),"Understanding psychosocial wellbeing in the context of complex and multidimensional problems," International Journal of Environmental Research and Public Health, vol. 17, https://doi.org/10.3390/ijerph17165937, no. 16, pp. 5937.
[14] R. Farmer, A. L. Chapman and American Psychological Association, (2016), Behavioural interventions in cognitive behaviour therapy: practical guidance for putting theory into action.American Psychological Association.
[15] S. Farrugia, (2020),"Some deliberations concerning the value and motivation of music education" [Unpublished manuscript]. University of Malta.
[16] P. Fonagy and E. Allison, (2011),"What is mentalization? The concept and its foundations in developmental research and social-cognitive neuroscience." UCL Discovery. https://discovery.ucl.ac.uk/id/eprint/1430329/
[17] P. Fonagy and G. Target, (2006), The mentalization-focused approach to social development, Handbook of Mentalization-Based Treatment, 1st ed. UK: John Wiley & Sons.
[18] L. S. Ho, (2009),"A cry for help: The perspective and experiences of primary school children with challenging behaviour within the Cottonera area." [Master's dissertation, University of Malta]. University of Malta Library. https://www.um.edu.mt/library/oar/bitstream/123456789/71611/1/Lai-See_Ho_2009.pdf
[19] G. Hornby, (2014), Including students with significant social, emotional and behavioural difficulties in mainstream school settings.
[20] A. Igel, (2019, January 7),"How to work with learners with SEBD (social, emotional, and behavioural difficulties) in the classroom," Teaching English with Oxford. https://teachingenglishwithoxford.oup.com/2019/01/07/emotional-behavioural-difficulties-classroom/
[21] C. A. Kearney and R. A. Lanius, (2022),"The brain-body disconnect: A somatic sensory basis for trauma-related disorders," Frontiers in Neuroscience, vol. 16, https://doi.org/10.3389/fnins.2022.1015749, Article 1015749.
[22] E. Karagiannopoulou, F. S.Milienos and M.Georgiadi, (2024),"Mentalisation in adolescents: A review of interventions and implications for education," Educational Psychology Review. https://doi.org/10.xxxxxx/xxxxx

[23] S. A. McLeod, (2024, January 24),"Maslow's hierarchy of needs," Simply Psychology. https://www.simplypsychology.org/maslow.html
[24] C. T. Morris, A. Hunte, L. Fox and M. L. Hemmeter, (2021),"The Pyramid Model and Trauma-Informed Care: A guide for early childhood professionals to support young children's resilience."https://www.challengingbehaviour.org/docs/Trauma-Informed-Care_Guide.pdf
[25] C. Nickerson, (2024, February 13),"Interpretivism paradigm & research philosophy," Simply Psychology. https://www.simplypsychology.org/interpretivism-paradigm.html
[26] B. Pizzuto, (2023),"Disengaged or misunderstood? Understanding student behaviour through trauma-informed and relational perspectives" [Unpublished master's dissertation, Malta Leadership Institute].
[27] M. Raudales, D. Davis and S. Frazier, (2019), Understanding trauma and resilience in students, Educational Psychology Review, vol. 31, no. 3, pp. 587–602, USA: Springer.
[28] E. Sellman, (2009,"Lessons learned: Student voice at a school for pupils experiencing social, emotional and behavioural difficulties," Emotional and Behavioural Difficulties, vol. 14, https://doi.org/10.1080/13632750802655687, no. 1, pp. 33–48.
[29] D. L. Stoewen, (2024),"The vital connection between emotional intelligence and well-being - Part 1: Understanding emotional intelligence and why it matters," PubMed, vol. 65, no. 2, pp. 182–184.
[30] M. K. Strickland-Cohen, A. Newson, K. Meyer, R. Putnam, L. Kern, B. Meyer and A. Flammini, (2022),"Strategies for de-escalating student behaviour in the classroom." https://assets-global.website-files.com/5d3725188825e071f1670246/632ccb7a3756f3529d3a7391_Strategies%20for%20De-escalating%20Student%20Behaviour%20in%20the%20Classroom.pdf
[31] J. R. Strawn, J. A. Mills, V. Suresh, T. S. Peris, J. T. Walkup and P. E. Croarkin, (2022,"Combining selective serotonin reuptake inhibitors and cognitive behavioural therapy in youth with depression and anxiety," Journal of Affective Disorders, vol. 298, https://doi.org/10.1016/j.jad.2021.10.047,Part A, pp./ 292–300.
[32] J. Traylor, L. Overstreet and D. Lang, (2022),"Psychodynamic theory: Freud," Iowa State University Digital Press. https://iastate.pressbooks.pub/individualfamilydevelopment/chapter/freuds-psychodynamic-theory/
[33] K. Weir, (2012, April),"The pain of social rejection."https://www.apa.org/monitor/2012/04/rejection

Simon, Farrugia:https://orcid.org/0009-0005-2039-2827
Bernice, Pizzuto:https://orcid.org/0009-0008-2273-241X

DEDICATED DATABASE FOR PERFORMANCE TESTS OF THE TRAINED NEURAL NETWORK MODEL YOLOV11N

Kamil FELTER

Faculty of Computer Science and Technology, University of Lomza, Poland
kfelter@al.edu.pl

ABSTRACT: This article presents an application of the YOLO algorithm for object recognition. To train the algorithm, images of six types of sweets were collected and categorized. Image enhancement using visual effects was then applied. The effectiveness of the learning process was tested, achieving a precision and recoilprec mAP@0.5 level of (72%).

Key words: YOLO, object detection, convolutional neural network

INTRODUCTION

The use of artificial intelligence algorithms in vision systems is now becoming increasingly common. Trained neural networks make it possible, using camera images, to classify individual objects with a high degree of accuracy. One example of a model used for this purpose is YOLO(You Only Look Once). By its open-source nature, it attracts many users. We can see its application in the work presented in the article [1].

Using the YOLOv11n model, a team of researchers prepared an algorithm to detect forest fires in real-time. The database prepared to teach the algorithm contained 3970 annotated images. The classes selected for annotation contained typical elements of fires such as flames or smoke. In the tests, the artificial intelligence algorithm achieved precision of (80%~88%) and repeatability (68%~83%). Tests with real-time fire recognition showed a detection precision of (52%) and repeatability of (28%).

Another interesting example of the application of the YOLOv11 model in object detection is presented in the paper [2]. The paper presents the learning process of a model designed to detect hazards on high-voltage lines. The database was obtained from photographs and video footage. The prepared material included 110 images with hazard cases such as nests, balloons, kites, or rubbish. Training results showed a precision of (93%) and a repeatability of (73%).

DATABASE AND MODEL

This chapter is devoted to the methodology of creating a custom dataset and presenting the model subjected to the learning process for object recognition.The process of data acquisition for learning artificial intelligence algorithms dedicated to object recognition is characterized by relative simplicity. It requires the collection of digital image representations, which can take the form of video sequences or single frames. The source material can be acquired using commonly available devices, such as cameras embedded in mobile phones, allowing the target objects to be recorded. It should be noted that a prerequisite is that images with a fixed resolution of 640x640 pixels are supplied to the algorithm. Consequently, the acquired images are subject to a scaling operation, regardless of their original resolution. A diagram of the described preparation process is illustrated in Figure 1.

Fig. 1. Preppering process for custom database.

Nevertheless, it should be noted that the specifics of this process may be modified depending on the individual needs and requirements of the implemented algorithm. The next step is to prepare the raw visual material for the model learning process. In the case of data extracted from video recordings, it is necessary to extract individual frames and save them in a graphic file format using a bitmap representation. In the situation where static images are used, it is recommended to avoid elements in excessively high resolutions. Once a set of images has been collected, it is recommended practice to organize them by giving them sequential numerical names. This approach systematizes the identification of individual elements of the dataset.

The prepared images are then subjected to a labeling process. Labeling involves an operator (human) assigning identifiers to objects present in the images, based on defined criteria. An example is the identification of an object based on its color, shape, or type, as shown in Figure 2.

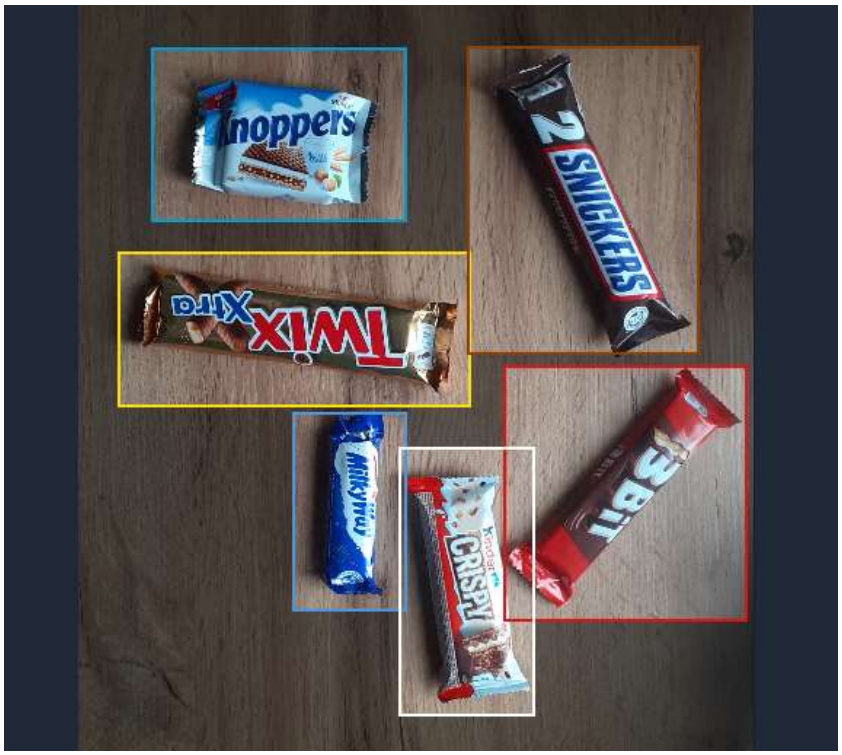


Fig. 2. Labelling objects.

This process aims to teach the algorithm to recognize objects in a way analogous to human perception. Dedicated software tools such as Roboflow [5] or Label Studio are available for tagging. Increasing the size of the training dataset in the learning process of neural networks is often achieved by using image augmentation techniques. Among the commonly implemented methods are:

- Blurring: Application of blurring filters to reduce high-frequency components of the image.
- Pixelization (Pixelization): Reduction of image resolution by aggregating groups of pixels, simulating lower-quality data acquisition.
- Rotation (Rotation): Geometric transformation of an image by rotation by a specified angle in the image plane.
- Perspective Transformation (Perspective Transformation): Transformation of image geometry by mapping points from one plane to another, simulating changes in the camera's point of view.
- Scaling (Scaling): Changing the size of an image by zooming in or out, which affects the size of objects in the frame.
- Cutout and Paste of Image Elements (Cutout and Paste): Randomly removing portions of an image and potentially replacing them with elements from other training images to increase the model's resistance to partial occlusions.

The use of the aforementioned image data augmentation operations enables efficient preparation of training material for machine learning algorithms, minimizing the need for time-consuming acquisition of additional data. Moreover, these techniques contribute to increasing the variance of the representation of a given object in the dataset.

After the annotation stage and the application of digital transformations, it is possible to create the structure of the database designed to teach the algorithm. By default, this database consists of three complementary subsets: training, validation, and testing. The proportions of the dataset allocation can be determined empirically; however, typical allocations are shown in Table 1.

Tab. 1. Dataset amoutn by type.

data type	amount
training	60%
validation	20%
testing	20%

A key aspect is to ensure that these subsets are disjunctive; duplication of samples would lead to overestimation of assessment metrics through over-fitting effects. The validation and test subsets should reflect the original data distribution, without applying additional transformations.

Once the database has been completed and structured, the next step is to select a suitable machine-learning model. One commonly used solution is the YOLO family, offered by Ultralytics. This architecture enables the detection, recognition, and classification of objects. The company provides a number of variants of the algorithm, with the latest iteration YOLOv11. Additionally, the model comes in six differentiated versions, detailed in Table 2. For our test, the YOLOv11n version will be chosen because of the learning process time required. YOLO models, depending on the size of the database, can be trained for several to hundreds of hours.

Tab. 2. Preformence of all YOLOv11 models.

Model	**size** (pixels)	**mAP^{val}** 50-95	**Speed** CPU ONNX (ms)	**Speed** T4 TensorRT10 (ms)	**params** (M)	**FLOPs** (B)
YOLO11n	640	39.5	56.1 ± 0.8	1.5 ± 0.0	2.6	6.5
YOLO11s	640	47.0	90.0 ± 1.2	2.5 ± 0.0	9.4	21.5
YOLO11m	640	51.5	183.2 ± 2.0	4.7 ± 0.1	20.1	68.0
YOLO11l	640	53.4	238.6 ± 1.4	6.2 ± 0.1	25.3	86.9
YOLO11x	640	54.7	462.8 ± 6.7	11.3 ± 0.2	56.9	194.9

RESULTS

This chapter presents the methodology and results of the evaluation of the trained YOLOv11n model against a dedicated dataset. Key metrics and aspects of the learning outcome analysis are discussed in detail. The test environment was implemented in Visual Studio, using the Python language and the Ultralytics and PyTorch libraries [4]. The architecture of the underlying model under training was obtained from the Ultralytics repository.

The learning process of the multi-class object detection algorithm, in this case, different types of candy, is illustrated in Fig. 3. It shows the sample size in each of the defined classes, which exceeded the value of 75 per class. The original dataset consisted of 37 images, each containing a single instance of each type of candy. Image augmentation techniques were used to increase the sample counts.

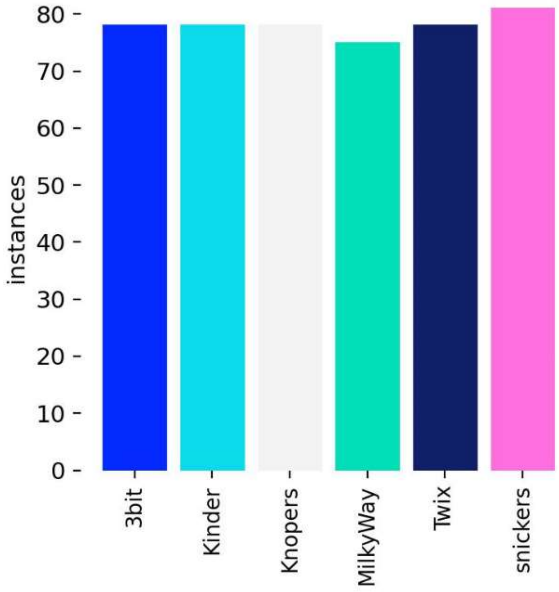


Fig. 3. Amount of classes for every candy.

The in-depth statistics generated during training of the YOLO algorithm, including both graphical visualizations and tabulated data, were used to conduct a detailed comparative analysis of the precision metrics and overall neural network learning efficiency. It is important to note that the percentage presented refers to the detection precision of the defined object categories.

Analysis of the data obtained from the learning process of the YOLO algorithm showed the value of the metric mAP@0.5, which quantifies the model's ability to correctly detect and locate objects with respect to the annotations contained in the image dataset. Values exceeding the threshold (50%) are commonly interpreted as an indicator of high model performance in the detection task. These conclusions were deduced from the analysis of the Precision-Recall curves shown in Figure 4.

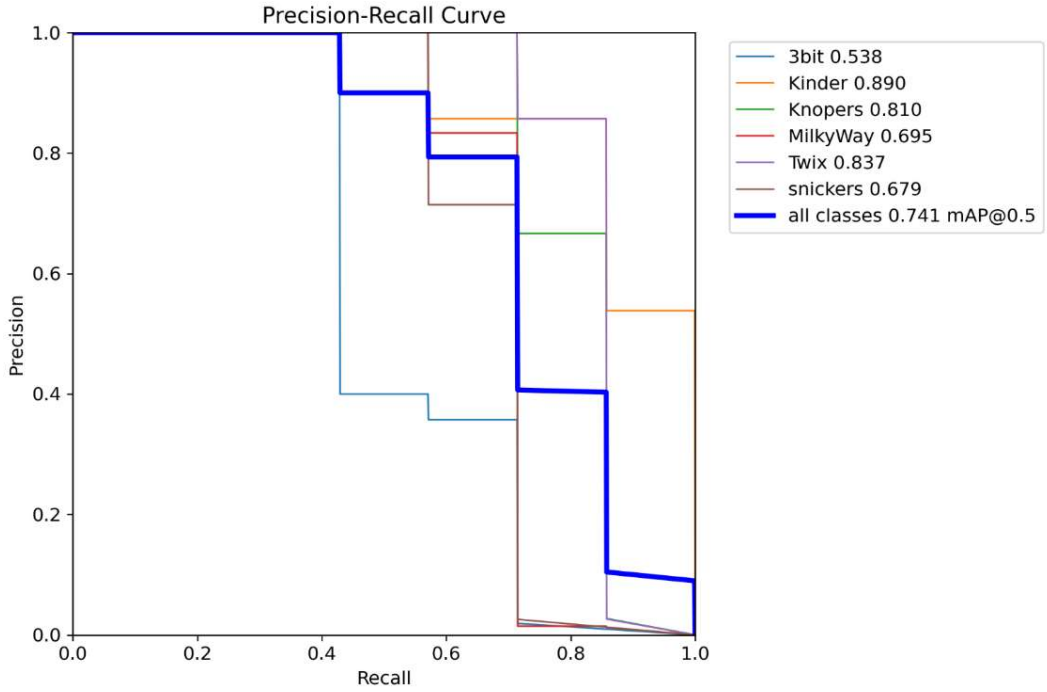


Fig. 4. Precision-Recall Curve for mAP0.50.

The results in Table 3 show the learning results of the algorithm on the prepared candy database. The value mAP@0.5 indicates the algorithm's learning problems for the 3bit class where the result reaches (53%). However, it is acceptable and we can consider that the learning of our algorithm has been completed successfully with a result of (74%) effectiveness for all classes.

Tab. 3. Precision-Recall curve results for all classes.

mAP@0.50	overall	3bit	Kinder	Knopers	Milky Way	Twix	Snickers
YOLOv11n	74%	53%	89%	81%	69%	83%	67%

We must also pay attention to the information we obtained after the learning process in the confusion matrix shown in Figure 5. It allows us to identify the issues our algorithm encountered and the most frequent mistakes in object identification that occurred. All classes obtained recognition scores above (50%). However, we can see that YOLOv11n had difficulties with confusing background elements for all classes (16%~29%). There were also problems with incorrect object detection. A class (Knopers) was confused with a checkout (MilkyWay, Kinder).

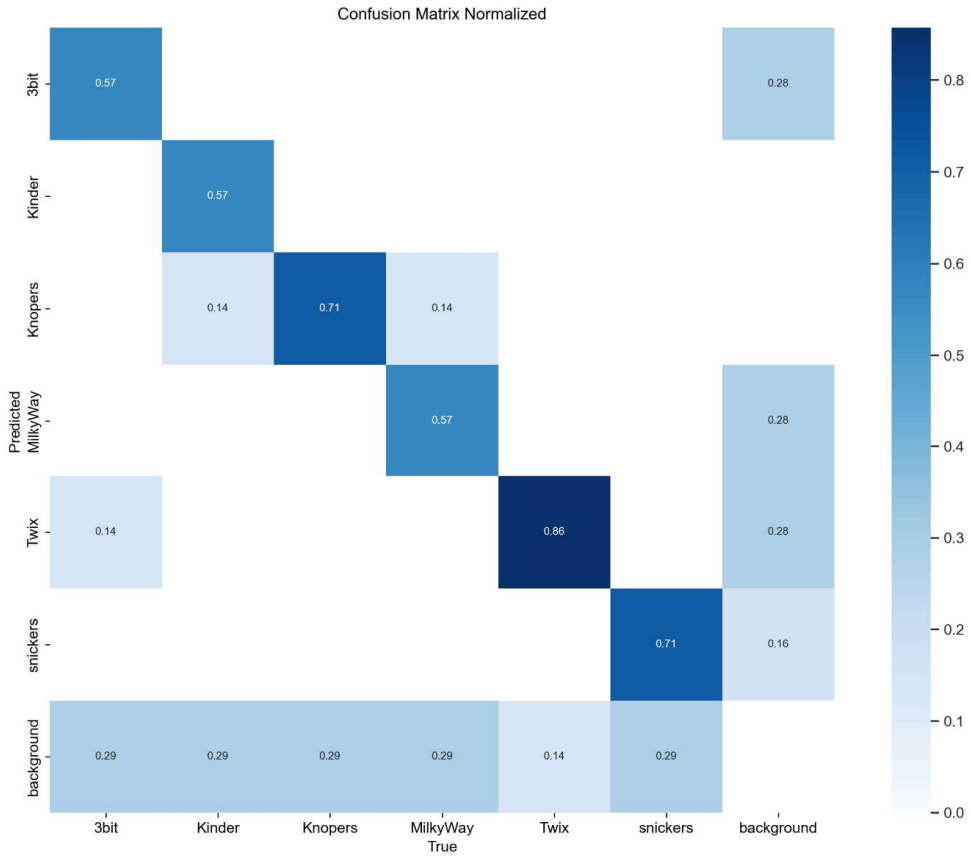


Fig. 5 Confusion Matrix for YOLOv11n model.

CONCLUSION

This article examines the application of artificial intelligence algorithms, in particular the YOLO environment, in the context of object recognition. The analysis carried out demonstrates the growing potential and availability of artificial intelligence methods in everyday applications. As part of the case study, a dataset consisting of photographs of six distinct categories of candy, acquired using a camera embedded in a mobile device, was created. To increase the size of the training samples, the dataset

was subjected to a visual augmentation process. The YOLOv11n model was then taught to recognize the defined object classes. The results showed a mAP@0.5 efficiency of 74%. Difficulties were observed for the algorithm to accurately distinguish classes, resulting in confusion with other objects and background elements. Increasing the volume of training data by including additional images and video sequences was identified as a potential solution.

REFERENCES

[1] Tao Y, Li B, Li P, Qian J, Qi L. Improved lightweight YOLOV11 Algorithm for Real-Time Forest Fire Detection. Electronics [Internet]. 2025 Apr 9;14(8):1508. Available from: https://doi.org/10.3390/electronics14081508

[2] Zou X, Hu Y. Hidden Danger Detection and Identification System of Power Transmission Tower based on YOLOV11. Academic Journal of Science and Technology [Internet]. 2024 Nov 6;13(1):224–31. Available from: https://doi.org/10.54097/rs28p954

[3] Ultralytics. YOLO11 🚀 NEW . 2025. Available from: https://docs.ultralytics.com/models/yolo11/

[4] PyTorch documentation - PyTorch 2.7 documentation [Internet]. Available from: https://docs.pytorch.org/docs/stable/index.html

[5] Roboflow: Computer vision tools for developers and enterprises [Internet]. Roboflow. Available from: https://roboflow.com/

[6] Open Source data Labeling | Label Studio [Internet]. Label Studio. Available from: https://labelstud.io/

Kamil, Felter: https://orcid.org/0009-0004-3903-3165

ADAPTIVE S-BOXES: CONCEPTS AND POTENTIAL IN LIGHTWEIGHT CRYPTOGRAPHY

Wiesław MALESZEWSKI

University of Lomza, Faculty of Computer Science and Technology, Lomza, Podlaskie, Poland
wmaleszewski@al.edu.pl

ABSTRACT

This article gives a detailed analysis of adaptive S-boxes as a contemporary approach to substitution layers in symmetric cryptography. The relevance of using adaptive S-boxes whose structures depend on keys, rounds, or other environmental parameters is their proven ability to strengthen defenses against linear, differential, and even side-channel attacks. A range of construction techniques are reviewed, including context-aware design, key-dependent generation, and chaos-based methods. Some key cryptographic attributes in relation to adaptive systems include nonlinearity, differential uniformity, and avalanche effect. The paper proposes a comprehensive framework for testing adaptive S-boxes that includes analytic measures, attack tests, and ease-of-implementation evaluations.

Key words: adaptive S-box, cryptographic primitives, chaos-based cryptography.

INTRODUCTION

In symmetric cryptography, a nonlinear layer plays a key role in securing the encryption process. The substitution box (S-box) is responsible for introducing confusion, obscuring the relationship between the key and the plaintext. In classic block ciphers such as AES, a predefined and unchanging S-box (designed using mathematical inverses in finite fields and affine transformations) is used. Although fixed S-box designs like that of AES are highly nonlinear and have been extensively vetted, their static nature can become a potential point of attack for increasingly sophisticated analytical and side-channel attacks [1].

To address the vulnerabilities of static S-boxes, researchers have explored adaptive S-box constructions that can change during the encryption process. One approach is to employ key-dependent S-boxes, where the substitution table itself varies based on the encryption key, significantly reducing the efficacy of any precomputed attacks an adversary might use [2]. Another technique involves integrating chaotic maps into S-box design, which has shown promise in increasing the randomness and nonlinearity of the substitution layer and thereby improving resistance to cryptanalysis [3]. This evolving paradigm strengthens the security framework of symmetric cryptography and aligns with the growing need for adaptability in cryptographic systems amidst rapidly advancing attack methods.Driven by rising security requirements – especially in resource-constrained environments like sensor networks and IoT devices – the idea of replacing static S-boxes with more variable solutions has gained traction. An adaptive S-box generates its substitution table depending on certain parameters such as the secret key, the encryption round, input data, or other environmental factors (e.g. time or hardware-specific information). The introduction of such variability makes it far more difficult for adversaries to determine or profile the S-box's properties, thereby raising the bar for various cryptanalytic and side-channel attacks. In particular, a static S-box that remains constant across operations can be profiled and exploited over time, whereas a dynamic S-box that changes with context increases unpredictability and resilience to analysis [6].In terms of flexibility, it is useful to outline what S-box variability entails. In some schemes, the S-box is fully key-dependent, meaning a bijective substitution mapping is generated anew for every encryption session or even each round of encryption. In other approaches, a fixed baseline S-box (such as the AES S-box) is used, but it is dynamically permuted using external inputs like chaotic

map outputs or key-derived permutations. These strategies all aim to inject additional entropy and randomness into the nonlinear layer of the cipher, preventing an adversary from easily identifying or exploiting the S-box through adaptive analysis or side-channel observations.

This review discusses the main classes of adaptive S-box solutions – including key-dependent, dynamic, and environment-dependent designs – and examines their cryptographic properties and resistance to various attacks. We also address implementation challenges and propose a methodology for evaluating the quality and security of such S-boxes.

KEY-DEPENDENT (SESSION-DEPENDENT) S-BOXES

One major class of adaptive S-boxes involves those that depend on the encryption key, changing infrequently – for example, only when a new session key is established. In these key-dependent S-box designs, an optimal S-box is derived from the secret key and is refreshed perhaps each session or encryption round. Because the S-box is effectively unique to the key in use, this approach can dramatically weaken an adversary's ability to perform classical differential or linear cryptanalysis, as the attacker no longer knows the exact substitution layer in advance. Indeed, studies have reported that key-dependent S-boxes effectively obscure the structural vulnerabilities present in static S-boxes by introducing ambiguity into the cipher's design [7]. Additionally, some research indicates higher resilience against side-channel attacks in key-dependent schemes, since the variation in S-box structure can spread the cryptographic operations' physical leakage over a broader range, complicating power or electromagnetic analysis [8].

A key-dependent S-box is typically regenerated whenever the encryption key changes so that an attacker cannot reuse knowledge of a previous S-box for a new key. This subclass of adaptive S-box has been a focus of extensive research due to its practicality – many proposals derive a new 8×8 S-box from each 128-bit key, for instance. One such method chooses from multiple AES-like S-box variants determined by different irreducible polynomials in GF(2^8), with the selection controlled by the key [10]. Other constructions generate the S-box entirely from the key material; for example, Jacob et al. proposed using the standard AES S-box as a starting point and then perturbing its entries with a "codeword" derived from a 64-bit secret key, producing a key-dependent bijective mapping over the 8-bit input space. In round-based ciphers, some have even suggested generating a fresh S-box from each round key for every round of encryption, so that each round uses a different substitution table derived from that round's subkey [3]. This per-round key-dependent approach enhances diffusion and unpredictability across rounds: since each nonlinear layer is both keyed and time-dependent, an attacker without the key cannot reconstruct the substitution table for any given round, greatly increasing the search space and hindering traditional cryptanalytic methods. Empirical studies have shown that ciphers with static S-boxes are more susceptible to structured attacks (for example, exploiting predictable difference distributions), while key-dependent S-box constructions obscure these patterns by introducing uncertainty into the S-box structure [11].

Designing key-dependent S-boxes does come with challenges. The transformation from key to S-box must produce a table that meets rigorous cryptographic criteria (bijectivity, high nonlinearity, low differential uniformity, etc.) for every possible key. Ensuring this can be difficult; for instance, early attempts to use chaotic maps to generate key-dependent S-boxes often resulted in substitution tables with suboptimal properties (e.g. lower than desired nonlinearity), leaving them vulnerable to differential cryptanalysis [12]. Recent research has begun to overcome these issues. It has been demonstrated that carefully integrating chaos into the S-box design can yield highly nonlinear and key-dependent structures that improve security against both differential and linear attacks. For example, Namuq's 2024 design uses 3D chaotic maps to enhance an S-box's nonlinearity and attack resistance [13]. Likewise, other studies highlight the potential of chaos-based key-dependent S-boxes to achieve excellent cryptographic strength when properly constructed [14–16]. In summary, a well-designed key-dependent S-box deprives attackers of a fixed target: without access to the secret key, they cannot know the S-box values, forcing any attack to contend with an unknown and variable nonlinear layer.

DYNAMICALLY UPDATED S-BOXES

Another category of adaptive S-boxes includes those that change more frequently than the key – in some cases, with every encryption round, per message block, or at fixed time intervals. These dynamic S-box designs continually alter the substitution layer during operation (even if the overall key remains the same). For example, a cipher might redefine its S-box for each round using a round counter or a pseudorandom function, or even generate a new S-box for every data block encrypted. This frequent re-initialization injects a high degree of unpredictability and entropy into the cipher's nonlinear component. It has been shown that if each block of data is encrypted with a unique S-box mapping, the statistical relationships that attackers exploit (such as in differential or linear cryptanalysis, or in chosen-plaintext attacks) can be effectively broken because the cipher behaves differently for each block. An adaptive design where the S-box changes on-the-fly forces an attacker to deal with a moving target, significantly increasing the difficulty of mounting effective cryptanalysis.

The main cryptographic merit of dynamically changing S-boxes is the increased difficulty for an attacker to predict or model the cipher's nonlinear transformation. In classical ciphers with a fixed S-box, an adversary can pre-compute properties of the S-box (like difference distributions or linear approximations) and use those in an attack. In a cipher with dynamic S-boxes, however, the substitution table varies with time (e.g. with each round or packet), so the attacker's model must continually adapt. If the S-box is refreshed faster than the attacker can gather sufficient data, traditional differential and linear attack techniques become nearly futile. For instance, in an image encryption system, Wang et al. demonstrated using a new chaotic S-box for each image block so that an opponent, even with full knowledge of the plaintext image, cannot ascertain the substitution table being used for each block [17]. Frequent S-box changes also help mitigate related-key attacks—scenarios where attackers exploit relationships between ciphers under two different keys. In a dynamic S-box scheme, even a small change in the key (or round index) can produce a completely different S-box, meaning an attacker cannot rely on any continuity of S-box structure between related keys. The output distributions and substitution patterns an adversary observes are highly mixed and inconsistent, which greatly weakens statistical evaluations and correlation attacks.

Despite their security advantages, dynamically updated S-boxes introduce practical challenges. Regenerating an optimal 8×8 S-box is a computationally expensive task if done arbitrarily often, and it must be done in a way that maintains strong properties (like bijectivity, high nonlinearity, strict avalanche, etc.) at every update. Moreover, each new S-box must remain secret and be synchronized between the sender and receiver. Some designs address performance concerns by limiting the scope of change—for example, dual S-box schemes use only two S-boxes that alternate or switch under certain conditions, which still adds variability while capping the overhead [18]. Zhu et al. proposed an image encryption scheme using dual chaotic S-boxes derived from a sine–tent chaotic system, achieving a high degree of cryptographic diffusion with less runtime cost by switching between two precomputed chaotic S-boxes rather than generating a completely new one each time. In general, dynamic S-box designs make a trade-off between security and efficiency: they greatly increase attack resistance at the cost of added complexity in the cipher's implementation.

CONTEXT-AWARE (ENVIRONMENT-DRIVEN) S-BOXES

A third class of adaptive S-box designs are those that incorporate external or environmental parameters into the S-box generation. These context-aware S-boxes (also described as environment-driven S-boxes) derive their substitution tables not only from cryptographic keys or algorithmic counters, but also from external data unique to the operating context. Examples include using time stamps, sensor readings, biometric data, or hardware-specific features as part of the S-box generation process. The goal of context-aware S-box design is to introduce an additional layer of uniqueness and unpredictability tied to the system's environment or the user, thereby enhancing security and providing ancillary benefits like device or user authentication.

Such context-dependent S-box schemes have practical applications in anti-counterfeiting and secure

hardware identification. For instance, a cipher might generate its S-box based on a device's physical unclonable function (PUF) output or a user's biometric input, so that the encryption process becomes intrinsically linked to that specific device or person. Leest and Tuyls demonstrated that incorporating hardware-intrinsic parameters can be highly effective in anti-counterfeiting measures, because an attacker cannot replicate the cipher's behavior without access to the same physical context [9]. Another illustrative example is the work of Indumathi and Sumathi, who proposed generating cryptographic S-boxes from fingerprint data. In their scheme, minutiae from a fingerprint (such as ridge bifurcations and endings) are converted into an 8-bit substitution box that is compatible with AES. The resulting S-boxes were reported to meet fundamental security requirements – passing standard randomness tests, achieving high nonlinearity, satisfying the strict avalanche criterion, and exhibiting low differential uniformity – making them as robust as classical S-boxes while being uniquely tied to an individual's biometric data [20]. More generally, using device-specific characteristics (like PUF responses or real-time system metrics) as inputs injects further entropy into the encryption scheme. It also makes reverse-engineering or cloning the algorithm significantly more difficult: even if an attacker discovers the cipher algorithm, they cannot reconstruct the S-box for a given encryption without replicating the exact external conditions (e.g., the same biometric input or hardware instance).

There is, however, an inherent challenge with context-aware S-boxes: asymmetry between encryption and decryption. Both parties need access to the same context to generate the same S-box for decryption. This limits the use of such schemes to scenarios where the environment can be shared or reproduced. In tightly controlled systems this is feasible – for example, in a personal data encryption system in the cloud, the server would not decrypt stored data until the legitimate user provides a fresh biometric sample to regenerate the S-box, thereby authenticating and enabling decryption. This ensures that the adaptive S-box (constructed from the user's context) remains hidden from the server – and any attacker – until the proper context is provided. Context-aware S-box generation is therefore mostly found in specialized applications where both sender and receiver (or encryptor and decryptor) can ensure the availability of the required external parameters during both encryption and decryption.

Overall, environment-driven adaptive S-box frameworks demonstrate significant security enhancements while also offering new functionalities (such as user or device binding of the encryption). They introduce an additional hurdle for attackers, who must not only break the cryptography but also replicate specific external conditions. When implemented carefully in scenarios that allow context sharing, these techniques can improve security without compromising operational efficiency.

CRYPTOGRAPHIC REQUIREMENTS AND CHALLENGES FOR ADAPTIVE S-BOXES

Every S-box, whether static or adaptive, must satisfy certain stringent cryptographic criteria to be considered secure. Chief among these are high nonlinearity, low differential uniformity, and low linear bias, along with properties like the Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC). For an n-bit bijective S-box, nonlinearity is a measure of how far its output bits are from any linear function of the inputs – the higher, the better. In the case of an 8-bit S-box (as used in AES and many modern block ciphers), it is known that the theoretical maximum nonlinearity is 112 (on a scale where 0 corresponds to a linear function and 128 would be an ideal but unattainable perfectly nonlinear function). The AES S-box, for example, achieves a nonlinearity of 112 and a very low maximum differential probability (it is differentially 4-uniform), which together make it resistant to both linear and differential cryptanalysis [21][22]. An adaptive S-box, despite its variability, must still operate within these bounds; if the S-box instances it produces have significantly lower nonlinearity or worse differential uniformity, they could inadvertently introduce weaknesses into the cipher.

One common issue observed in early adaptive S-box constructions (especially those using chaotic maps or other heuristic methods) is that while they increase entropy and complexity, they sometimes fail to achieve the optimal cryptographic parameters of well-designed static S-boxes. Researchers have noted that many chaos-based S-box proposals yield nonlinearity in the range of about 100–106 – somewhat lower than the AES S-box's 112 – which can make them more susceptible to differential

attacks if not improved. This gap arises because achieving both high nonlinearity and low differential uniformity simultaneously is challenging when designing S-boxes through arbitrary or random processes. To address this, various optimization techniques have been applied. Didoub et al. integrated specialized processes to guide the construction of chaotic S-boxes, managing to significantly improve their cryptographic metrics. Other groups have employed evolutionary algorithms and systematic search methods to traverse the vast space of 8-bit bijections in order to find adaptive S-box configurations that meet or exceed the strength of conventional S-boxes. Such approaches have, in some cases, produced adaptive S-boxes with nonlinearity and uniformity characteristics on par with AES's—proving that it is possible for adaptively generated S-boxes to "catch up" to the gold standard of static design.

For example, Ibrahim and Abbas devised an S-box construction based on key-dependent permutations of elliptic curve points, which consistently achieves a nonlinearity of 112 in every produced S-box instance. Their design is bijective and exhibits output distributions and avalanche properties (SAC) close to ideal, while maintaining low differential and linear probabilities – essentially matching the cryptographic quality of the AES S-box in a dynamic, key-driven context. Likewise, the fingerprint-derived S-box mentioned earlier is reported to fully satisfy SAC and other criteria, placing it among the most thoroughly tested adaptive designs in terms of classical cryptographic strength [20]. The lesson from these efforts is clear: adaptive S-boxes must be held to the same standards as static ones. Each individual S-box generated on the fly should be as secure as a carefully hand-crafted static S-box. This often necessitates adding extra steps in the generation algorithm, such as injecting additional randomness or performing post-processing permutations, to ensure that each instance uniformly samples from the space of strong S-boxes.

In summary, adaptive S-box techniques offer unprecedented flexibility and potential for improved security, but they come with the caveat that every generated S-box needs to uphold the baseline cryptographic properties. Designers often must balance randomness with control: they introduce adaptability and secret variation, yet also enforce conditions (through mathematical constraints or iterative improvement algorithms) so that the resulting S-boxes do not fall below the desired security threshold. When this balance is achieved, a customizable adaptive S-box can provide scrambling and confusion effects beyond what fixed implementations like the AES S-box can, especially if combined with context-dependent inputs, key-sensitive generation, and entropy-maximizing design principles.

METHODS FOR CONSTRUCTING ADAPTIVE S-BOXES

Researchers have proposed many methods to generate adaptive S-boxes, each with its own complexity, security benefits, and suitability for resource-limited settings. Below we outline some of the most popular approaches and discuss their pros and cons.

ALGEBRAIC MODIFICATIONS OF THE AES S-BOX

One straightforward approach is to derive new S-boxes by algebraically tweaking the well-studied AES S-box design. For instance, designers can change the irreducible polynomial used in the GF(2^8) field for the inversion step, or modify the affine transformation constants. These changes still result in bijective 8×8 S-boxes with non-trivial cryptographic properties (since the general structure of the AES S-box is preserved), but yield many possible S-box variants. A specific S-box from this family can then be selected based on the encryption key or some secret. The primary benefits of this approach are that it produces S-boxes with reliably high cryptographic metrics (many AES variants remain highly nonlinear and have low differential uniformity) and it is relatively easy to implement – often it's as simple as changing some fixed parameters in the S-box generation logic. This method is also compatible with existing hardware optimizations to some extent; for example, using a different affine constant might still be implemented via similar circuits. However, the number of distinct S-boxes obtainable through small algebraic modifications is limited. If an attacker obtains even a few plaintext–ciphertext pairs, they might infer which variant of the S-box is in use and drastically reduce their search space (since the structure is known except for a few bits of information). Additionally, such modifications break compatibility with standard AES hardware accelerators (like AES-NI instructions), as those expect the fixed AES S-box –

any change means those accelerators can no longer be directly used, potentially impacting performance.

GENERATION OF S-BOXES USING CHAOS AND PSEUDORANDOM TECHNIQUES

Another rich area of research is using chaotic systems, fractals, and pseudorandom number generators to construct S-boxes. Chaotic maps (such as logistic maps, Hénon maps, or other nonlinear recurrences) can produce sequences of values that appear random and highly sensitive to initial conditions. These sequences can be transformed into 8-bit permutation boxes (S-boxes). The appeal of chaos-based S-box generation lies in its flexibility and the fact that it doesn't rely on algebraic structures – the resulting S-boxes are often non-algebraic and irregular, which can make them resistant to algebraic cryptanalysis. They can also be keyed: a secret seed or initial condition for the chaotic system can produce a key-dependent S-box. Some studies have even suggested that the irregular structure of chaos-based S-boxes might confer better side-channel resistance, as their implementation doesn't have the regular patterns of a fixed S-box lookup.

On the downside, S-boxes generated purely from chaotic or random processes often require additional processing to meet cryptographic standards. The raw output of a chaotic map might not be a permutation, or it might yield a permutation with low nonlinearity or poor differential uniformity. Thus, researchers typically apply heuristics or optimization algorithms to the chaotic output – for example, discarding or tweaking S-boxes until they meet a threshold for nonlinearity. Moreover, implementing chaotic functions in constrained devices can be inefficient: many chaotic systems involve real-valued computations or iterative calculations that are not naturally efficient on digital hardware. Quantizing chaos into an S-box also needs careful handling to avoid precision issues. In summary, chaotic and pseudorandom techniques offer a vast space of candidate S-boxes and can produce highly unconventional designs (a plus for security), but they might incur higher computational cost and often demand a post-generation optimization step to ensure the S-box is cryptographically strong.

EVOLUTIONARY AND HEURISTIC OPTIMIZATION ALGORITHMS

Given the difficulty of analytically designing a perfect S-box, a number of researchers have turned to evolutionary algorithms (like genetic algorithms) and other heuristic optimization methods (such as particle swarm optimization or hill-climbing searches). The idea is to treat the S-box as an individual in a population and define a fitness function based on cryptographic criteria (e.g. maximize nonlinearity, minimize differential uniformity, etc.). Through simulated evolution – applying mutations, crossovers, and selections – the algorithm "evolves" a pool of candidate S-boxes towards those with better cryptographic properties. Such methods have successfully discovered S-boxes with very low linear and differential probabilities and high nonlinearity that would be hard to find through random sampling. They are also adaptable: constraints can be added to prefer S-boxes that, for example, have simpler structures or are easier to implement, which is useful when considering hardware efficiency.

The major drawback of these heuristic approaches is their computational cost. Evolving a strong S-box can require an enormous number of fitness evaluations, which is feasible offline but not something you can do during an encryption session. As a result, evolutionary algorithms are typically used to design S-box generation methods rather than generate S-boxes on the fly. For instance, one might evolve a general algorithm or formula parameterized by the key, so that at runtime the actual S-box is produced by a relatively efficient computation that was tuned by evolutionary search beforehand. Some hybrid approaches exist as well, where part of the S-box is generated at runtime with lightweight operations, guided by a structure that was optimized in advance. Chen and Chen (2008) presented a heuristic method where the key is deterministically tied to certain algebraic transformations in the S-box, striking a balance between performance and adaptability [26]. In general, evolutionary methods are powerful for discovering high-quality S-boxes and novel design strategies, but their direct use in real-time encryption is limited. Instead, they often inform the design of key-dependent S-box algorithms that can be executed quickly during encryption.

DATA-DEPENDENT AND PLAINTEXT-DEPENDENT S-BOXES

Some adaptive schemes go as far as making the S-box depend on the data being encrypted, rather than (or in addition to) the key. These input-dependent S-boxes are particularly considered in domains like multimedia or image encryption, where an attacker might have some knowledge of or control over the plaintext. The idea is that if each plaintext (or each block of plaintext) uses a different S-box derived from the data itself, it becomes extremely difficult for an adversary to craft a harmful chosen-plaintext or known-plaintext attack, since any change in the input causes a change in the cipher's core substitution layer. For example, one might take a hash of the current plaintext block and use it to generate or select an S-box for encrypting that block. In such a scenario, even if an attacker knows part of the plaintext, that knowledge does not directly translate into an ability to predict or manipulate the S-box – the slightest modification of the plaintext will produce a completely different S-box, and thus a different ciphertext output.

While this approach can thwart certain attacks (especially those where the attacker can ask for encryption of chosen data), it tends to be very domain-specific and not easily integrated into standard cryptographic protocols. Making the S-box depend on plaintext could interfere with decryption (the decryptor would have to derive the same S-box from the plaintext, which they may not fully know if any part of the plaintext is transformed during encryption). In practice, plaintext-dependent S-boxes have mainly been explored in custom schemes like image encryption systems, where the entire image is available to both parties and they can progressively update the S-box as they encrypt each part. Even then, a caveat arises: if the S-box is too directly influenced by plaintext data, a partial leakage of the S-box might inadvertently leak information about the plaintext. Designers must then incorporate additional cryptographic measures (like hashing the plaintext or using a secondary key) to decouple the S-box from revealing raw plaintext bits. In summary, data-dependent S-boxes can provide an extra layer of security in specialized scenarios (by making the cipher self-adapting to its input), but they are not commonly used in general-purpose encryption due to their complexity and potential risks if not carefully managed.

To summarize this section, adaptive S-boxes encompass a broad spectrum of design strategies – from simple algebraic tweaks of known boxes to elaborate dynamic constructions driven by chaos or evolutionary search. Each approach comes with a unique balance of security benefits versus implementation cost. The current trend in research is to strengthen the nonlinear layer's security without unduly impacting performance. The most effective adaptive S-box designs reported in the literature manage to meet or even surpass the classic AES S-box in terms of cryptographic criteria, while also providing an extra disguise or variability that a static S-box lacks. Notably, in constrained domains like IoT and real-time video encryption, there is growing evidence that carefully implemented adaptive S-box techniques are practical and can substantially bolster data security in those applications.

EVALUATION METHODOLOGY FOR ADAPTIVE S-BOXES

When evaluating the quality and security of an adaptive S-box scheme, a multi-pronged approach is necessary. Such an evaluation should include theoretical analysis, simulation-based cryptanalysis, and hardware-based testing, conducted step by step.

Cryptographic Property Validation: As an initial step, one must verify that the S-boxes generated by the scheme satisfy the fundamental requirements of a cryptographic substitution box. Each candidate S-box (for different keys or contexts) should be tested for bijectivity (each S-box should be a permutation of 0–255 in the 8-bit case, ensuring that decryption is possible). The nonlinearity of each S-box is computed for every output bit, with particular attention to the minimum nonlinearity among those bits – the lowest nonlinear output determines the S-box's vulnerability to linear cryptanalysis. Ideally, even the "weakest" output bit should have high nonlinearity.

In addition, the differential uniformity of each S-box is evaluated by constructing its difference distribution table and finding the maximum differential probability (DP). A low maximum DP (e.g. 4/256

for a 4-uniform S-box) indicates strong resistance to differential cryptanalysis. The S-box should also fulfill the Strict Avalanche Criterion (SAC) – flipping any single input bit should result in each output bit flipping with a probability of about 50%. The Bit Independence Criterion (BIC) is checked to ensure that any change in one output bit is uncorrelated with changes in other output bits when an input bit is flipped, implying that output bits appear independent of one another in the face of input changes. Additionally, the output bit distribution should be balanced (each output bit is 0 or 1 roughly half the time across all inputs), and there should be no simple algebraic relation linking inputs and outputs. Meeting all these criteria guards against known cryptanalytic attacks and is a prerequisite for trust in the S-box design [27].

It's important to assess these metrics not just for one instance of the S-box, but across a broad sample of S-boxes produced by the adaptive mechanism (for different keys, different contexts, etc.). Statistical descriptors – such as minimum, maximum, and average nonlinearity or differential probability – can be collected over many generated S-boxes to ensure that the scheme consistently produces strong boxes and does not occasionally output a weak one. This can be done efficiently with computer tools (using Python or MATLAB, for example, to automate the generation and testing of thousands of S-box instances).

Cipher-Level Cryptanalysis Simulations: Once the S-box instances themselves appear sound, the next step is to embed the adaptive S-box in a full encryption algorithm and test the algorithm's resistance to attacks. Classic differential and linear cryptanalysis can be simulated on the cipher under various scenarios to measure how much harder it is to recover the key compared to a similar cipher with a static S-box. If the S-box changes with each encryption or each session, the attacker's advantage from any one data set should diminish. Key-dependent and dynamically changing S-boxes are expected to significantly impede these attacks because the attacker cannot precompute differential characteristics or linear masks without knowledge of the secret-dependent S-box. It is also important to evaluate related-key attack resistance: one can test the cipher by slightly altering the key and observing how the S-box and encryption outputs change. Ideally, even a small change in the key should result in a substantially different S-box and thus entirely different encryption behavior, leaving no simple relationship for an attacker to exploit between runs of the cipher with related keys. In a robust adaptive S-box scheme, the slightest key modification produces an unpredictable shift in the substitution layer, greatly reducing the possibility of any structural correlation that an attacker could leverage.

Reverse-Engineering Resistance: Another angle of attack to consider is an adversary attempting to deduce the S-box itself by analyzing a collection of plaintext–ciphertext pairs. For a static S-box, there are known techniques to recover the S-box if enough pairs are available. For an adaptive S-box, especially one that might change every session or message, this becomes much more complex. Evaluators should attempt S-box recovery attacks assuming an attacker has access to multiple encryptions under the same key/context. If reconstructing the S-box requires the attacker to make prohibitive assumptions or if the recovered S-box is highly uncertain, then the design shows merit. As part of this, one can apply randomness tests (such as the NIST Statistical Test Suite) to the ciphertext output to ensure that the adaptive substitution layer isn't inadvertently introducing patterns. If the ciphertexts consistently pass randomness tests even when an attacker controls certain inputs, it indicates the S-box variability is effectively preventing the leakage of structural information [28].

Side-Channel Leakage Evaluation: Finally, it is crucial to test the adaptive S-box implementation against side-channel attacks at the hardware level. This involves measuring physical information (like power consumption or electromagnetic emissions) from a device performing encryption with the adaptive S-box. One common test is differential power analysis (DPA): the evaluator collects many power traces from encryption operations and tries to detect correlations that reveal key bytes. With a fixed S-box (like in AES), an attacker often knows the S-box output for a guessed key and can use that in DPA analysis. But if the S-box is key-dependent or dynamically changing, the attacker does not know the actual values being looked up, which should make correlating power traces to specific bits much harder. To quantify this, one can compare the number of power traces needed to recover the key in a

static S-box implementation versus in the adaptive S-box implementation. A successful adaptive design will require substantially more traces, potentially to the point where the attack becomes impractical. It should be noted, however, that improving side-channel resistance through adaptivity has its limits: given enough traces, even a changing S-box might still be profiled by a determined attacker. Therefore, adaptivity should be seen as complementary to, not a replacement for, established countermeasures like masking or noise injection. If testing shows that the adaptive S-box delays or blunts the efficiency of side-channel attacks – for example, the attacker's machine learning models cannot easily classify which S-box or key is in use from the traces – that is a clear security win for the design [24]. On the other hand, if the adaptive S-box generation is too simple (for instance, if it introduces only a linear transformation based on the key), then injecting a fault or performing advanced analysis on the side-channel data might still expose a relationship between the key and the S-box outputs, negating the advantage. Thus, side-channel evaluation also feeds back into the design: it ensures that the method of generating the S-box is itself cryptographically robust and doesn't create new side-channel or fault vulnerabilities.

In summary, a comprehensive assessment of an adaptive S-box scheme involves checking that each generated S-box meets cryptographic quality standards, testing the cipher's resilience to various cryptanalytic attacks, and analyzing its behavior in real hardware for side-channel resistance. Only through such a holistic evaluation can one trust that an adaptive S-box design is both theoretically sound and practically secure.

IMPLEMENTATION AND PERFORMANCE CONSIDERATIONS

Beyond security, adaptive S-box designs must be evaluated for their feasibility in real-world implementations, especially in contexts with limited resources (like IoT devices, smart cards, or embedded systems). One important aspect is the computational and energy cost of S-box generation. If an S-box is generated once per encryption key (say at key setup time), the cost might be a one-time hit that is amortized over many encryption operations. However, if the design calls for generating a new S-box every round or every block, this could introduce significant overhead in terms of CPU cycles and memory operations during encryption. It is crucial to measure how long it takes to produce an S-box on the target platform and how much extra time (or latency) this adds to the encryption process. For instance, if encryption throughput drops markedly compared to a standard AES implementation, that might be unacceptable for certain applications. Similarly, in energy-harvesting or battery-powered devices, the additional energy required to frequently compute new S-boxes should be quantified to ensure it does not exceed the system's budget.

Memory usage is another concern. A static S-box can be stored in a compact table (256 bytes for an 8×8 S-box). In contrast, a dynamic S-box scheme might need to store multiple S-boxes or the logic to generate them on the fly. On hardware like FPGAs or microcontrollers, one should analyze how many logic elements or how much RAM is consumed by the adaptive S-box mechanism. If, for example, a scheme keeps a small set of pre-validated S-boxes and just switches between them, it will use more memory than a single S-box but could avoid the cost of computing a brand new one each time. Some lightweight implementations avoid full table storage altogether by computing S-box outputs algorithmically as needed, bit by bit or nibble by nibble, trading memory for computation. Others exploit hardware parallelism: for example, one part of an FPGA could be dedicated to computing the next S-box while another part is actively encrypting data with the current S-box, thus overlapping computation with encryption to mask latency.

In highly constrained ciphers (like those with 4×4 S-boxes such as PRESENT or GIFT), the cost of regenerating the S-box is naturally lower simply because the S-box is smaller. This makes full S-box adaptation more practical even in environments with very limited CPU power. For larger S-boxes, partial or incremental updates can be a strategy – for instance, only substitute a portion of the S-box entries each time, or cycle through a precomputed set of S-boxes. A design might include, say, 16 distinct 8×8 S-boxes that have all been vetted for security; the cipher can then use an index derived from the key or

context to pick which S-box to use for a given session or round. This way, the variability is introduced without heavy on-line computation, at the expense of storing those 16 S-boxes in memory.

Another factor is compatibility with existing systems. AES, for example, benefits from dedicated hardware instructions (AES-NI) and well-optimized software routines. Replacing or augmenting AES's static S-box with a dynamic one means those hardware accelerations can no longer be directly used. The implementation might have to fall back to software or custom hardware, which could be significantly slower. There is an ongoing debate about whether the security gains of dynamic S-boxes are worth the performance trade-off in such cases. In settings where AES acceleration is unavailable (like some IoT microcontrollers without AES hardware), a dynamic S-box might be more acceptable. But in high-throughput environments (like disk encryption on a CPU with AES-NI), even a moderate performance loss might be problematic unless the threat model absolutely requires the extra security.

Hybrid solutions have been proposed to balance these concerns. For instance, a cipher could operate mostly in a standard mode and only switch to a dynamic S-box mode under certain conditions, such as when a side-channel attack is suspected or when entering a high-security mode. This could potentially provide the best of both worlds: normal high speed operation most of the time, and adaptive high-security operation when needed, at the cost of performance only in those moments.

Overall, many of the initial performance penalties associated with adaptive S-boxes have been mitigated by research and engineering. For example, recent work on key-dependent dynamic S-boxes based on elliptic curves has shown that using standard computing hardware, one can construct a new 8-bit S-box in just a few milliseconds by leveraging efficient finite field arithmetic and permutation logic [14]. Furthermore, various lightweight techniques (bit-sliced implementations, loop-unrolling for on-the-fly S-box computation, etc.) have been introduced to optimize adaptive S-box generation. In hardware like FPGAs, parallelism can be exploited to hide S-box generation latency, as mentioned earlier. In summary, while adaptive S-box schemes do impose overhead, careful implementation can reduce this overhead to an acceptable level for many applications. Each use case (sensor networks, IoT devices, real-time video encryption, etc.) requires a balance: ensuring that added security does not cause cryptographic operations to miss their timing deadlines or energy budgets.

INTEGRATION TESTING IN APPLICATIONS

The final stage of evaluating an adaptive S-box scheme is to test it in the context of the real applications for which it was designed. This kind of integration testing ensures that the adaptive S-box cipher can be seamlessly incorporated without causing unintended issues in system operation.

In the context of IoT communication protocols, for example, one can implement the cipher (with adaptive S-box) on a sensor node and the corresponding decryption on a gateway or base station. Then, under realistic operating conditions, monitor metrics like data throughput, latency, and packet loss. An important consideration is whether the adaptive S-box's generation or negotiation adds any protocol complexity or delays. If the S-box needs to be derived from shared parameters, the protocol must handle that without introducing vulnerabilities or significant handshake overhead. The system should be scrutinized to ensure that encryption and decryption remain synchronized – any desynchronization (say, if one side updates the S-box out of sync with the other) could lead to data loss or the need for re-transmission. Ideally, after integration, the communication should continue with minimal additional delays. For instance, if an IoT device normally sends encrypted sensor readings every second, using an adaptive S-box cipher should not cause it to miss those intervals due to re-computation of S-boxes or excessive processing. If minor delays are introduced, it must be verified that they do not violate the application's real-time constraints.

In the multimedia domain, such as adaptive S-boxes applied to video or image encryption, the evaluation focuses on real-time performance and quality of service. Video encryption often has tight timing requirements to maintain streaming without buffering. Using an adaptive S-box per frame or per group of frames, for instance, should not cause frame drops or significant latency. Testing might involve encrypting a video stream with the adaptive cipher and measuring metrics like frame rate, end-to-end

latency, and any impact on video quality (if the encryption is selective or partial). Another aspect is interoperability with existing standards or libraries. For example, if one tries to integrate an adaptive S-box cipher into an OpenSSL library or as a plugin for a secure communication suite, it needs to co-exist with other cryptographic components. Some cryptographic libraries make assumptions about block cipher implementations (such as constant memory access patterns, or availability of certain hardware). A custom S-box integration might conflict with those assumptions, especially if it introduces dynamic memory allocation or other behaviors. As a concrete case, Kodikara Arachchi et al. explored adaptation-aware encryption for video and had to ensure that the encryption did not disrupt the codec's normal operation or significantly degrade compression efficiency [30]. In general, integration testing should verify that the adaptive S-box cipher can operate within the application's ecosystem (network stack, media pipeline, etc.) without causing errors or requiring excessive modification of surrounding components.

Ultimately, the wrap-up from integration testing is an understanding of how the adaptive S-box scheme performs under realistic conditions and what the trade-offs are in the intended use case. It helps answer questions like: Does the added security come at a manageable cost in performance? Are there any unexpected interactions or vulnerabilities introduced at the system level? This kind of feedback is invaluable for refining the design or choosing parameters (for instance, how frequently to update the S-box in practice) to balance security and practicality.

CONCLUSION

The analysis presented above provides a thorough profile of adaptive S-box designs, illuminating their strengths and weaknesses. In the best-case scenarios, an adaptive S-box scheme can perform comparably to traditional static S-box ciphers in terms of throughput and resource usage, while offering greater resilience to certain attacks (notably side-channel and analytical attacks). For instance, a well-implemented adaptive S-box might impose only a minor computational overhead yet substantially increase an attacker's workload by obfuscating the cipher's internals. Any identified weaknesses – such as slightly decreased nonlinearity for specific keys or extra processing time in certain contexts – need to be carefully examined and, if possible, mitigated through design adjustments or by restricting the scheme's use to appropriate scenarios.

Looking ahead, adaptive S-boxes offer intriguing new directions for the evolution of symmetric cryptography. Their chief advantage is in breaking the static assumptions that most classical cryptanalytic attacks rely on, thereby creating additional hurdles for would-be attackers. This dynamic approach could become increasingly valuable as attackers develop more powerful analytic techniques and as computing power grows (which makes brute-force and precomputation attacks more feasible on fixed algorithms). However, the deployment of adaptive S-boxes is not without difficulties. Some schemes require frequent re-initialization or complex synchronization, which can be impractical in high-speed or ultra-low-power environments. Others demand more computational resources than traditional ciphers, which can be a barrier to adoption.

Despite these challenges, research has shown that there are efficient adaptive S-box implementations suitable even for constrained devices like sensors and wearables [18]. As this technology matures, we can expect to see more cryptographic systems where the nonlinear components are variable and context-aware rather than fixed. Such designs will need to be accompanied by rigorous security analysis and careful engineering to ensure they meet both security and performance requirements. In conclusion, adaptive S-boxes represent a promising avenue to bolster the security of encryption algorithms against evolving threats. With ongoing improvements in design and optimization, they may well become a standard feature in next-generation cryptographic primitives, providing robust protection by continuously shifting the ground beneath the attacker's feet.

REFERENCES

[1] L. Mittenthal, (1996), Nonlinear dynamic substitution devices and methods for block substitutions employing coset decompositions and direct geometric generation, United States: U.S. Patent Office.

[2] S. Elramly, T. El-Garf, and A. H. Soliman, (2001), Dynamic generation of S-boxes in block cipher systems, in Proc. National Radio Science Conf., Egypt: IEEE. DOI: 10.1109/NRSC.2001.929396.

[3] A. M. Alshahrani and S. D. Walker, (2014), Implement a novel symmetric block cipher algorithm, Int. J. Cooperative Information Systems, vol. 4, no. 4, India: Academy & Industry Research Collaboration Center. DOI: 10.5121/IJCIS.2014.4401.

[4] N. Nedjah and L. de M. Mourelle, (2007), Designing substitution boxes for secure ciphers, Int. J. Innovative Computing and Applications, vol. 1, no. 3, UK: Inderscience Publishers. DOI: 10.1504/IJICA.2007.013404.

[5] I. Hussain, T. Shah, and M. A. Gondal, (2012), A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm, Nonlinear Dynamics, vol. 70, Netherlands: Springer. DOI: 10.1007/s11071-012-0573-1.

[6] A. Kadhim and Z. A. Kamal, (2018), Dynamic S-box based on primitive polynomial and chaos theory, in Proc. IICETA 2018, Iraq: IEEE. DOI: 10.1109/IICETA.2018.8458093.

[7] A. Alamsyah, A. Bejo, and T. B. Adji, (2018), The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box, Nonlinear Dynamics, vol. 94, Netherlands: Springer. DOI: 10.1007/s11071-018-4310-2.

[8] A. Cengiz and D. Avci, (2019), Review of chaotic-based S-box structures, in Proc. ISDFS 2019, Turkey: IEEE. DOI: 10.1109/ISDFS.2019.8757513.

[9] V. van der Leest and P. Tuyls, (2013), Anti-counterfeiting with hardware intrinsic security, in Proc. DATE 2013, Germany: IEEE.

[10] M. Ratiner, (2005), The method of S-box construction, J. Discrete Mathematical Sciences and Cryptography, vol. 8, no. 2, India: Taylor & Francis. DOI: 10.1080/09720529.2005.10698030.

[11] I. Hussain, A. Anees, T. A. Al-Maadeed, and M. T. Mustafa, (2019), Construction of S-box based on chaotic map and algebraic structures, Symmetry, vol. 11, no. 3, Switzerland: MDPI. DOI: 10.3390/sym11030351.

[12] G. Xu, G. Zhao, and L. Min, (2009), A method for designing dynamical S-boxes based on a discrete chaos map system, in Proc. ICCCAS 2009, China: IEEE. DOI: 10.1109/ICCCAS.2009.5250385.

[13] J. Namuq, (2024), S-box design utilizing 3D chaotic maps for cryptographic applications, Basrah J. Engineering Sciences, vol. 24, no. 2, Iraq: University of Basrah. DOI: 10.33971/bjes.24.2.9.

[14] D. Wenxia and W. Hao, (2013), Design of S-boxes based on discrete chaos system, China: Chinese Journal of Electronics. DOI: 10.3969/j.issn.1001-2486.2013.01.016.

[15] A. H. Zahid, H. A. M. Elahi, M. Ahmad, R. S. A. Said, and L. Maghrabi, (2023), Secure key-based substitution-box design using systematic search for high nonlinearity, IEEE Access, vol. 11, USA: IEEE. DOI: 10.1109/ACCESS.2023.3339389.

[16] H. Liu, X. Wang, and Y. Li, (2021), Cryptanalyze and design strong S-box using 2D chaotic map and application to irreversible key expansion, arXiv preprint, USA: Cornell University. arXiv:2103.15124.

[17] S. Bukhari, A. Yousaf, S. Niazi, and M. R. Anjum, (2019), A novel technique for the generation and application of substitution boxes (S-box) for image encryption, Nucleus, vol. 56, no. 3, Pakistan: Pakistan Atomic Energy Commission.

[18] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, (2016), A new image encryption scheme based on dynamic S-boxes and chaotic maps, 3D Research, vol. 7, no. 4, Singapore: Springer. DOI: 10.1007/s13319-016-0084-9

[19] X. Di, (2010), A method for generating S-box based on iterating chaotic maps, J. Chongqing Univ. of Posts and Telecommunications, vol. 22, no. 3, China: CQUPT Press.

[20] S. Marochok and P. Zajac, (2023), Algorithm for generating S-boxes with prescribed differential properties, Algorithms, vol. 16, no. 3, Switzerland: MDPI. DOI: 10.3390/a16030157.

[21] W. Zhang and E. Pasalic, (2014), Highly nonlinear balanced S-boxes with good differential properties, IEEE Trans. Information Theory, vol. 60, no. 11, USA: IEEE. DOI: 10.1109/TIT.2014.2360880.
[22] C. Bracken and G. Leander, (2010), A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree, Finite Fields and Their Applications, vol. 16, no. 6, USA: Elsevier. DOI: 10.1016/j.ffa.2010.03.001.
[23].-N. Chen and S.-M. Yen, (2003), Differential fault analysis on AES key schedule and some countermeasures, in Proc. ICISC 2002, LNCS vol. 2587, Germany: Springer. DOI: 10.1007/3-540-45067-X_11.
[24] C. R. Teegarden, M. Bhargava, and K. Mai, (2010), Side-channel attack resistant ROM-based AES S-box, in Proc. IEEE HOST 2010, USA: IEEE. DOI: 10.1109/HST.2010.5513101.
[25] V. Panchami and A. Wahi, (2017), Dynamic colour table: A novel S-box for cryptographic applications, Int. J. Communication Systems, vol. 30, no. 17, UK: Wiley. DOI: 10.1002/dac.3318.
[26] G. Chen and G. Chen, (2008), A novel heuristic method for obtaining S-boxes, Chaos, Solitons & Fractals, vol. 36, no. 4, UK: Elsevier. DOI: 10.1016/j.chaos.2006.08.003.
[27] W. Pilarczyk, B. Kowalczyk, and E. Bakinowska, (2015), Comparison of uniformity decisions in DUS testing for full and reduced numbers of measurements, Biometrical Letters, vol. 52, no. 1, Poland: De Gruyter. DOI: 10.1515/bile-2015-0005.
[28] A. Freyre-Echevarría, I. Martínez-Díaz, C. M. Legón Pérez, G. Sosa-Gómez, and O. Rojas, (2020), Evolving nonlinear S-boxes with improved theoretical resilience to power attacks, IEEE Access, vol. 8, USA: IEEE. DOI: 10.1109/ACCESS.2020.3035163.
29[] R. Rahmani, S. Han, Y. Li, and Z. Hu, (2018), A time-scaling data generation method for Internet of Things simulation, in Proc. ITNEC 2018, China: IEEE. DOI: 10.15224/978-1-63248-162-7-10.
[30] H. Kodikara Arachchi, X. Perramon, S. Dogan, and A. M. Kondoz, (2009), Adaptation-aware encryption of scalable H.264/AVC video for content security, Signal Processing: Image Communication, vol. 24, no. 6, Netherlands: Elsevier. DOI: 10.1016/j.image.2009.02.004.

Wiesław Maleszewski: https://orcid.org/0000-0001-8852-3532

ANN AIDED ILC FOR REPEATABILITY AND ACCURACY CONTROL OF ROBOT MANIPULATOR

Arkadiusz NIECECKI[1], Arkadiusz MYSTKOWSKI [2]

Department of Automation and Robotics, Faculty of Information Technology and Science, University of Łomża, Poland [1]

Departament of Automatic Control and Robotics, Faculty of Electrical Engineering, Bialystok University of Technology, Poland [2]

anieciecki@al.edu.pl [1], a.mystkowski@pb.edu.pl [2]

ABSTRACT

This thesis discusses the problem of increasing the accuracy and repeatability of robotic manipulators through the use of advanced control strategies. It introduces the concepts of Iterative Learning Control and Artificial Neural Networks as methods for improving precision in repetitive tasks. The paper reviews current research in this area, highlighting the potential of learning algorithms. The preparation of a simulation environment using the UR5 robot, MATLAB, ROS and URSim software, and a testing methodology based on ISO 9283 are described. Preliminary results of trajectory simulations and a dataset of the robot's joint configuration and velocity are presented. Data gathered from offline simulator shows overshoot from desired position. The work indicates the need for further research on AI controllers to fully explore their capabilities in robotic applications.

Key words: Robotic manipulators, Iterative Learning Control, Artificial Neural Networks, Positioning accuracy, ISO 9283

1. INTRODUCTION

The repeatability of a manipulator is its ability to reach a point from the previous repetition in each subsequent iteration [1]. We do not refer to the position indicated by the program but to the grouping of the achieved end positions of the movement as they may vary as a result of many factors such as varying environmental conditions at different repetitions, friction, stability of the control system and others. The next important point for the subject is accuracy [2]. It can be defined as the distance of the circle of focus of the endpoints from the position set by the program. The main [3] factors can be poor calibration of the position, manufacturer's tolerances, rigidity of the structure, varying environmental conditions and others. Iterative Learning Control further referred to as ILC is an open-loop system control for activities that are performed repeatedly [4,5]. Such activities largely include tasks performed by robotic manipulators are, for example, welding, applying glue, riveting, palletizing in a specific order or pick and place. The idea is for each iteration to draw information from previous repetitions to achieve a finer result [6]. The goal of ILC is not only to ensure stability, but also to achieve high tracking performance, which ideally means reducing the error to zero [7]. In the review, the performance of ILC systems is evaluated based on the asymptotic value of the error that the system aims for after many iterations, and the conditions under which it is possible for the error to converge to zero. ILC not only reduces the error, but eliminates it completely for the iterative aspects of the task. This is a key differentiator compared to standard closed-loop control, which often has a non-zero fixed error. By learning the inverse of an object's dynamics for a specific reference trajectory, ILC aims to achieve a

higher level of precision in repetitive tasks.

ANN, or artificial neural networks, is an architecture that mimics biological neuron systems for solving complex operations such as finding patterns in large databases, adjusting parameters of control systems or predicting solutions to complex calculations with high accuracy [8]. There are many architectures based on artificial neurons, such as:

- Multilayer perceptron,
- Perceptron networks with feedback,
- Convolution Neural Nets,
- Cellular neural networks.

The Levenberg-Marquardt algorithm (LMA) is an iterative nonlinear least squares optimization method. Combined with today's hardware, it is one of the faster methods for networks up to several hundred weights [9]. A key element of LMA is the adaptation of interpolation between the least-squares method and the Gauss-Newton method. In many cases, it is able to outperform the coupled gradient method when high speed and high accuracy are expected. It shows equality high robustness and can converge even under difficult conditions. The problem is the high computational cost per epoch and the memory requirements caused by computing the Jacobian, which will limits the use of LMA in large neural networks.

ISO norms broadly define the standards to be met by robotic manipulators. From the vocabulary used to safety requirements. One such standard is ISO 9283 [10] which plays an important role by defining performance criteria for manipulators and methods for testing them. It describes many important performance criteria and methods for testing them. These include:

- Pose Accuracy (AP), Pose Repeatability (RP) - describe the robot's precision in reaching set points in the robot space.
- Distance Accuracy (AD) AND Distance Repeatability (RD) - The ability of the robot to maintain a preset distance between two points.
- Pose stabilization time - The time it takes for the robot to stabilize in a preset position after a move.
- Position overshoot - The maximum overshoot of a preset position while moving to it.
- Path Accuracy (AT) and Path Repeatability (RT) - evaluation of the robot's ability to precisely follow a programmed trajectory.

Noticeable examples of research in field of AI robotic manipulator controllers for increased accuracy are [11-14].

The research paper [11] focuses on the application of advanced control techniques in robotics. The main research problem of the paper was to explore the use of Artificial Neural Networks as an alternative to conventional controllers to improve position control precision and reduce drift in robotic manipulators. Precise positioning is crucial in many applications, and drift poses a significant challenge to long-term accuracy. The authors implemented and compared two ANN learning methods, the Levenberg-Marquardt (LM) algorithm and Bayesian regression (BR). LM is effective for nonlinear problems, while BR offers a probabilistic approach to help avoid overfitting. The neural controller had 36 inputs, two hidden layers and six outputs, with satlin and purelin activation functions. The experimental platform was a six-axis UR5 robot. The test involved tracking a Lissajous trajectory, transformed to the robot's joint space. Training and test data were collected during experiments with the UR5 robot controlled by a classical PID controller. The goal was to match or improve PID performance. Networks were trained to map the robot's state to control signals. The key result is that the trajectory tracking performance of the LM and BR controllers was comparable to the classical PID controller. This confirms that ANNs can be a viable alternative. The root mean square error (RMSE) for position and velocity was used to assess quality. The RMSE values were similar for all three controllers in simulations and on the real robot. Comparing the neural algorithms, the network trained with BR showed slightly better RMSE results than the network with the LM. The authors conclude that an approach using ANN controllers to track trajectories is possible. Neural controllers are characterized by good trajectory tracking capabilities

for a given trajectory. A key advantage is the generalization and adaptability of the neural controller, which can compensate for small differences between robot units without manual fine-tuning. This is a significant advantage over traditional controllers. The authors suggest future research, including a comparison with other machine learning methods and the application of ANN control to more complex applications, such as structural vibration damping.

The article [12] addresses the challenge of precise trajectory tracking in industrial robots. While these robots often have external motion command interfaces, their actual performance is limited by complex internal dynamics and proprietary joint servo controllers, which are typically inaccessible to end-users. Communication delays further complicate achieving high-fidelity motion. To overcome these issues, authors propose a method combining Multi-Layer Neural Networks (MLNN) with Iterative Learning Control (ILC). The core idea involves using ILC in a simulation to learn command adjustments for specific trajectories, generating data to train an MLNN. The research aims to create an outer-loop feedforward controller to compensate for these combined effects. The proposed methodology is a two-stage process, Iterative Learning Control (ILC) for Data Generation and Multi-Layer Neural Network (MLNN) for Feedforward Control. ILC is used offline within a high-fidelity simulator (ABB RobotStudio) to generate accurate input-output data for MLNN training. For a desired joint trajectory, ILC iteratively refines the external command by measuring tracking error and updating the command until the simulated robot follows the trajectory accurately. This model-free approach is ideal for black box systems as it doesn't require an explicit model of the robot's internal dynamics. The MLNN is trained on the data generated by ILC to learn the relationship between desired motion and the required compensated command, effectively approximating the inverse dynamics of the robot's inner control loop. Once trained, the MLNN functions as a feedforward controller, predicting commands for new, unseen trajectories to improve tracking accuracy. The ILC-MLNN approach was evaluated in the ABB RobotStudio simulation environment using an ABB IRB 6640-180 robot model. The study reports that for various single-joint motions and multi-joint motions, the MLNN-based compensation significantly reduced tracking errors by mitigating phase lag and amplitude attenuation. Performance was also assessed for Cartesian space tasks, such as tracking a square trajectory, where the MLNN compensation again led to substantial error reductions. For tracking a straight line path, the proposed method achieved accuracy comparable to the robot's proprietary MoveL command. Transitioning from simulation to a physical ABB IRB 6640-180 robot revealed sim-to-real gap, where initial performance on the physical robot was less improved than in simulation. To address this, the researchers employed transfer learning. The MLNN, initially trained on extensive simulation data, had its output layer fine-tuned using a small amount of experimental data from the physical robot. This allowed the network to adjust for the real hardware. The article indicates that this transfer learning approach significantly improved tracking performance on the physical robot, especially for more dynamic trajectories, effectively correcting phase lag and magnitude degradation. The study also investigated whether the MLNN controller trained on the IRB 6640-180 could generalize to other ABB robot models (IRB 120 and IRB 6640-130) in simulation. The results showed that applying the pre-trained MLNN improved tracking accuracy for these different models compared to uncompensated commands. The methodology was validated experimentally, showing significant tracking error reductions on a physical industrial robot.

The paper [13] addresses the challenge of making robotic manipulators move along a predefined path in the shortest possible time while ensuring the motion is actually possible on the physical robot. Problem with traditional Time-Optimal Path Tracking (TOPT) is that it relies on mathematical models of the robot, which often don't perfectly match the real robot's behaviour. This mismatch can lead to trajectories that are slower than truly optimal, track the path poorly, or even attempt to violate the robot's physical limits. The paper introduces a specific two-step iterative algorithm Nonparametric Model Correction and Optimal Path Tracking. In each iteration, the algorithm takes data like joint position, velocity, acceleration, and the torque from the robot's previous execution. Then it calculates a correction term. This term represents the difference between the torques predicted by an initial, potentially inaccurate, robot model and the torques that were actually measured during the previous run. This

correction is nonparametric, meaning it doesn't try to adjust specific physical parameters of the model but rather learns a direct adjustment to the model's output. This updated model is expected to more accurately predict the torques needed for a given motion. Then using this newly corrected and more accurate model, a standard TOPT problem is solved. This step calculates a new trajectory that is time-optimal according to this improved model and, is designed to use the robot's operational constraints as predicted by this updated model. New trajectory is then commanded to the robot for the next execution. The process repeats. The robot executes the trajectory, new data is collected, the model is further corrected, and a new TOPT trajectory is calculated. The first iteration typically uses the initial robot model without any correction. Through these cycles of execution, learning, and recalculation, the system aims to converge on a trajectory that is both genuinely time-optimal for the real robot and guaranteed to be possible within its actual physical limits. The authors also note the importance of using computationally efficient algorithms for the TOPT calculation step to make the iterative process practical. The effectiveness of this ILC was demonstrated through experiments on an industrial robotic manipulator. The robot was tasked with following a predefined geometric path as quickly as possible. The experimental results showed that the iterative learning algorithm successfully reduced the overall execution time compared to trajectories calculated using only the initial, uncorrected model. In conclusion, the paper presents a practical method that combines ILC with TOPT to address the issue of model-plant mismatch. By iteratively learning from experience, the system refines its understanding of the robot and computes trajectories that are faster and more accurate, while also being safely executable on the physical hardware.

Proportional-Derivative Iterative Second-Order Neural-Network (PDISN) [14] learning control method is presented to address the motion-tracking control problems of robotic manipulators, particularly when performing repetitive tasks. The paper acknowledges that achieving excellent control performance with learning controllers like Iterative Learning Control (ILC) is challenging due to nonlinearities, uncertainties, and disturbances inherent in robotic system dynamics. The PDISN control framework is structured with two layers: Time-Based Control Layer and Iterative-Based Control Layer. Time-Based Control Layer: The total systematic dynamics are initially stabilized by a conventional Proportional-Derivative (PD) control signal operating in the time domain. Iterative-Based Control Layer: The control objective is then achieved using an intelligent ILC decision. This component is designed to compensate for other nonlinear uncertainties and external disturbances within the robot's dynamics. The control signal from the previous iteration is reused in the current iteration, but its contribution is weighted by an appropriate portion based on the reliability of the current control performance. Furthermore, any remaining iterative-based modelling deviation is handled by a functional neural network. This neural network is distinctively activated by a second-order learning law that utilizes information synthesized from current and previous iterations. These include the structured two-layer control framework, the intelligent generation of the ILC decision which involves the reliability-based reuse of the previous signal, and the second-order learning law for activating the neural network based on inter-iteration information. The authors claim that the PDISN method is chattering-free, universal, adaptive, and robust. The article also states that the stabilities of both the time-based nonlinear subsystem and the overall system are rigorously analysed using extended Lyapunov theories and high-order regression series criteria. These simulations indicated that the control accuracies of the PDISN controller increased from iteration to iteration, reaching promising results. After 50 iterations, steady-state control errors for joint 1 and 2 reached values of 0.00036 radians and 0.00015 radians. The simulation results highlighted in the article suggest its potential for achieving high precision and robustness. While the abstract describes the PDISN's concept and claimed benefits, the detailed mathematical formulation of the second-order learning law and the precise mechanism for quantifying the reliability of the current control performance are not fully explained. Furthermore, the available abstract focuses on simulation results, and there is no mention of experimental validation on physical robotic systems within these initial descriptions.

2. METHODOLOGY

2.1. Preparation of the environment

The Universal Robots UR5 is a 6-degree-of-freedom collaborative robot widely utilized in various industrial applications, academic research, and educational settings due to its collaborative nature, ease of programming, and versatility. At first model of the UR5 robot was supposed to be simulated only in MathWorks MATLAB in conjunction with Simscape, Simulink, and Robotics System Toolbox. With use of ROS connection, communication between MATLAB and URSim which is the official offline simulator for Universal Robots was possible. This allows to test virtual twin before future tests on a physical robot. The Denavit-Hartenberg (DH) convention provides a standardized method for parameterizing the geometry of robotic manipulators, defining coordinate frames for each link and the transformations between them. These parameters are fundamental for deriving forward and inverse kinematics. The DH parameters for a standard UR5 robot are accessible from the manufacturer's site [15]. These parameters are essential for understanding the robot's geometric structure and are often used for custom kinematic and dynamic calculations or for verifying the imported model

2.2. Description of the research methodology

The test method will be based on the ISO 9283:1998 standard. [10]. We determine the largest working field in the form of a regular cube located within the working range of the manipulator. Inside it we establish test points or trajectory. The main indicators to be tested will be AP and RP. AP is defined as the degree of consistency between the preset position and the actual average executed position, i.e. how close on average the robot reaches the preset point. The measurement is carried out by performing at least 30 cycles during which we record the achieved positions. Having groups of points, we calculate the arithmetic averages of the measured coordinates of the x, y, z axes. We then calculate Pose Accuracy as the distance passed from the calculated average position. RP determines the robot's ability to return to the same position on multiple attempts by describing the spread of reached points relative to the previously mentioned average position. Define it as the sphere containing most of the points reached by the robot. It is based on a statistical analysis of each of these points relative to the barycentre of each iteration and its standard deviation. We assume that the RP ratio equals 3S, where S is the calculated standard deviation.

3. MODELLING

3.1. Kinematic model of the robot

For this and future works, the UR5 robotic manipulator will be used. Its kinematic model is described by [15] as Denavit–Hartenberg parameters. These parameters describe a standard method for describing the geometry of robotic manipulators.

They define the spatial relationship between consecutive links in the robotic arm using four parameters associated with each link and its joint. Theta (Tab.1.) is joint angle, which is variable in this example. The third column is link length, then link offset and link twist. These parameters allow us to find the position and orientation of the end effector relative to the base of the robot by using homogeneous transformation.

Tab. 1. UR5 Denavit–Hartenberg parameters.

Kinematics	theta [rad]	a [m]	d [m]	alpha [rad]
Joint 1	q_1	0	0.089159	π/2
Joint 2	q_2	-0.425	0	0
Joint 3	q_3	-0.39225	0	0
Joint 4	q_4	0	0.10915	π/2
Joint 5	q_5	0	0.09465	-π/2
Joint 6	q_6	0	0.0823	0

3.2. Simulation setup

Simulation for this paper is limited to the creation of an environment, the process of control, and data collection. Setup consists of MATLAB, ROS and URSim. URSim and ROS are deployed on Linux based virtual machine and MATLAB on the host computer. This setup allows us to control the manipulator in various ways. For validation of control and data collection process, mocked ISO 9283 based test was performed. It consisted of 5 evenly spaced points located in the test cube described in Tab.2.

Tab. 2. Position of end effector in relation to base of robot and tool orientation.

X (mm)	250	-250	0	250	-250
Y (mm)	350	350	600	850	850
Z (mm)	0	0	250	500	500
RX (°)	270	270	270	270	270
RY (°)	0	0	0	0	0
RZ (°)	0	0	0	0	0

Then positions from Tab.2. are translated to joint angles (Tab.3).

Tab. 3. Position of end effector in relation to base of robot and tool orientation.

Joint 1	67.18	157.09	105.45	81.28	118.13
Joint 2	-163.33	-163.33	-130.72	-159.09	-159.09
Joint 3	-118.34	-118.34	-107.76	-8.23	-8.23
Joint 4	101.68	101.68	58.47	-12.68	-12.68
Joint 5	112.82	22.91	74.55	98.72	61.87
Joint 6	0.00	0.00	0.00	0.00	0.00

For test purposes, polynomial trajectory using B-splines was used with 5 repetition and total run time of 30 seconds. Data was recorded at a 100 Hz rate.

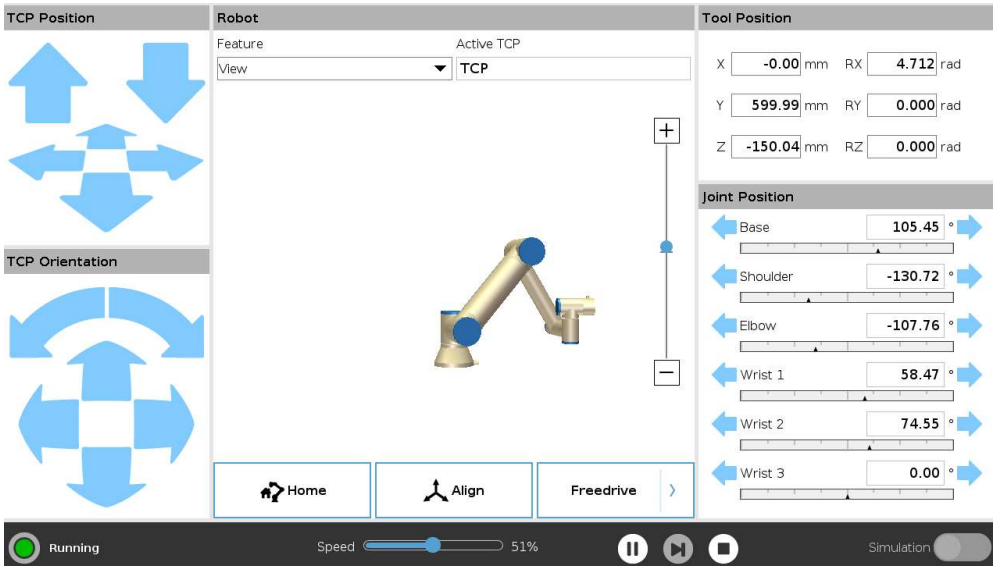


Fig. 1. UR5 robotic manipulator in URSim environment.

The given joint positions and joint velocities consist of 20 positions and looks as Fig.2.

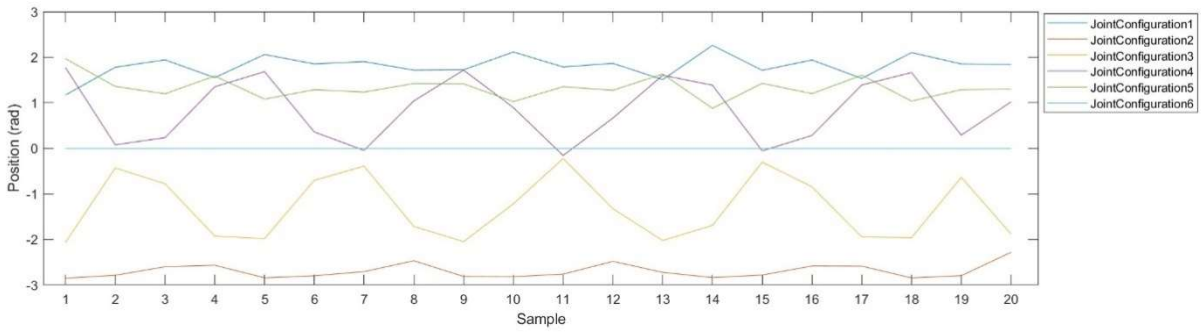


Fig. 2. UR5 robotic manipulator desired joint configurations.

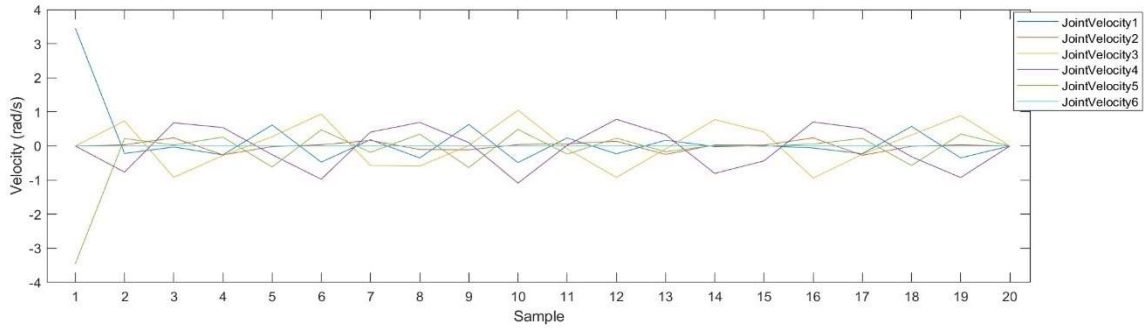


Fig. 3. UR5 robotic manipulator desired joint velocities.

4. TEST RESULTS

Collected data consists of joint configuration, joint velocity, end-effector pose and end effector velocity each having almost 6,000 measurements for every joint. The ones that we will talk about are JointConfiguration and JointVelocity as they can tell us if performed movement is consistent on every joint.

Performed movement is presented by Fig. 4. and their velocity by Fig. 5.

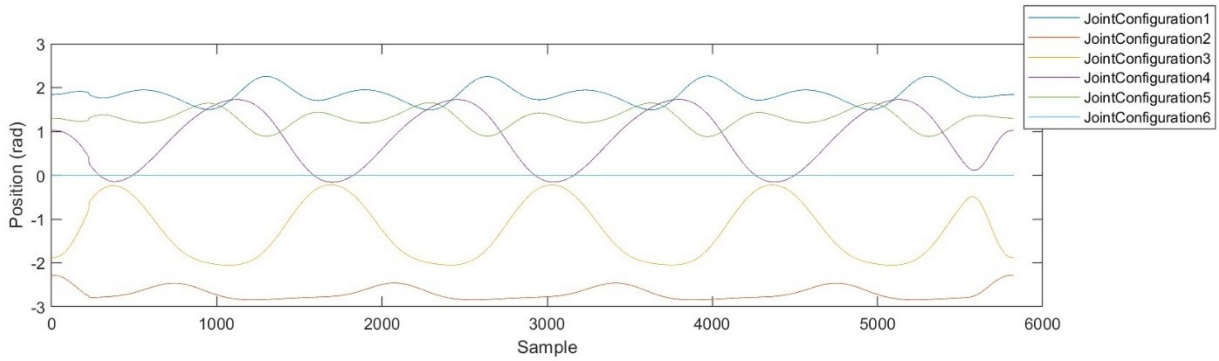


Fig. 4. UR5 robotic manipulator measured joint configurations.

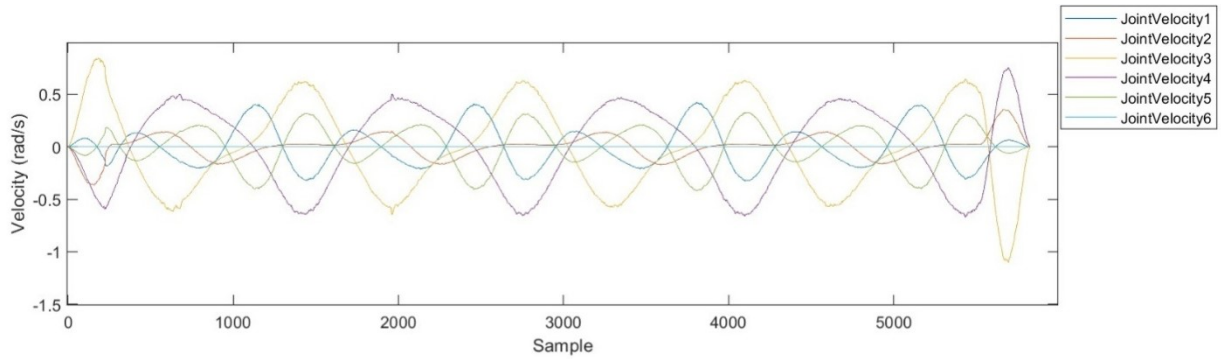


Fig. 5. UR5 robotic manipulator measured velocities.

Comparing Fig. 2 to Fig. 4 and Fig. 3 to Fig. 5 we can clearly see similarities. The difference in the X axis comes from the sample rate for performed movement compared to desired position. Proportions for the X axis are the same. Some overshoot from control points can be explained with the use of bsplinepolytraj. Further tests need to be concluded to verify differences between input and output positions.

CONCLUSIONS

Based on the presented examples ANN controllers show encouraging results in possible accuracy improvement but there is still not enough data to state it, certainly. This shows that AI controllers for robotic manipulators are not fully explored field.

Data obtained from the UR5 offline robot performing a given task in URSim shows high consistency with how the polynomial trajectory should look and slight imperfections from restrictions of the robot. A slight deviation from desired positions is visible when comparing Fig 2, 3 to Fig 4, 5. This should be tested to see if there are errors in bsplinepolytraj translation, restriction of virtual model or delays in connection between ROS and MATLAB. Future development of the project should consist of extensive testing in this field as well as a PID controller and a vast variety of ILC ANN aided controllers tested on an offline simulator and real UR5 robot.

REFERENCES

[1] Ahmad, M.A.; Xu, J.; Deng, X. Preface to the Special Issue on Nano-Enabled Approaches for Sustainable Development of the Construction Industry. Appl. Sci. 2022, 12, 12043. https://doi.org/10.3390/app122312043

[2] Karan, Branko & Vukobratović, Miomir. (1994). Calibration and Accuracy of Manipulation Robot Models. Mechanism and Machine Theory. 29. 479-500. 10.1016/0094-114X(94)90130-9.

[3] Khanesar, Mojtaba Ahmadieh & Piano, Samanta & Branson, David. (2022). Improving the Positional Accuracy of Industrial Robots by Forward Kinematic Calibration using Laser Tracker System. 263-270. 10.5220/0011340200003271.
[4] Illustration, Cover & Norrlof, Mikael. (2000). Iterative Learning Control - Analysis, Design, and Experiments.
[5] Schwegel, Michael & Kugi, Andreas. (2024). A Simple Computationally Efficient Path ILC for Industrial Robotic Manipulators. 2133-2139. 10.1109/ICRA57147.2024.10610623.
[6] Chen, Shuyang & Wen, J.T.. (2021). Industrial Robot Trajectory Tracking Control Using Multi-Layer Neural Networks Trained by Iterative Learning Control. Robotics. 10. 50. 10.3390/robotics10010050.
[7] Bristow, D.A. & Tharayil, M. & Alleyne, A.G.. (2006). A survey of iterative learning. Control Systems, IEEE. 26. 96 - 114. 10.1109/MCS.2006.1636313.
[8] Macukow, Bohdan. 2020. „Sieci neuronowe, historia badań i podstawowe modele". W Prace Naukowe Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, zredagowane przez Andrzej Jakubiak, 1:90–108. Oficyna Wydawnicza Politechniki Warszawskiej. http://www.wydawnictwopw.pl/index.php?s=karta&id=3602.
[9] Hagan MT, Menhaj MB. Training feedforward networks with the Marquardt algorithm. IEEE Trans Neural Netw. 1994;5(6):989-93. doi: 10.1109/72.329697. PMID: 18267874.
[10] Manipulating industrial robots - Performance criteria and related test methods (ISO 9283:1998) Retrieved May 2, 2025 https://standards.iteh.ai/catalog/standards/cen/bd6e0b51-df41-44c2-806f-fbd0f53f30de/en-iso-9283-1998
11[] Mystkowski, A.; Wolniakowski, A.; Kadri, N.; Sewiolo, M.; Scalera, L. Neural Network Learning Algorithms for High-Precision Position Control and Drift Attenuation in Robotic Manipulators. Appl. Sci. 2023, 13, 10854. https://doi.org/10.3390/ app131910854
[12] Chen, Shuyang & Wen, J.T.. (2021). Industrial Robot Trajectory Tracking Control Using Multi-Layer Neural Networks Trained by Iterative Learning Control. Robotics. 10. 50. 10.3390/robotics10010050
[13] Steinhauser, Armin & Swevers, Jan. (2017). Iterative learning of time-optimal trajectories for robotic manipulators. 10.1109/ICMECH.2017.7921092
[14] Ba, Dang & Thien, Nguyen & Bae, Joonbum. (2023). A Novel Iterative Second Order Neural-Network Learning Control Approach for Robotic Manipulators. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3280979
[15] Universal-Robots Online document. Retrieved May 2, 2025, from https://www.universal-robots.com/articles/ur/application-installation/dh-parameters-for-calculations-of-kinematics-and-dynamics/

Arkadiusz Nieciecki: https://orcid.org/0009-0007-6528-4074

Arkadiusz Mystkowski: https://orcid.org/0000-0002-5742-7609

A REVIEW OF THE APPLICATION OF REINFORCEMENT LEARNING METHODS IN THE STABILIZATION OF THE FLEXIBLE MANIPULATOR EFFECTOR

Mateusz ZALEWSKI [1], Arkadiusz MYSTKOWSKI [2]

Department of Automation and Robotics, Faculty of Information Technology and Science, Łomża University, Poland [1]

Departament of Atomatic Control and Robotics, Faculty of Electrical Engineering, Bialystok University of Technology, Poland [2]

mzalewski@al.edu.pl [1], a.mystkowski@pb.edu.pl [2]

ABSTRACT

Flexible manipulators, unlike their rigid counterparts, offer advantages such as lower mass, which translates into lower energy consumption. However, their flexibility introduces challenges in the form of reduced precision and susceptibility to vibrations. Reinforcement learning is a promising solution to the problem, enabling the creation of systems capable of reducing vibrations and increasing the precision of the end effector. This paper reviews the applications of RL in the stabilization of flexible manipulator end effectors in recent years, focusing on vibration suppression and trajectory tracking.

Keywords: reinforcement learning, flexible manipulator, RL, stabilization

INTRODUCTION

The use of manipulators in industry and scientific research is invaluable in the current times. Their greatest advantage is precision, accuracy and repeatability of movement in 3D space. In order to achieve high precision, the manipulator structure must be rigid to avoid positioning errors caused by deformation of any of its parts. However, with the development of technology, flexible manipulators are finding wider and wider application, including in minimally invasive surgical procedures [1] or for performing manipulation tasks on space stations [2].

The flexibility of the manipulator results from various mechanical elements. It can occur both on the links and on the joints of the manipulator. This is a challenge because classic robotic models assume rigid connections [3]. By reducing the mass of the manipulator, actuators that consume less electrical energy can be used, which reduces the cost of purchasing and operating the manipulator. However, the main disadvantage is the reduced precision and vibrations caused by the flexibility of the manipulator [4]. The solution to this problem may be the use of current artificial intelligence methods, thanks to which it is possible to create a system that will allow to reduce these vibrations, which will increase the precision of the end effector [5,6]. Studies from recent years show great potential in the use of reinforcement learning for this task. Thanks to this, even with changing flexibility due to mechanical damage to the manipulator, the system will adapt to the current situation in order to maintain precision [7–9].

This paper aims to review the latest applications of reinforcement learning methods in the stabilization of the end effector of flexible manipulators. In the first chapters, the theoretical background of the manipulator flexibility and reinforcement learning is discussed. Then, different RL algorithms used in Open Access scientific publications from recent years are compared. Finally, challenges and future research directions are discussed.

1. THEORETICAL BACKGROUND

Manipulator flexibility can occur at the links, joints or at the base itself. In such a situation, the manipulator members can be deformed under the influence of gravity, inertia and external forces. Such undesirable flexibility is also called parasitic structural flexibility [10]. The aforementioned flexibility can

occur, for example, in harmonic gears. This mechanism uses the flexibility of a rotating metal element, the model of which can be treated as a spring composed of many elements. The situation is similar with all kinds of elements located between the motor and the manipulator link (Figure 1). However, their inertia is low compared to motors and beams, so in the dynamics characteristics they can be treated as springs [11].

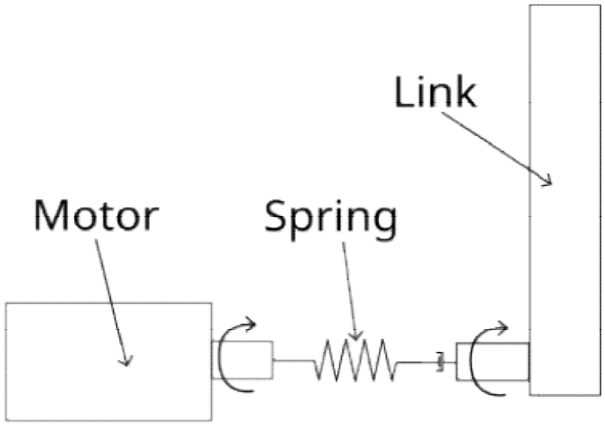


Fig. 1. Schematic diagram of the flexible connection between the motor and the manipulator link.

It happens that flexibility is introduced to reduce mass, but this introduces significant complexity to their analysis and control [12].

1.1 Basics of modeling flexible manipulators

Flexible manipulators, unlike their rigid counterparts, are characterized by susceptibility to elastic deformations, which introduces additional challenges in their modeling and control. Two main approaches to modeling such systems are:

- Assumed Modes Method (AMM): It consists in approximating elastic deformations by combining a limited number of basis functions, which leads to a simplification of the dynamic model. This method is particularly effective for systems with small deformations and allows obtaining models with a limited number of degrees of freedom [13-14]
- Finite Element Method (FEM): It allows for more accurate modeling of the strain distribution in the manipulator structure by dividing it into smaller elements. Although more computationally complex, this method allows for taking into account material and geometric nonlinearities, which is important in the case of large deformations [15].

1.2 Specific Control Challenges Related to Flexibility

The flexibility of manipulators creates a number of specific control challenges that distinguish them from the control of rigid manipulators. The most important of these include:

- Vibration damping: Achieving fast and accurate end effector positioning requires effective damping of vibrations induced during motion [16].
- Control in the presence of uncertainty: The dynamic parameters of flexible manipulators can be difficult to accurately determine and may change over time (e.g., due to load changes). This requires the use of advanced control techniques such as adaptive control and robust control [16].
- Non-colocation of actuators and sensors: Placing actuators and sensors in different locations on a flexible structure leads to non-colocation problems, which complicates the design of stable and efficient control systems [17].

- Unstable zero-phase dynamics: The occurrence of unstable zero-phase dynamics in non-minimum-phase systems limits the applicability of methods based on inversion of the system dynamics [17]
- Time delays: Delays in the control loop, resulting from signal processing or actuator operation, can destabilize the system and degrade its performance [17].

2. REINFORCEMENT LEARNING – BASIC CONCEPTS

Reinforcement Learning (RL) is a field of machine learning in which an agent learns optimal action strategies through interaction with the environment. This process can be formalized in the framework of a decision problem described as a Markov Decision Process (MDP), defined by four elements:

- S – state space,
- A – action space,
- P – transition function (a model of the dynamics of the environment),
- R – reward function.

At each time instant, the agent observes the state of the environment , takes action , receives reward , and transitions to a new state '. The agent's goal is to maximize the expected cumulative reward, often discounted over time.

In the context of control, the RL agent learns a policy function (), a rule that determines the choice of action depending on the observed state. In the problem of stabilizing the effector of a flexible manipulator, the reward function can be, for example, the negative value of the effector deviation from the desired position and the vibration energy of the structure.

2.1. Reinforcement learning methods for controlling manipulators

Reinforcement learning in the control of flexible manipulators uses both classical RL methods and modern deep reinforcement learning (DRL) approaches. Popular algorithms used for robot control tasks include:

- Deep Q-Networks (DQN): this algorithm uses deep neural networks to approximate the Q function, which estimates the expected cumulative reward for taking a given action in a given state [18].
- Deep Deterministic Policy Gradient (DDPG): an actor-critic algorithm designed for continuous action spaces. It is built from two neural networks: an actor learning a deterministic policy, and a critic assessing the quality of the action [19].
- Proximal Policy Optimization (PPO): a policy optimization algorithm with a confidence region constraint. It optimizes the policy to achieve high quality while limiting the policy change at each step, which ensures the stability of the learning processes [19].
- Soft Actor-Critic (SAC): An entropy-based actor-critic algorithm that aims to learn a policy that maximizes the expected reward and etropy of the policy. This encourages exploration of what ultimately produces a more robust policy [19].

In manipulator control, algorithms that are resistant to environmental variability, capable of working in conditions of incomplete observability (e.g. POMDP – Partially Observable Markov Decision Process), and those that can generalize to new trajectories or changing manipulator load conditions are particularly important. In practice, the problem of stabilizing the effector in a flexible manipulator using RL includes challenges related to:

- high-dimensional state space,
- limited knowledge of the dynamics model,
- the requirement of safe learning (minimizing damage to the physical system during training),
- the need for rapid adaptation to unforeseen disturbances.

In response to these challenges, simulation-to-real transfer approaches are being developed, using simulation models to pre-train agents and safe RL techniques.

3. REVIEW OF RL APPLICATIONS IN THE STABILIZATION OF THE EFFECTOR OF FLEXIBLE MANIPULATORS

The last three years have seen the publication of numerous scientific papers on the use of reinforcement learning in the stabilization of the effector of flexible manipulators. These papers cover a wide range of algorithms, control strategies, and types of flexible manipulators.

3.1 RL for vibration control

Many studies have focused on the use of reinforcement learning for active vibration suppression. In the paper by Shu et al. [18], a method using a deep residual shrinking network based on a prioritized multi-reward experience retrieval mechanism was proposed for the control of high-frequency and high-dimensional vibration. The vibration reduction was achieved by 20,240 dB, which was superior to the DDPG algorithm which achieved a reduction of 12,728 dB. In addition, the network used had a much smaller number of parameters. Adel et al. [20], while studying the vibration control of a flexible manipulator, proposed a method for end-effector position estimation based on the virtual sensor principle and function approximation schemes such as neural networks, support vector machines, and Gaussian processes.

The work by Sasaki et al. [21] focuses on the use of Trust region policy optimization (TRPO) algorithm to simultaneously control vibration and position of a two-joint flexible manipulator. Reward functions are designed to minimize vibration and deformation of the manipulator during movement to the desired position. The proposed approach effectively suppresses both vibration and deformation.

In their paper, Wanyonyi et al. [22] conducted a comparative analysis of different reinforcement learning algorithms in the context of vibration control of simple systems such as mass-spring-damper system. PPO and DQN algorithms were implemented for vibration control of discrete action space system. From the obtained results, it was determined that PPO algorithm outperformed DQN algorithm in training, but it needed more time for setup.

3.2 RL for trajectory tracking

Many works focus on using RL to enable flexible manipulators to follow a designated end-effector trajectory while suppressing vibration (21). Such studies use PPO and DDPG algorithms to learn a control policy that minimizes trajectory tracking errors and suppresses vibration.

3.3 Comparison of scientific articles

In order to provide a comparison of different approaches to stabilizing flexible manipulators using reinforcement learning algorithms, selected articles published in recent years are presented in Table 1. The table includes key aspects of each study, including the RL algorithms used, the main research objectives, the use of performance metrics, and key conclusions.

The comparative analysis of these papers reveals several key trends and conclusions. Deep reinforcement learning algorithms are widely used in the task of stabilizing the end effector of flexible manipulators. Additionally, these algorithms demonstrate the ability to learn complex control policies directly from the interactions with the environment, without the need for accurate dynamic models. The design of reward functions plays a key role. These functions are usually designed to reward the agent for achieving desired states and punish undesirable behavior. However, transferring learning from simulations to real systems remains a challenge. This is often due to the computational complexity that prevents the algorithm from being later implemented in real systems.

Table 1. Comparison of scientific articles on the use of RL in manipulator effector stabilization.

Article	Algorithm(s)	Main research goals	Performance metrics	Key conclusions
Tapia Sal Paz et al., 2025 [19]	SAC, DDPG, PPO	End effector stabilization during disassembly of flexible elements	Reduction of interaction force, disassembly success rate	RL effectively reduces interaction strength by at least 20% compared to traditional methods. Adaptive reward function improves generalization
Sasaki et al., 2023 (21)	PGM, TRPO	Achieving the target position while minimizing vibration and stress at the base of the link	Distance between end effector and target position, minimizing stress at the link root	The use of reinforcement learning successfully suppressed vibrations and stresses while moving the end effector to the target position.
Shu et al., 2024 (18)	DRSL-MPER, DRSN, TD3	Vibration damping with computational efficiency that enables adaptation to real systems	Vibration reduction, number of neural network parameters	Better vibration damping was achieved with the proposed DRSL-MPER algorithm than the standard DDPG algorithm, while reducing the number of neural network parameters by more than 7.5 times.
Dhakate et al., 2025 (23)	RL (model-free)	Kinematic control of the end effector position with consideration of rope sag	Accuracy of end effector positioning, an advantage over the classic kinematic approach	The RL-based controller effectively handles rope sag and outperforms classical kinematic methods, especially under dynamic conditions.
Viswanadhapalli et al., 2024 (8)	DRL - DDPG	Improving tracking performance while managing system constraints	Trajectory tracking accuracy, vibration suppression, immunity to external interference	The proposed DRL-DDPG controller outperforms traditional MPCs in terms of trajectory tracking and immunity to external interference.

To summarize the RL algorithms, Table 2 presents a brief description, typical applications in robot control, and their strengths and weaknesses in the context of stabilizing flexible manipulators.

Table 2. Summary of RL algorithms used in manipulator effector stabilization.

Algorithm	Description	Typical applications	Strengths	Weaknesses
DQN	It uses deep neural networks to approximate the Q function	Control in discrete action spaces, navigation, games	Can learn complex control strategies without a model	Limited to discrete action spaces, potential learning instability
DDPG	An actor-critic algorithm for continuous action spaces	Controlling robot arms, autonomous vehicles	Suitable for continuous action spaces, relatively simple to implement	Hyperparameter sensitive, potential learning instability
PPO	Confidence Region Constraint Policy Optimization Algorithm	Robot control, manipulation tasks	Stable learning process, copes well with continuous and discrete action spaces	Implementation complexity
SAC	Entropy-based actor-critic algorithm.	Robot control, manipulation tasks, exploration	Promotes exploration, may lead to more resilient policies	Algorithm Complexity
TRPO	Confidence Region Policy Optimization Algorithm, directly optimizes policy with a policy change constraint	Robot control	Theoretically guaranteed policy	Complexity of implementation, requires large computational effort

4. CHALLENGES AND FUTURE TRENDS

Despite the progress in the application of reinforcement learning algorithms to stabilize the end effector of flexible manipulators, there are still challenges that require further research. One of the challenges that researchers face is the complexity of the state and action space of multi-degree-of-freedom manipulators. Another significant challenge is the transfer of learning from simulations to real systems. Additionally, exploration in environments with sparse rewards can be difficult and time-consuming. Investigating the use of RL in adaptive control of flexible manipulators under changing environmental conditions is a promising research direction. The development of algorithms that require less interaction with the environment may be crucial for practical applications.

5. CONCLUSIONS

In summary, the review of the scientific literature in recent years indicates a growing interest and intensive research on the application of reinforcement learning methods in the stabilization of the end effector of flexible manipulators. Various reinforcement learning algorithms, including DQN, DDPG, PPO, and SAC, have shown promising results in the vibration control and trajectory tracking of flexible manipulators. Despite significant progress, challenges such as the complexity of the state and action space, the design of reward functions, and the transfer of learning from simulation to reality still require further investigation. Future research will probably focus on the development of more sample-efficient methods and algorithms requiring less interaction with the environment. Reinforcement learning is a promising approach to solving complex control and stabilization problems, and further development in this field has the potential to significantly expand the capabilities of robotic systems.

REFERENCES

[1] Zhang Y, Lu M. A review of recent advancements in soft and flexible robots for medical applications. Int J Med Robot. 2020 Jun;16(3):e2096.

[2] Sabatini M, Gasbarri P, Monti R, Palmerini GB. Vibration control of a flexible space manipulator during on orbit operations. Acta Astronaut. 2012 Apr;73:109–21.

[3] Della Santina C. Flexible Manipulators. In: Ang MH, Khatib O, Siciliano B, editors. Encyclopedia of Robotics [Internet]. Berlin, Heidelberg: Springer Berlin Heidelberg; 2021 [cited 2025 Apr 6]. p. 1–15. Available from: https://link.springer.com/10.1007/978-3-642-41610-1_182-1.

[4. Lee TS, Alandoli EA. A critical review of modelling methods for flexible and rigid link manipulators. J Braz Soc Mech Sci Eng. 2020 Oct;42(10):508.

[5] Abdollahi F, Talebi HA, Patel RV. A Stable Neural Network-Based Observer With Application to Flexible-Joint Manipulators. IEEE Trans Neural Netw. 2006 Jan;17(1):118–29.

[6] Fu X, Ai H, Chen L. Repetitive Learning Sliding Mode Stabilization Control for a Flexible-Base, Flexible-Link and Flexible-Joint Space Robot Capturing a Satellite. Appl Sci. 2021 Aug 31;11(17):8077.

[7] He W, Gao H, Zhou C, Yang C, Li Z. Reinforcement Learning Control of a Flexible Two-Link Manipulator: An Experimental Investigation. IEEE Trans Syst Man Cybern Syst. 2021 Dec;51(12):7326–36.

[8] Viswanadhapalli JK, Elumalai VK, S. S, Shah S, Mahajan D. Deep reinforcement learning with reward shaping for tracking control and vibration suppression of flexible link manipulator. Appl Soft Comput. 2024 Feb;152:110756.

[9] Long T, Li E, Hu Y, Yang L, Fan J, Liang Z, et al. A Vibration Control Method for Hybrid-Structured Flexible Manipulator Based on Sliding Mode Control and Reinforcement Learning. IEEE Trans Neural Netw Learn Syst. 2021 Feb;32(2):841–52.

[10] Della Santina C. Flexible Manipulators. In: Ang MH, Khatib O, Siciliano B, editors. Encyclopedia of Robotics [Internet]. Berlin, Heidelberg: Springer Berlin Heidelberg; 2021 [cited 2025 Apr 8]. p. 1–15. Available from: https://link.springer.com/10.1007/978-3-642-41610-1_182-1.

[11. Tang L, Zhao D. Dynamic Modeling of a Flexible-Link Flexible-Joint System with Tip Mass Considering Stiffening Effect. Appl Sci. 2022 Jun 27;12(13):6496.
[12] Dermawan D, Abbas H, Syam R, Djafar Z, Muhammad AK. DYNAMIC MODELING OF A SINGLE-LINK FLEXIBLE MANIPULATOR ROBOT WITH TRANSLATIONAL AND ROTATIONAL MOTIONS. IIUM Eng J. 2020 Jan 20;21(1):228–39.
[13] Feng C, Chen W, Shao M, Ni S. Trajectory Tracking and Adaptive Fuzzy Vibration Control of Multilink Space Manipulators with Experimental Validation. Actuators. 2023 Mar 25;12(4):138.
[14] Martins JM, Mohamed Z, Tokhi MO, Sá Da Costa J, Botto MA. Approaches for dynamic modelling of flexible manipulator systems. IEE Proc - Control Theory Appl. 2003 Jul 24;150(4):401–11.
[15] Tokhi MO, Mohamed Z, Hashim AWI. Modelling of a Flexible Robot Manipulator Using Finite Element Methods: A Symbolic Approach. J Low Freq Noise Vib Act Control. 1999 Jun;18(2):63–76.
[16] Li B, Li X, Gao H, Wang FY. Advances in Flexible Robotic Manipulator Systems — Part II: Planning, Control, Applications, and Perspectives. IEEE/ASME Trans Mechatron. 2024 Jun;29(3):1680–9.
[17] Kumar DEV. Performance augmentation of Flexible-Link manipulator in presence of uncertainty.
[18] Shu Y, He C, Qiao L, Xiao B, Li W. Vibration Control with Reinforcement Learning Based on Multi-Reward Lightweight Networks. Applied Sciences. 2024 Apr 30;14(9):3853.
[19] Tapia Sal Paz B, Sorrosal G, Mancisidor A, Calleja C, Cabanes I. Reinforcement Learning-Based Control for Robotic Flexible Element Disassembly. Mathematics. 2025 Mar 28;13(7):1120.
[20] Adel M, Ahmed SM, Fanni M. End-Effector Position Estimation and Control of a Flexible Interconnected Industrial Manipulator Using Machine Learning. IEEE Access. 2022;10:30465–83.
[21] Sasaki M, Muguro J, Kitano F, Njeri W, Maeno D, Matsushita K. Vibration and Position Control of a Two-Link Flexible Manipulator Using Reinforcement Learning. Machines. 2023 Jul 19;11(7):754.
[22] Wanyonyi SN, Ferhat I, Kurtulus DF. Comparative Study on Vibration Control Using Reinforcement Learning. In: 2023 10th International Conference on Recent Advances in Air and Space Technologies (RAST) [Internet]. Istanbul, Turkiye: IEEE; 2023 [cited 2025 May 9]. p. 01–6. Available from: https://ieeexplore.ieee.org/document/10197999/.
23] Dhakate R, Jantos T, Allak E, Weiss S, Steinbrener J. CaRoSaC: A Reinforcement Learning-Based Kinematic Control of Cable-Driven Parallel Robots by Addressing Cable Sag through Simulation [Internet]. arXiv; 2025 [cited 2025 May 9]. Available from: http://arxiv.org/abs/2504.15740.

Mateusz Zalewski: https://orcid.org/0000-0001-9958-7718
Arkadiusz Mystkowski:https://orcid.org/0000-0002-5742-7609

SECURITY OF OBJECT DETECTION SYSTEMS UTILIZING STEREOSCOPIC IMAGE PROCESSING TECHNIQUES

Marta CHODYKA [1], Jakub BEDNARCZYK [2]

University of Łomza, Poland [1, 2]

mchodyka@al.edu.pl [1], jakub.j.bednarczyk@gmail.com [2]

ABSTRACT

The paper analyzes the security of a laboratory object detection system based on close-range stereoscopic vision (0.60 m – 0.90 m). Four approaches were investigated: classic block-matching StereoBM, semi-global StereoSGBM, a lightweight deep network Fast ACV (ONNX implementation), and an original hybrid algorithm combining a trained cascade classifier with local stereo matching based on normalized correlation. Experiments were conducted on objects with varied textural and color characteristics at three camera baseline distances (7.5 cm / 18.5 cm / 23.5 cm), under ideal lighting conditions and with induced photometric disturbances (overexposure and dimming of one camera channel). Results showed that StereoSGBM provided the best accuracy-speed trade-off (error 3–5 mm; continuous depth map even under disturbance conditions), whereas StereoBM featured the highest processing speed at the cost of increased noise under uneven lighting. The Fast ACV network achieved the lowest error (< 2%) in reference scenes but reversed depth relationships under severe overexposure, indicating the need for further training on datasets including challenging lighting scenarios. The hybrid algorithm determined object distances with 3–4% accuracy while reducing computational load through selective processing of regions of interest (ROI), achieving ≥15 fps suitable for real-time operation. Its main drawback remains its dependency on the effectiveness of the applied detector and measurement issues during occlusion of the nearest object. Analysis indicates that an optimal camera baseline of 18.5 cm balances near-object visibility and parallax resolution. System resilience to lighting disturbances can be improved using methods based on mutual information (SGM) or adequately expanded training of deep networks. A redundancy strategy was proposed, combining fast classical matching for initial obstacle detection and a deep or hybrid layer for verification of critical cases. Future research directions include disparity uncertainty estimation, network training under low-light conditions, and integration of stereovision with radar for enhanced-range security systems.

Key words: stereovision, object detection, security, stereo matching algorithms, deep learning, photometric robustness

INTRODUCTION

In modern security systems from advanced driver assistance systems (ADAS) to autonomous warehouse robots correct object identification and precise spatial localization play crucial roles. A delayed or inaccurate distance evaluation can directly impact system effectiveness in braking, obstacle avoidance, or halting robotic manipulators in warehouse robotics. Therefore, ensuring effective, rapid, and reliable operation of object detection and localization systems is critical for user safety and infrastructure protection.

Stereoscopic cameras, mimicking human binocular vision, simultaneously provide texture and geometric information about scenes, offering significant advantages over monocular systems lacking absolute depth scaling. This capability allows precise distance measurement to detected objects, significantly enhancing the quality and reliability of security systems. Literature emphasizes that integrating semantic classification with accurate distance measurements substantially improves situational awareness and reduces false alarms [6]. However, practical implementation of stereoscopic

technology in security applications presents several technical challenges. The first challenge is stereoscopic matching precision, as even minor errors of a few centimeters can influence the effectiveness of security system activation. A second critical challenge is photometric robustness, the system's ability to operate correctly under changing or uneven lighting conditions, potentially causing significant luminance differences between left and right images. A third issue is the temporal performance of the system, especially in scenarios requiring near-real-time responses (≥ 15–30 fps), posing significant challenges for advanced deep learning methods. The fourth aspect involves selecting and controlling the geometry of the stereoscopic setup, as choosing an optimal camera baseline is crucial for maintaining balance between long-range object measurement capabilities and avoiding occlusions or dead zones in stereo views [8].

This paper aims to provide a comprehensive review, practical implementation, and comparison of three representative classes of stereo vision methods for security applications: (i) classical local and semi-global methods, (ii) modern approaches using deep neural networks, and (iii) an original hybrid solution integrating object detection with depth measurement performed exclusively in regions of interest. Experiments were carried out in a laboratory environment with objects exhibiting diverse texture and color characteristics, within distances ranging from 0.60 to 0.90 m, at three camera baseline distances (7.5 cm, 18.5 cm, 23.5 cm), under two lighting scenarios: ideal and photometrically disturbed (overexposure and dimming of one camera channel). The experimental results allowed formulation of engineering recommendations regarding optimal algorithm selection, geometric parameters of the camera setup, and computational redundancy strategies to meet stringent modern security application requirements.

LITERATURE REVIEW

In contemporary security system applications, encompassing advanced driver assistance systems (ADAS) and autonomous warehouse robots, correct classification of objects and precise, timely localization in space are crucial requirements. One of the most effective technologies for achieving these objectives is stereoscopic vision, mimicking human binocular vision. Stereoscopic systems simultaneously acquire texture and geometric scene information, assuming correct pixel matching and disparity calculation [6]. However, the implementation of stereoscopic technologies faces significant challenges such as measurement accuracy, photometric robustness (e.g., uneven illumination or contrast differences), real-time performance, and optimal geometric setup [8]. Accuracy is crucial, as even minor errors of a few centimeters can affect system effectiveness in emergency braking or collision avoidance [1].

Literature typically classifies stereo matching methods according to key stages: matching cost calculation, aggregation, disparity selection, and depth map refinement [7]. Simple local methods, such as block-matching algorithms (StereoBM), use fixed support windows and similarity measures like Sum of Absolute Differences (SAD) or Sum of Squared Differences (SSD). These methods are favored for ease of hardware implementation and high processing speed but suffer significantly from noise and texture-related artifacts, leading to grainy depth maps [3, 5]. Significant improvements in disparity map quality came from semi-global optimization methods, particularly Semi Global Matching (SGM), combining local matching costs with semi-global optimization across multiple directions. SGM employs mutual information metrics robust to exposure differences between image channels, generating consistent and continuous depth maps, beneficial in automotive applications despite higher computational demands [1]. Recent developments have focused intensively on deep neural network approaches. Initial studies leveraged CNNs for matching cost calculation, markedly enhancing depth map precision [11]. Subsequent research introduced comprehensive end-to-end trained models predicting disparity maps directly from stereo image pairs [2, 4]. A notable recent advancement, the ACVNet architecture, utilizes Attention Concatenation to dynamically weight correlation information, achieving high accuracy with reasonable computational requirements [10]. Despite these advances, challenges remain regarding deep model robustness under varied lighting and hardware variability [9].

An alternative hybrid approach selectively computes depth only in regions identified by object detection methods, significantly reducing computational load while maintaining precision in critical image regions, such as potential collision areas [6]. Another important literature aspect concerns optimal geometry selection for stereo camera systems. Research suggests an optimal stereo baseline balancing parallax resolution for distant objects and minimizing near-object occlusions [8]. In engineering practice, recommended camera baselines typically range around 18-20 cm for automotive and autonomous robot applications at close to medium ranges.

In summary, classic block-matching and SGM methods remain attractive when prioritizing speed and deterministic behavior, whereas deep learning approaches provide maximum accuracy, albeit at higher computational costs and potential reliability risks beyond training conditions. Hybrid detection-stereo combinations present a promising path, reducing computations while enhancing semantic usefulness. The last two decades of literature consistently emphasize that effective and secure stereovision systems require harmony among geometry, photometry, computational power, and semantic knowledge. No single algorithm ensures universal reliability, yet a deliberate combination and fusion of available methods can achieve stringent security requirements..

RESEARCH METHODOLOGY

To evaluate the effectiveness of selected stereoscopic depth measurement methods, a laboratory measurement system was constructed. It comprised two synchronized digital camera modules (Logitech C270, native resolution 1280 × 720 px, focal length 4 mm) mounted on a common rigid beam made from an aluminum profile. The use of neodymium magnets allowed smooth adjustment of the baseline distance between the optical axes of the lenses within the range of 12 cm to 30 cm, without compromising the parallel alignment of the optical axes. A schematic diagram of the setup is shown in Figure 1.

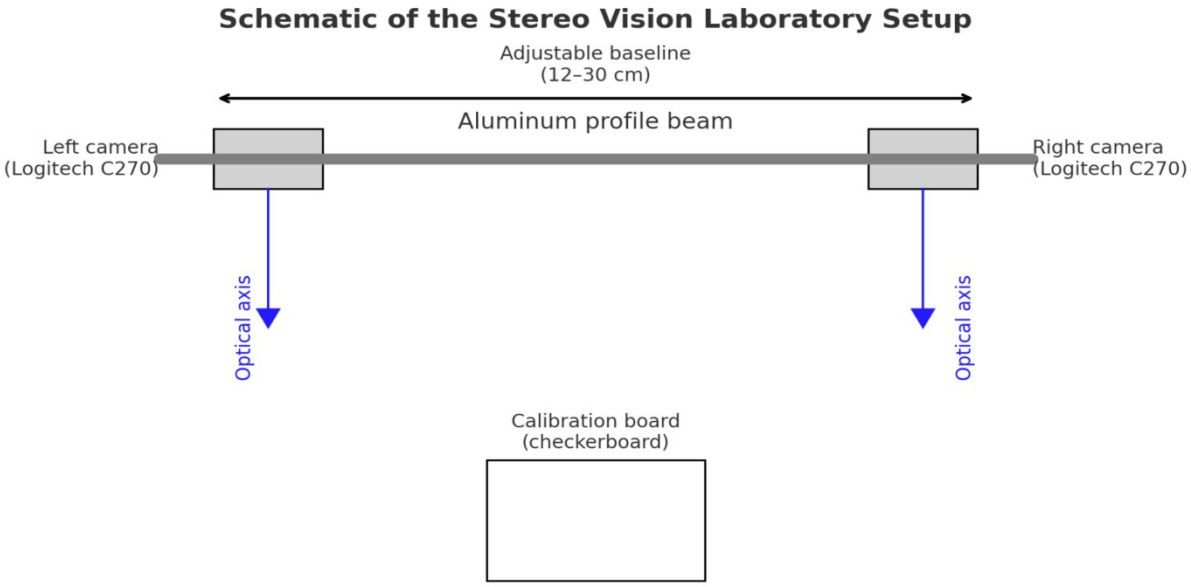


Fig. 1. Schematic of the stereo vision laboratory setup showing the arrangement of Logitech C270 cameras, optical axes, calibration checkerboard, and the adjustable baseline range.

Before each measurement series, a full rectification of the stereo setup was performed using Zhang's method [12], employing a checkerboard pattern with 20 × 20 mm squares. This allowed the reduction of residual image misalignment to less than 0.05 px, ensuring result comparability across various baseline distances.

Processing was conducted on a workstation equipped with an Intel Core i5 13420H processor, 16 GB DDR5 RAM, and an NVIDIA RTX 4050 graphics card. The implementation was performed in Python using OpenCV 4.9.0 and the ONNX Runtime environment. Four algorithmic variants were investigated. The first one, StereoBM, served as a reference for local methods; the matching window (9 × 9 px) and 64 disparity levels were preselected to minimize mean deviation on a calibration dataset. The second variant, StereoSGBM, represented semi-global methods; parameters P1, P2, the number of scanning directions, and the maximum disparity were tuned to balance depth-map smoothness and computation time. The third group comprised the deep-learning-based "Fast" version of the ACVNet model, provided in ONNX format; input images were scaled to 640 × 480 px, and resulting disparity maps were directly extrapolated to the original resolution. The last, original hybrid variant combined YOLOv5 M-based object detection (analyzing only the left image) with template matching in constrained windows of the right image. Local correlation was normalized to reduce sensitivity to exposure differences, while the shift range was geometrically calculated to cover distances from 1 m to 12 m based on the current baseline.

The research program was divided into three scenarios. In the first scenario, described as ideal conditions, the scene was illuminated by two studio lamps with a color temperature of 5600 K, and ambient daylight was eliminated by an opaque curtain. Three spherical calibration objects (apples with diameters of 75 ± 2 mm) were positioned against a neutral background at distances of 0.60 m, 0.75 m, and 0.90 m, measured using a steel tape with an accuracy of 2 mm. Twelve image pairs were captured for each configuration to minimize temporal sensor noise effects. Figure 2 shows sample left and right camera images with appropriate illumination for measurements. Each algorithm underwent evaluation using four representative examples of such stereo image pairs.

Fig. 2. Stereo image pair under ideal lighting conditions.

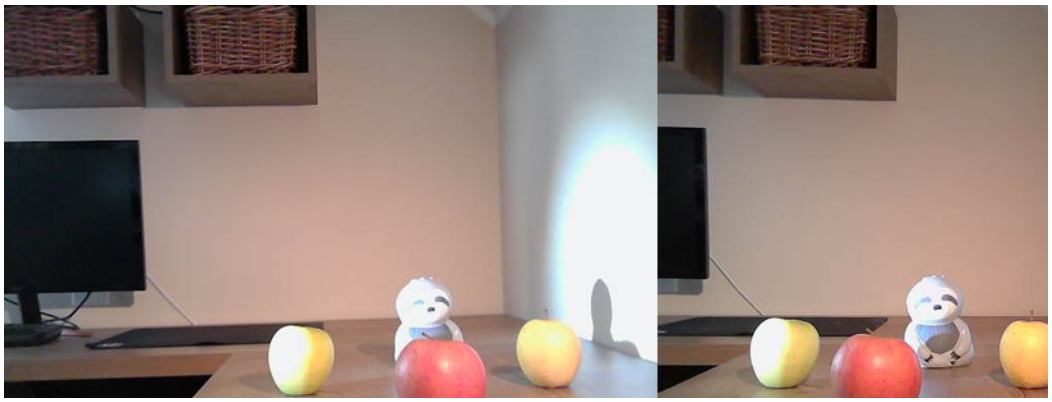


Fig. 3. Stereo image pair with introduced overexposure.

The second scenario introduced photometric disturbances: the left camera was periodically overexposed using a short flash from a 3000 lm LED diode, while the right camera lens was darkened with an ND 0.6 filter. Additional shots were recorded in a combined configuration. A representative pair of stereo images with induced overexposure is presented in Figure 3.

Figure 4 presents a disparity map obtained using the deep neural network algorithm ACVNet (ONNX) for a scene with localized object overexposure. Visible artifacts and loss of depth information in the overexposed regions can be observed.

Fig. 4. Disparity map obtained using the deep network algorithm ACVNet (ONNX) under conditions of local object overexposure.

Figure 5 presents the result of the hybrid algorithm, which combines a cascade classifier and local stereo matching, under conditions of localized overexposure. The algorithm correctly detected most objects; however, disparity estimation issues were observed within the overexposed region.

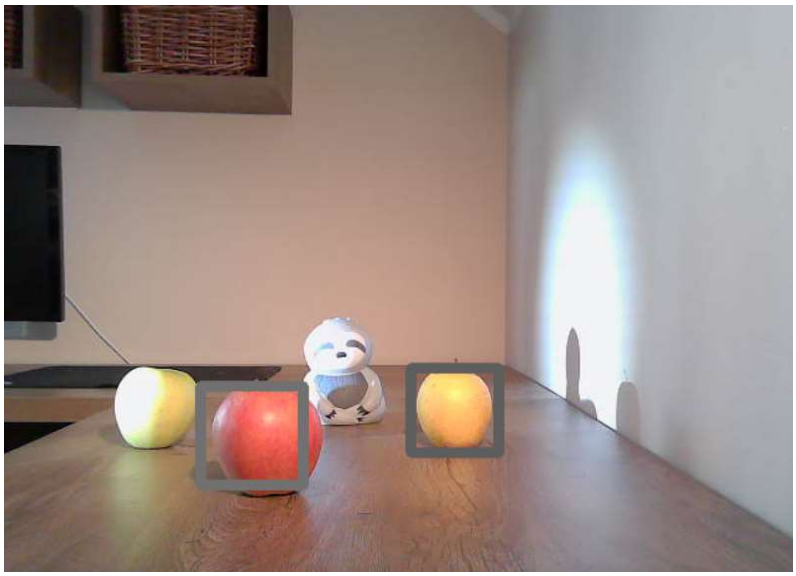


Fig. 5. Results of the hybrid algorithm (Cascade classifier + local stereo matching) under conditions of local overexposure.

The third stage analyzed the influence of stereopair geometry the system was successively configured for baseline distances of 7.5 cm, 16 cm, and 23.5 cm, with objects placed identically as in the first scenario, allowing separation of baseline effects from target positioning effects.

For each pair of images, the absolute linear error, representing the deviation of the measured distance from the reference distance, was calculated according to formula:

$$e_{|abs|=d_{measured}-d_{reference}\vee} \tag{1}$$

where:

$d_{measured}$ – distance measured by the stereoscopic system,

$d_{reference}$ – reference (actual) distance.

Subsequently, the RMS error relative to the reference distances was calculated according to formula:

$$e_{RMS} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(d_{measured,i} - d_{reference,i})^2} \tag{2}$$

where:

$d_{measured,i}$ – measured distance in the i-th measurement,

$d_{reference,i}$ – reference (actual) distance in the i-th measurement,

N – total number of measurements performed.

Moreover, the processing time per frame was measured. Processing times from 100 repetitions were sorted in ascending order ($t_1 < t_2 < \cdots < t_N$) and subsequently averaged after discarding the extreme 5% of results (2.5% shortest and 2.5% longest times), thus eliminating the cold-cache effect. The trimmed mean processing time was calculated according to formula:

$$\underline{t}_{trimmed} = \frac{1}{N-2k}\sum_{i=k+1}^{N-k} t_i \, , k = 0.0025 \cdot N \tag{3}$$

where:

t_i – processing time of the i-th frame,

N – total number of measurements performed,

k – number of discarded extreme results (2.5% from each end).

For the hybrid variant, the YOLO detector's effectiveness was additionally evaluated. The recall metric, defining the percentage of all objects correctly detected by the algorithm, and the precision metric, describing how frequently detected objects were correctly identified, were assessed. Additionally, the proportion of cases where depth measurements failed due to the absence of a clear correlation peak between the left and right images was analyzed. This metric reflected the stability and robustness of the applied stereo method under challenging measurement conditions. The structured protocol described above ensured a coherent dataset enabling objective comparisons of classical matching methods, deep networks, and selective approaches across a full range of conditions relevant to safety-critical systems.

EXPERIMENTAL RESULTS

In the first measurement series, conducted under stable and uniform lighting conditions (5600 K LED lamps, daylight fully blocked), all algorithms correctly reconstructed the order of three test objects—apples placed at distances of 0.60 m, 0.75 m, and 0.90 m—but reported differing error values. StereoBM achieved an average absolute error of 5–10 mm (1–2% of the measurement range) but generated a noisy disparity map, where the smooth table surface appeared as a cluster of points with zero values. Using the StereoSGBM algorithm reduced the error to 3–5 mm, while applying a depth discontinuity penalty resulted in a uniform disparity map for the table surface; apple contours were determined with sub-millimeter precision. Fast ACVNet (ONNX version at 640 × 480 px resolution) achieved the lowest error, not exceeding 2% (3–5 mm), with variability twice as low as that of SGBM. The network successfully reconstructed even a thin wire in the background, missed by classical

methods. The hybrid algorithm (HYB), restricting stereo computations only to regions detected by YOLOv5m, reported distances with an error of 1–2%, primarily due to disparity quantization (step of 1 px) and narrowing the search window to ±10 px around the predicted parallax. The background was entirely ignored, reducing computational load. A graph comparing average absolute errors of different stereo methods under ideal lighting conditions is presented in Figure 6.

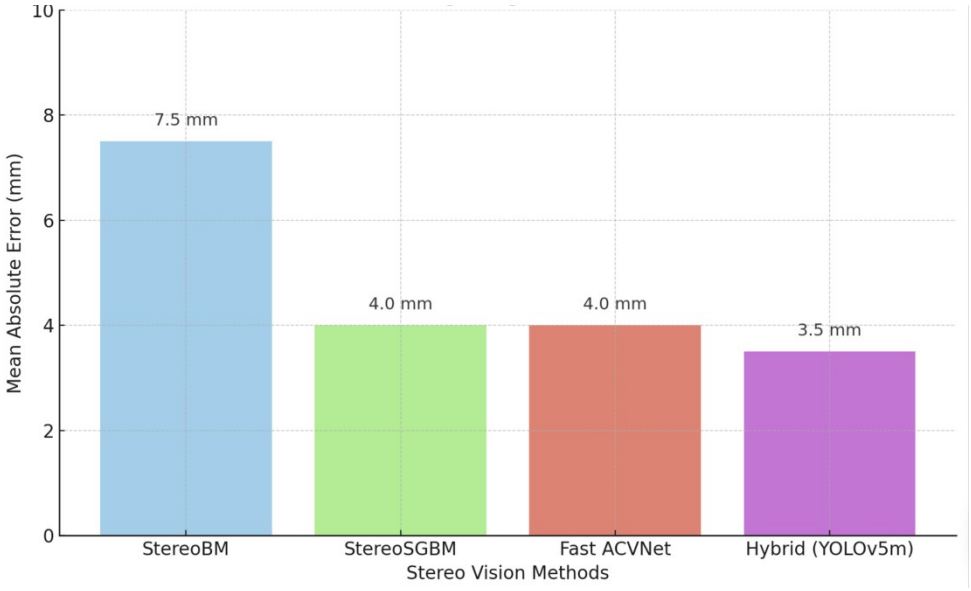


Fig. 6. Comparison of mean absolute errors (mm) for StereoBM, StereoSGBM, Fast ACVNet, and Hybrid (YOLOv5m) methods under ideal lighting conditions.

After establishing baseline accuracy, photometric disturbances were introduced: initially, the left lens was overexposed using a 3000 lm strobe, then the right lens was darkened using an ND 0.6 filter, and finally, both effects were combined. Under these challenging conditions, the StereoBM method lost stability its error increased to 4–5 cm, random matching islands appeared in the disparity maps, and correspondence failed even on well-textured apple surfaces. In contrast, StereoSGBM, employing a mutual-information-based cost function, maintained an average error within 10 mm and preserved map continuity except in areas of intense glare. The Fast ACVNet method, thanks to luminance augmentation during training, experienced only a slight increase in error (from 4 mm to approximately 7 mm), with visible artifacts appearing only during peak flash conditions. The hybrid method (HYB) inherited the robustness of the YOLO detector (though correct detections dropped by approximately 10%), yet the local stereo method faced ambiguous correlation peaks in overexposed areas, increasing local errors up to approximately 10%. Nevertheless, the system continued correctly classifying objects as near or distant, crucial in alarm-oriented applications.

The subsequent stage investigated the influence of camera baseline distance: at 7.5 cm baseline, the disparity for the furthest apple dropped to approximately 6 px, increasing BM and HYB errors by 1–2 mm due to quantization. Conversely, at a 23.5 cm baseline, accuracy improved for distant objects; however, the apple at 0.60 m was partially cropped in the right camera's view, causing HYB to fail in depth estimation, and resulting in gaps in foreground disparity maps for BM and SGBM. An optimal compromise was identified at a baseline of 16 cm—standard in other tests—ensuring sufficient disparity resolution with minimal occlusions.

The performance of all methods was measured on an HP Omen 16 laptop equipped with an Intel i5 13420H CPU and an RTX 4050 GPU; results are summarized in Table 1. StereoBM demonstrated unmatched processing speed (66 fps on CPU), but was sensitive to photometric disturbances. SGBM achieved 31 fps after GPU acceleration, providing more stable depth maps. Fast ACVNet managed only 12 fps despite optimized TensorRT inference, with the full 720p model exceeding 200 ms per image

pair. The hybrid method (HYB), by restricting stereo matching to 2–3 regions of interest (ROI), processed each frame in approximately 50 ms (20 fps), sufficient for robotic platforms operating below 30 km/h, while simultaneously providing selective, semantically focused measurement of critical objects.

Tab. 1. Average processing time of a stereo image pair depending on the algorithm.

Algorithm	Hardware / mode	Average time [ms]	Speed [fps]
StereoBM	CPU (i5 13420H)	15	66
StereoSGBM	CPU	120	8
StereoSGBM	CUDA (RTX 4050)	32	31
Fast ACVNet (640 × 480)	TensorRT (RTX 4050)	85	12
HYB (YOLOv5m + NCC, 2–3 ROI)	GPU (RTX 4050)	50	20

The overall results indicate that the classic BM method is attractive when extreme processing speed is critical; however, its usefulness is limited to scenes with controlled lighting conditions. StereoSGBM, particularly in its GPU-accelerated implementation, provides a beneficial balance between speed and accuracy, and better handles luminance fluctuations. Fast ACVNet excels in precision and completeness of depth maps but at a significant computational cost. The proposed hybrid algorithm (HYB) presents a valuable compromise: its selective approach allows faster operation than a full-depth neural network while providing localized depth measurements sufficient for accurate collision risk assessment, particularly when the primary objective is to identify potentially hazardous objects rather than generate a dense 3D map of the entire scene.

DISCUSSION

The results obtained from the stereovision experiments using test apples provide several key insights for designing secure object detection systems. Firstly, incorporating depth information significantly enhances the value of visual detection alone: the trained cascade classifier (179 positive samples, minHitRate = 0.998, maxFalseAlarmRate = 0.3) accurately recognizes an apple, but only parallax measurement allows determining if an object is located within a critical collision zone. Measurements indicated that even modest disparity resolution (1 px step) with an 18.5 cm baseline was sufficient to estimate distances between 0.60–0.90 m with a mean error of 2.8–5.3%, already enabling accurate threat classification. Concurrently, the results demonstrate that depth accuracy must be known and integrated into safety logic. For a 7.5 cm baseline, the error for an object at approximately 0.90 m increased above 8% (up to 11%), potentially causing overly aggressive or overly cautious maneuver decisions in vehicles. Therefore, redundancy is recommended in practice: a fast classical algorithm (StereoBM or SGBM) initially detects obstacles, followed by distance verification using a more accurate method (e.g., a deep learning variant) in the subsequent frame [1]. Such a two-step strategy has long been standard practice in aviation and automotive applications.

Photometric robustness emerged as another critical parameter. In scenarios with localized overexposure and dimming of one lens, StereoBM completely lost disparity coherence, generating distances deviating several centimeters from actual values. StereoSGBM, employing a mutual-

information-based cost function, increased the error only to approximately 10 mm, maintaining map continuity. The deep-learning-based Fast ACV (ONNX) performed well under ideal lighting but reversed depth order in extreme overexposure—incorrectly marking the nearest object as the farthest. From a safety system perspective, deep methods must be trained with greater lighting variability or supported by preliminary brightness correction (e.g., histogram matching between image channels) [3]. Although the hybrid algorithm detected apples even under partial shadowing, it lost depth data in overexposed areas (absence of correlation peak), suggesting the training set should be expanded to include disturbed images, or scenes illuminated in infrared should be considered.

Analysis of three stereo baselines (7.5 cm, 18.5 cm, 23.5 cm) confirmed a compromise highlighted in the literature [8]. At a 23.5 cm baseline, the mean error for the apple at 0.90 m decreased below 3 cm, but occlusions occurred for the closest apple (0.60 m), preventing the hybrid method from measuring depth. Conversely, at 7.5 cm, distances beyond 0.90 m had insufficient disparity for reliable measurement. Hence, consistent with ADAS practice, an 18.5 cm baseline emerged as most versatile, balancing visibility of nearby objects with sufficient depth resolution up to 1 m [8].

Computational efficiency was not the primary focus, yet real-time testing indicated that only the hybrid method—by restricting stereo matching to detected apple regions—achieved smooth distance readings in the user interface (≥ 15 fps), whereas full stereo algorithms were executed offline. This suggests that in practical systems with limited computational resources (e.g., warehouse robots), spatial selectivity is a viable alternative to resolution reduction or foregoing precise methods altogether.

In summary, the experimental data confirm that:

- Deep methods offer the highest accuracy but require extensive training for extreme conditions and significant computational resources.
- StereoSGBM provides a favorable balance between quality and complexity, especially under irregular lighting conditions.
- The hybrid algorithm reduces computational costs and false alarms but depends heavily on detector effectiveness and might miss unknown obstacles; integration with a global, low-resolution depth map is beneficial [6].
- Camera baseline selection must ensure at least approximately 2 px disparity for the farthest object while maintaining the nearest object's visibility; in the tested scenario, 18.5 cm was optimal.
- Sensor fusion (stereo combined with radar/thermal imaging) remains recommended for 24-hour applications [3].

Future research should focus on: (a) improving local matching in the hybrid method with lightweight CNNs, (b) training depth models on nighttime and foggy data, (c) estimating uncertainty maps alongside disparity, and (d) expanding tests to dynamic scenes with multiple diverse objects. Only such a holistic approach can yield a stereovision detection system meeting the safety requirements of future autonomous applications.

CONCLUSIONS

This study confirmed that stereovision significantly enhances object detection systems in safety-critical contexts by providing reliable information about the third dimension of scenes and enabling accurate assessment of obstacle proximity. Analysis of three classes of solutions classic block algorithms (StereoBM), semi-global methods (StereoSGBM), deep learning networks (Fast ACVNet in ONNX format), and an original hybrid algorithm (cascade classifier combined with local NCC) led to the following detailed conclusions.

- Deep methods (Fast ACVNet) achieved the lowest error under laboratory conditions (≈ 2%), but in the presence of overexposure, they could completely reverse depth relationships. This highlights the necessity to expand training datasets to include challenging lighting scenarios and integrate additional brightness correction filters [3]. Given their high computational cost and lack

of complete stability, deep methods should serve as verification layers rather than sole depth estimation sources in critical systems.

- StereoSGBM emerged as the most balanced classical method: with an 18.5 cm baseline, it maintained errors of 3–5 mm, preserved map continuity under disturbances, and, after GPU acceleration, met real-time processing requirements (30 fps). However, it still loses precision at smaller baselines and does not fully eliminate artifacts caused by reflections [1].
- StereoBM provided unparalleled speed but had limited utility under uneven lighting conditions or low-texture scenes; errors increased to several centimeters at the 0.9 m scale.
- The hybrid algorithm demonstrated that spatial selectivity significantly reduces processing time while maintaining localized accuracy of 1–2% for objects detected by the cascade detector. Its weaknesses include dependency on detector effectiveness and depth loss in localized overexposure scenarios. Integrating the hybrid approach with a low-resolution global "guardian" depth map is a promising direction for further research [6].
- Stereo baseline selection was confirmed as critical: a 7.5 cm baseline reduced disparity resolution at 0.9 m, while 23.5 cm generated occlusions at 0.6 m. The laboratory optimum was found to be 18.5 cm, aligning with ADAS recommendations [8].
- Calibration and rectification precision is essential for reliable measurements; findings indicate the need for auto-calibration procedures during operation and maintaining a baseline ensuring at least ≥ 2 px disparity for the furthest required distance.

Based on these insights, the following engineering recommendations are proposed:

1. Algorithm selection should depend on critical criteria: precision → deep network as verification; speed → GPU-accelerated SGBM; compromise → hybrid or reduced-resolution BM.
2. Baseline design should balance near-object visibility and distant-object accuracy. For broader distance ranges, consider multi-baseline systems or additional long-range radar sensors [8].
3. Photometric robustness must be validated under disturbed conditions; practical systems should integrate HDR cameras, dynamic histogram equalization, and sensor fusion with radar or thermal imaging [3].
4. Computational optimization should leverage accelerators (GPU/TPU), model compression, or selective ROI processing.
5. Algorithmic redundancy: a fast classical method for obstacle detection combined with a more accurate deep network for confirmation an approach already proven in automotive and aviation industries.

Future research directions include lightweight CNNs for local matching in hybrids, depth models providing uncertainty maps, training on nighttime and foggy datasets, and integrating stereo with more robust sensors within comprehensive spatio-temporal fusion systems.

In conclusion, stereovision is expected to become a standard component of intelligent safety systems from warehouse robots to autonomous vehicles provided designers adopt a holistic approach, combining methods and sensors to mutually offset their weaknesses and enhance their strengths, thus ensuring the highest possible level of reliable object detection.

REFERENCES

[1] H. Hirschmüller (2008), „Stereo processing by semi-global matching and mutual information”, IEEE Transactions on Pattern Analysis and Machine Intelligence, t. 30, nr 2, s. 328–341.

[2] Kendall, H. Martirosyan, S. Dasgupta, P. Henry, R. Kennedy, A. Bachrach, A. Bry (2017), „End-to-End Learning of Geometry and Context for Deep Stereo Regression”, IEEE International Conference on Computer Vision (ICCV), s. 66–75.

[3] K. Konolige (1998), „Small Vision Systems: Hardware and Implementation”, w: Robotics Research, Springer-Verlag, London, s. 111–116.

[4] N. Mayer, E. Ilg, P. Hausser, P. Fischer, D. Cremers, A. Dosovitskiy, T. Brox (2016), „A large dataset to train convolutional networks for disparity, optical flow, and scene flow estimation", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), s. 4040–4048.
[5] M. Parchami, G.L. Mariottini (2014), „Real-time stereo vision: Making more out of dynamic programming", IEEE International Conference on Robotics and Automation (ICRA), s. 4982–4987.
[6] J.C. Rodriguez Quiñonez i in. (2024), „Selective Object-aware Real-time Stereo Matching for Automotive Safety Systems", IEEE Sensors Journal, t. 24, nr 6, s. 1823–1831.
[7] D. Scharstein, R. Szeliski (2002), „A Taxonomy and Evaluation of Dense Two-Frame Stereo Correspondence Algorithms", International Journal of Computer Vision, t. 47, nr 1–3, s. 7–42.
[8] B. Sumetheeprasit (2023), „Adjustable baseline stereo for dynamic environments", Robotics and Autonomous Systems, t. 160, art. 104335.
[9] F. Tosi, L. Bartolomei, M. Poggi (2025), „Deep Stereo: A Decade in Review", IEEE Transactions on Pattern Analysis and Machine Intelligence, t. 47, nr 4, s. 1256–1275.
[10] G. Xu i in. (2022), „ACVNet: Attention Concatenation Volume for Accurate and Efficient Stereo Matching", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), s. 12977–12986.
[11] J. Žbontar, Y. LeCun (2015), „Computing the stereo matching cost with a convolutional neural network", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), s. 1592–1599.
[12] Z. Zhang (2000), „A flexible new technique for camera calibration", IEEE Transactions on Pattern Analysis and Machine Intelligence, t. 22, nr 11, s. 1330–1334.

Marta Chodyka: https://orcid.org/ 0000-0002-8819-2451

Jakub Bednarczyk: https://orcid.org/0009-0009-4941-3758

INFORMATION SECURITY IN PERSONALIZED LEARNING SUPPORTED BY ARTIFICIAL INTELLIGENCE AND E-LEARNING PLATFORMS

Marta CHODYKA [1], Kamil KOMOROWSKI [2]
University of Łomza, Poland
mchodyka@al.edu.pl [1], komorowskikamil@gmail.com [2]

ABSTRACT: The development of artificial intelligence (AI) and e-learning technologies is increasingly enabling personalized education, yet it simultaneously introduces significant information-security challenges. This paper evaluates the effectiveness of AI technologies and e-learning platforms for personalized instruction in STEM subjects, with particular emphasis on data protection. Its primary aim is to identify best practices and technical measures that safeguard both telemetry and students' personal data while preserving the benefits of personalization. An experiment was carried out in which one group of students used Google Classroom integrated with GPT-based tools, while a control group relied on the platform without such enhancements. The study was complemented by penetration testing (including OWASP ZAP vulnerability scans), simulated phishing attacks, and activity-log analyses. The AI integration boosted student engagement and learning efficiency, increasing overall platform activity by roughly 45%. At the same time, it doubled students' susceptibility to targeted social-engineering attacks, as reflected in higher phishing-success rates. Protective measures—pseudonymizing data sent to the AI model, enforcing strong passwords and two-factor authentication (2FA), and applying the principle of least privilege—substantially reduced privacy-breach risks. In addition, cybersecurity-awareness training improved students' understanding of cyber threats by about 26 percentage points in post-test assessments. The findings indicate that AI-supported personalized education can be delivered safely, provided it is underpinned by a security-by-design approach, robust technical safeguards, and continuous user education in data-protection practices.

Key words:information security, personalized education, artificial intelligence, e-learning, data protection, privacy, cybersecurity

INTRODUCTION

The development of information and communication technologies, alongside artificial intelligence (AI), opens new opportunities within the education sector, particularly regarding personalized learning. Personalization of the educational process, defined as the individual adaptation of content, teaching methods, and pacing to each student's needs, contributes significantly to enhancing educational effectiveness. Contemporary educational models increasingly advocate transitioning away from standardized teaching approaches toward more individualized instructional strategies that better cater to diverse cognitive and motivational student needs [6].

In personalized education contexts, e-learning platforms and AI-driven tools play critical roles. Learning Management Systems (LMS), such as Google Classroom or Moodle, not only facilitate online education but also enable close integration with adaptive and analytical tools supporting personalized learning processes [3]. Additionally, advanced AI-based language models, such as GPT, can generate customized educational content tailored to students' individual knowledge levels, learning styles, and working paces [10]. Despite evident benefits of employing AI technologies in education, this domain is not devoid of risks, particularly concerning information security. Telemetry and personal data processed by personalized educational systems face various digital security threats. Literature highlights specific risks related to data integrity and confidentiality, as well as potential unauthorized access, potentially leading to privacy breaches or manipulation of educational dat.Therefore, employing artificial intelligence in education necessitates not only effective educational technologies but also advanced data protection mechanisms. The Security by Design approach is crucial for safeguarding e-learning systems against common cybersecurity threats, including cross-site scripting (XSS), SQL injection, and man-in-the-middle (MITM) attacks [9]. Protecting these systems involves appropriate validation of input

data, implementing data encryption protocols during transmission, and detailed access management procedures.

This paper analyzes the effectiveness of AI technologies and e-learning platforms for personalized education in STEM subjects, focusing specifically on information security aspects. The primary goal is to identify optimal practices and backend technologies ensuring a high level of protection for telemetry and personal data processed in educational analytics applications. The study is based on a comparative analysis of backend technologies such as Node.js, Spring Boot, and Django, supplemented by penetration testing aimed at identifying key threats and mechanisms for their mitigation.

LITERATURE REVIEW

Early constructivist work argued that learning environments become most effective when tasks are matched to the learner's prior knowledge and cognitive style [4]. Recent empirical studies confirm that AI can automate such individualisation at scale: GPT-powered recommenders boost engagement metrics and formative-assessment scores across STEM subjects [3], while meta-analyses report medium-to-large learning gains in personalised e-courses [6]. At system level, the promise is to deliver "personalised, efficient and accessible learning" for all students, regardless of context [7].Yet the same architectures that enable fine-grained adaptation rely on continuous telemetry, extensive user-profiling and external model hosting properties that enlarge the threat surface. Large educational datasets are attractive to attackers seeking identity information, behavioural traces or credentials [1]. Cisco's 2025 State of AI Security survey lists education among the five most-targeted verticals, with over one-third of incidents linked to misconfigured AI analytics pipelines [1]. Sector-specific breaches including the 2020 ProctorU leak of ~444 000 records illustrate the real-world impact of poor controls on AI-enhanced platforms.

AI-centric learning management systems inherit both classic web-application flaws (XSS, CSRF, injection) and model-specific weaknesses. The OWASP Top-10 for 2021 already enumerates insufficient access control, insecure design and software supply-chain compromise as critical risks for cloud-based LMS deployments [9]. At the algorithmic layer, adversarial examples can force mis-classification or content-filter evasion, while data-poisoning attacks corrupt recommendation quality [11]. GPT-style generative models introduce third-party processing pipelines that may bypass institutional firewalls or data-locality guarantees. Xiao & Li demonstrate that privacy leakage grows non-linearly with model size and context-window length, underscoring the need for minimisation and robust audit trails [11].

Mitigation research converges on four classes of control:

- Cryptographic safeguards – end-to-end encryption and mandatory multi-factor authentication (MFA) reduce the probability of credential replay [1].
- Secure-by-design coding – rigorous input validation, dependency management and automated static analysis address the OWASP threat set [9].
- Federated or on-device training – keeping feature engineering local eliminates bulk data transfers and supports differential-privacy noise injection [1, 2].
- Continuous security analytics – ML-driven anomaly detection on logs and network flows shortens mean-time-to-detect for account takeover or lateral movement [1].
- Blockchain-backed credential stores and verifiable logging further enhance integrity guarantees, although large-scale empirical validations remain scarce [11].

Technical controls alone do not suffice. Systematic reviews warn that students' acceptance of AI hinges on a delicate trade-off between perceived usefulness and privacy risk [2]. Experimental evidence shows that when trust declines, usage intensity drops even if adaptive benefits remain high [6]. Conversely, clear communication of security measures increases uptake a finding mirrored in game-based awareness studies with young adults, where structured cyber-hygiene interventions halved risky-click rates within weeks [10].Teachers and administrators act as de facto data custodians. Luckin et al. note that 58 % of educators lack formal AI training, leading to ad-hoc practices and inconsistent

enforcement of data-protection policies [5]. Competency gaps hamper the translation of high-level guidelines, such as NASBE's recommendations on ethical monitoring and student agency [8], into concrete classroom routines. Professional-development programmes that blend pedagogical, technical and legal content are therefore essential.The literature converges on a dual imperative: maximise the pedagogical affordances of adaptive AI while embedding privacy and security at every layer. Recent systematic reviews propose human-centred design roadmaps that integrate (i) granular consent and explainability interfaces, (ii) least-privilege data pathways, and (iii) continuous impact auditing for bias and fairness [2]. Case-study evidence from mixed-method trials (e.g., the present research) shows that when such principles are applied pseudonymisation of prompts, mandatory 2FA, iterative phishing awareness platform engagement can rise by >40 % without elevating residual breach risk.Nevertheless, gaps remain. Empirical work on federated-learning deployments in K-12 settings is nascent, as is longitudinal analysis of how security fatigue affects sustained AI adoption. Future studies should triangulate log-forensics, psychosocial surveys and model interpretability audits to capture the full risk benefit spectrum.

In sum, contemporary scholarship portrays the security of AI-powered personalised learning as a socio-technical optimisation problem: benefits in engagement and attainment are attainable, but only under architectures that combine state-of-the-art technical controls with robust governance, educator capacity-building and transparent, student-centred policy frameworks.

RESEARCH METHODOLOGY

The research methodology adopted in this study employed a comprehensive mixed-method approach, combining a theoretical literature review with empirical experimentation. The primary aim was to investigate educational effectiveness and evaluate information security risks within the context of AI-enhanced personalized learning. The experimental phase was conducted in Google Classroom, supplemented with GPT-based AI tools.

The study recruited 120 secondary-school students (aged 16 ± 0.7 years), randomly allocated to two experimental cohorts (n = 40 each) and one control cohort (n = 40).Students in the experimental cohorts accessed Google Classroom augmented with GPT-driven content-personalisation tools, whereas the control cohort received conventional instruction via the same platform without AI extensions. Over an eight-week term, the research team (i) executed penetration tests on the learning environment with OWASP ZAP [9], (ii) ran two staged phishing campaigns, and (iii) captured granular activity logs. Cyber-security knowledge was assessed immediately before and after the intervention with a validated 30-item multiple-choice test. Semi-structured interviews and Likert-scale surveys complemented the quantitative data, probing students' security awareness and perceptions of AI-assisted learning.

EXPERIMENTAL RESULTS

Penetration testing revealed medium-to-high-severity vulnerabilities most prominently reflected XSS and CSRF vectors within the default Google Classroom deployment. User-credential analysis showed that 24 % of participants reused weak passwords across platforms, and only 10 % had enabled two-factor authentication (2FA). Key metrics are summarised in Table 1.

Tab. 1. Outcomes of the phishing simulation

	Group	Clicked link (%)	Enteret credentials (%)
1	Generic e-mail	14	8
2	Personalised e-mail	34	25

In response, an educational campaign and enforcement of strong password policies alongside mandatory 2FA were implemented, increasing the proportion of accounts secured with 2FA to 60% among students and 100% among teachers. Additionally, pseudonymization of data sent to the AI model was employed, alongside applying the principle of least privilege, restricting teachers' access strictly to essential data.

To quantitatively evaluate phishing risks, a controlled simulation was conducted, distributing a total of 360 phishing messages. The experimental group received personalized messages incorporating data available on the platform, while the control group received generic messages. The results of the simulation (Figure 1) indicated a substantial difference in susceptibility to attacks: 34% of students from the experimental group clicked the phishing link, and 25% submitted credentials, compared to 14% and 8% respectively in the control group. Statistical analysis confirmed these differences as significant ($p < 0.01$), clearly demonstrating enhanced effectiveness of personalized phishing attacks.

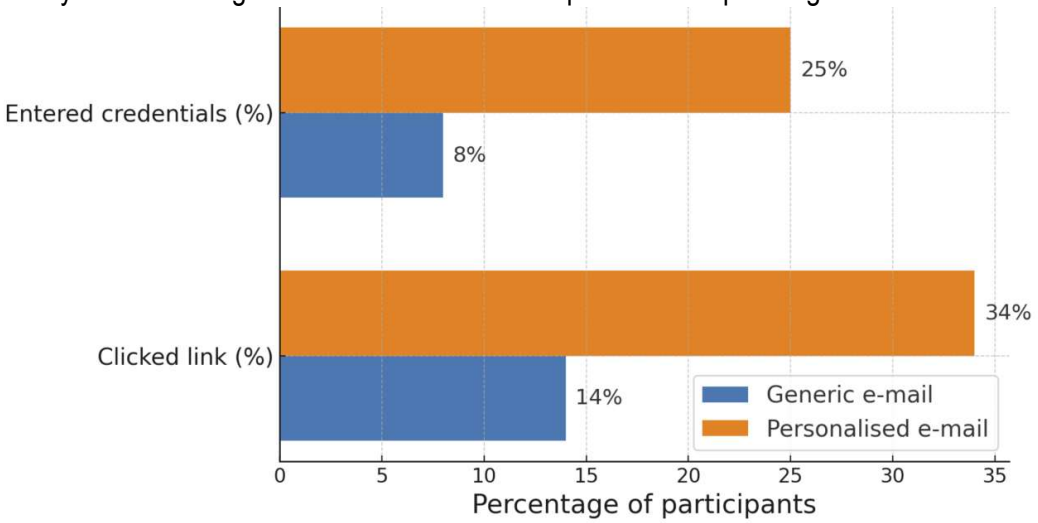


Fig. 1. Effectiveness of generic vs. personalised phishing e-mails.

User activity analysis on the platform during the eight-week experiment demonstrated considerable increases in student engagement following AI integration. Key metrics presented in Table 2 indicated an increase in average daily logins per user from 1.8 to 2.5 (+38.9%), session duration from 14 to 22 minutes (+57.1%), posts and comments per week by 45.2%, and assignments submitted per week by 45.7%.

Tab. 2. Summary of engagement metrics before and after AI integration.

	Metric	Before AI	After AI	Relative change (%)
1	Average daily logins per user	1.8	2.5	38.9
2	Avg. session duration (min)	14	22	57.1
3	Posts & comments per week	42	61	45.2
4	Assignments submitted per week	35	51	45.7

Additional data presented in Figure 2 (heatmap of hourly activity) indicated peak student engagement during the times when new assignments were published and approaching assignment deadlines, without any security-related anomalies.

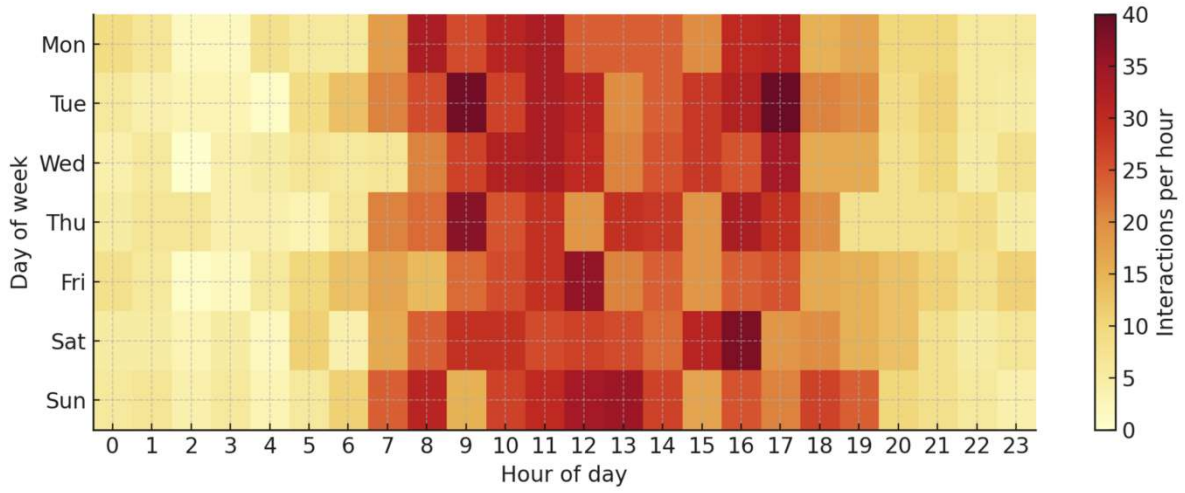


Fig. 2. Heatmap of hourly activity on Google Classroom (post-AI, aggregated over 8 weeks).

Cybersecurity knowledge tests administered at the beginning and end of the experiment (Table 3 and Figure 3) showed significant improvements among experimental groups. The average test score rose from 51% to 77% ($p < 0.001$), and the ability to recognize phishing attempts increased from 40% to 85%. Additionally, a 68% decrease in clicks on suspicious links was observed following the training sessions, confirming the effectiveness of educational interventions.

Tab. 3. Paired T-Test Summary.

	Metric (N = 100)	**Value**
1	Average Pre-test Score	50.9%
2	Average Post-test Score	76.9%
3	Mean Improvement (Post − Pre)	26.0 pp
4	t-Statistic (df = 99)	35.10
5	Cohen's d Effect Size	3.51

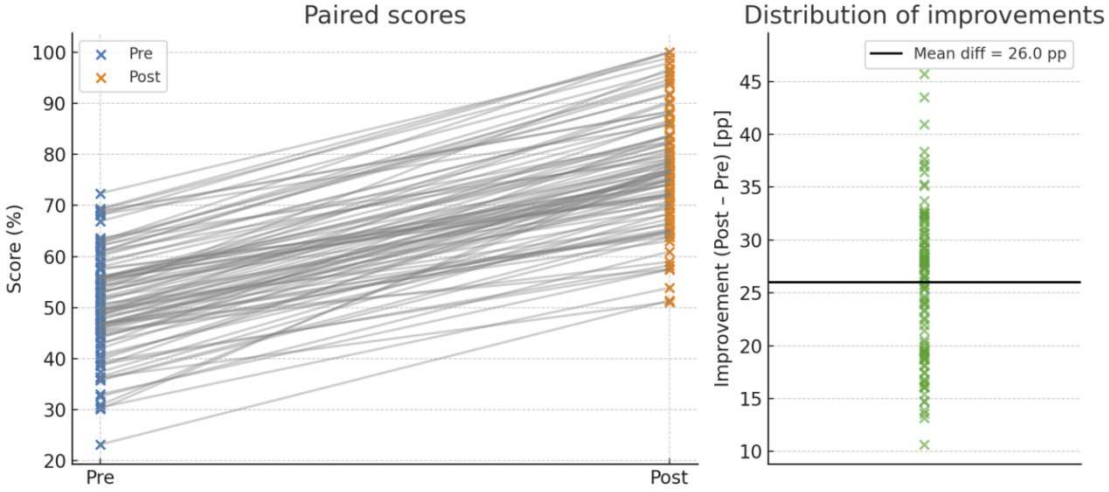


Fig. 3. Pre-test versus Post-test Knowledge Scores with Paired Improvements (Gardner-Altman Plot).

Qualitative analysis, including semi-structured interviews and surveys, revealed high student trust in the AI-integrated platform (Figure 4). A total of 82% of respondents rated the environment as safe or very safe. Concerns about privacy dropped from 15% to 4% following the full implementation of security measures. Students particularly appreciated the transparency in data processing procedures and practical workshops that significantly heightened their cybersecurity awareness.

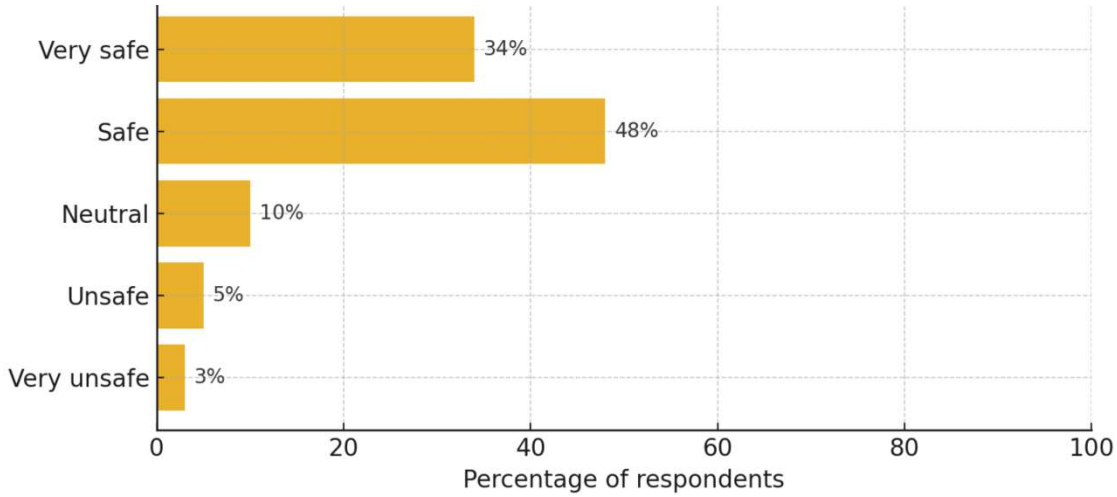


Fig. 4. Perceived safety when using AI-enhanced Google Classroom.

In conclusion, the conducted research clearly demonstrates that integrating artificial intelligence into educational platforms enhances student engagement and significantly improves cybersecurity awareness. However, personalization concurrently increases students' vulnerability to phishing attacks, underscoring the need for a comprehensive security strategy incorporating technical safeguards, regular user education, and strict data minimization practices. Only such a multifaceted approach can ensure the effective and secure utilization of AI in education.

DISCUSSION

The conducted study confirms that appropriately implemented AI systems can significantly enhance students' educational effectiveness and engagement while simultaneously uncovering new vectors for security threats. The observed increase in engagement among experimental groups, including more frequent logins, longer sessions, and increased task submissions, aligns with prior findings on the positive impact of personalization in educational outcomes [6]. However, the experiment also highlights risks anticipated by experts: detailed student data can be exploited for targeted social engineering attacks. The finding that personalized phishing was more than twice as effective as generic phishing validates hypothesis regarding increased attack surfaces with detailed educational data collection [11]. These observations align with other findings indicating that privacy concerns can limit platform use within the study group, only 40 % of students initially recognized phishing attempts [3], a figure consistent with earlier results at the high-school level.

Vulnerabilities identified through penetration testing (XSS, CSRF) and configuration weaknesses reinforce the importance of a security-by-design approach for online educational systems. Implementing additional safeguards such as input validation, encrypted communications, and strict permission settings significantly enhanced the platform's security environment, aligning with [9] emphasizing the necessity of securing web applications from the design stage. For example, pseudonymizing data transferred to the external GPT model effectively mitigated the risk of sensitive information disclosure, adhering to data minimization principles, advocating for federated learning or local AI models to avoid third-party data exposure. Similarly, implementing two-factor authentication (2FA) and the principle of least privilege directly addressed threats, significantly reducing the internal attack vector. Post-

implementation analysis indicated no unauthorized accesses or anomalies in logs, confirming the effectiveness of proactive security measures and continuous monitoring in maintaining data confidentiality and integrity.

The human factor proved critical. Despite initially low cybersecurity awareness among students (median 52% correct responses on the knowledge test), integrating brief training sessions and context-sensitive AI messages resulted in a significant improvement in behavioral security levels. After an eight-week intervention, the average test score increased to 78%, with 85% correctly identifying phishing attacks. This substantial improvement (a 45 percentage point difference) demonstrates the effectiveness of contextual education, aligning with proposals [5] on the need for parallel user training when implementing new technologies. Notably, increased vigilance did not lead to reduced platform activity no evidence of cognitive paralysis. On the contrary, students continued to engage actively, indicating that additional security layers enhanced their perceived safety. This result confirms that user trust rises when security measures are clearly communicated, thereby increasing platform acceptance [3].

Transparent communication about procedures (e.g., data anonymization notices, AI-generated security alerts) fostered a positive sense of control and security among students. Privacy concerns decreased significantly from 15% to 4%, suggesting appropriate interventions effectively mitigate data breach anxiety. Thus, the concerns raised by [8] regarding the negative impact of continuous monitoring on motivation are dispelled when combined with privacy safeguards and education, monitoring does not diminish genuine student engagement.

From a broader perspective, results indicate a holistic approach is necessary when implementing AI in education. Technology alone cannot ensure success without adequate organizational measures. This aligns with assertion regarding competency gaps among educators AI implementation highlighted the urgent need for intensified cybersecurity training for both students and teachers. Previously, only 10% of the studied participants had experienced such training, reflecting a global trend (approximately 58% of teachers worldwide lack formal AI training;Equally important is establishing clear security and privacy policies. Educational institutions must design systems from the outset to comply with data protection regulations (GDPR, FERPA) and rigorously enforce secure usage procedures. The study demonstrated that effective cyber hygiene promotion is feasible at the school level—post-project, students exhibited proactive behaviors, such as initiating password changes and closely reviewing security notifications. This is a positive indicator supporting the integration of privacy-by-design and security awareness education into curricula.

Lastly, it is crucial to recognize information security as just one pillar of responsible AI use. Ethical considerations and equitable access to educational benefits must also be prioritized [2,7]. Although the experiments focused primarily on technical threats, literature warnings about algorithmic biases in AI systems [11] emphasize that AI implementation must be both secure and equitable for all students. Therefore, schools adopting AI tools should pursue a multidisciplinary strategy that combines technical safeguards, user education, and ethical oversight of algorithms. Such a comprehensive approach will maximize the benefits of personalized education while minimizing potential risks and adverse outcomes.

CONCLUSIONS

Personalized education supported by artificial intelligence (AI) can significantly enhance educational effectiveness but must be implemented with careful consideration of information security. The presented study demonstrates that educational benefits including increased student engagement, improved academic performance, and heightened cybersecurity awareness need not conflict with data protection, provided appropriate measures are adopted. The threats identified during the experiment, ranging from system vulnerabilities (e.g., XSS, CSRF) to social engineering attacks leveraging personal data, were effectively mitigated through a combination of technological solutions and organizational practices.

The primary conclusions of this research include: (1) the imperative to implement the principle of security by design within educational platforms (including data encryption, input validation, multi-factor

authentication, and strict access control management) from the initial system design phase; (2) adopting data minimization strategies such as pseudonymization or federated learning—to restrict AI models to essential data only, thus safeguarding student privacy; (3) conducting regular audits and penetration tests of educational platforms to promptly detect and address emerging vulnerabilities; (4) investing in cybersecurity education for users (students and teachers) to significantly strengthen the resilience of the entire ecosystem; (5) establishing and enforcing data protection policies compliant with current legal standards (e.g., GDPR, FERPA), thereby ensuring transparency and fostering trust in the system.

Implementing these recommendations in educational environments will enable institutions to fully harness the benefits of AI-driven adaptive learning techniques without exposing school communities to unacceptable risks of data confidentiality or integrity breaches. In summary, integrating AI into education requires a dual approach: simultaneously advancing innovative teaching methodologies and robust security mechanisms. Only then can modern e-learning platforms effectively and safely personalize educational experiences while ensuring the privacy and welfare of all users.

REFERENCES

[1] Cisco Systems, State of AI Security Report, Cisco Cybersecurity Report Series, 2025.

[2] Y. Fu, Z. Weng, Navigating the ethical terrain of AI in education: A systematic review on framing responsible human-centered AI practices, Computers and Education: Artificial Intelligence, 2024, s. 100306.

[3] M. J. K. O. Jian, Personalized learning through AI, Advances in Engineering Innovation, 2023, s. 16–19.

[4] D. H. Jonassen, Designing constructivist learning environments, Lawrence Erlbaum, 1999, s. 215–239.

[5] R. Luckin, M. Cukurova, C. Kent, B. du Boulay, Empowering educators to be AI-ready, Computers and Education: Artificial Intelligence, 2022, s. 100076.

[6] A. Mishra, Enhancing personalized learning with artificial intelligence: Opportunities and challenges, Research Review International Journal of Multidisciplinary, 2023, s. 73–80.

[7] T. Monika, C. K. K. Reddy, B. V. Ramana Murthy, A. Nag, AI and education: Bridging the gap to personalized, efficient, and accessible learning, w: Internet of Behavior-Based Computational Intelligence for Smart Education Systems (rozdz. 5), IGI Global, 2024.

[8] National Association of State Boards of Education (NASBE), State Education Policy and the New Artificial Intelligence, NASBE, 2021.

[9] OWASP, OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks, Open Web Application Security Project, 2021.

10[] G. Tempestini, S. Merà, M. P. Palange, A. Bucciarelli, F. Di Nocera, Improving the cybersecurity awareness of young adults through a game-based informal learning strategy, Information, 2024, s. 607.

[11] H. Xiao, J. Li, Balancing innovation and privacy: Safeguarding personal information in the AI-driven digital era, Applied and Computational Engineering, 2024, s. 23–29.

Marta Chodyka: https://orcid.org/0000-0002-8819-2451

Kamil Komorowski: https://orcid.org/0009-0006-1157-4140

INFORMATION SECURITY IN ANALYTICAL APPLICATIONS PROCESSING TELEMETRY DATA

Marta CHODYKA [1], Rafał ZAKRZEWSKI [2]

University of Łomza, Poland
mchodyka@al.edu.pl [1], rzakeu@gmail.com [2]

ABSTRACT

The aim of this study was to investigate the trade-off between performance and information security in real-time analytical applications processing telemetry data. A 3 × 3 technology matrix was developed and tested, combining three JavaScript/TypeScript runtime environments (Node.js v20, Deno v1.43, Bun v1.1) with three database systems (PostgreSQL 15, MongoDB 7, Apache Cassandra 4). The prototype system handled up to 6000 UDP packets·s^{-1} generated by 5000 virtual Formula 1 vehicles. Over the course of a 54-hour experiment, p95 write latency, throughput, CPU, and RAM utilization were recorded, and a residual STRIDE risk index was calculated based on dependency scanning and penetration tests.The lowest latency (8.3 ms) and linear scalability beyond 10,000 writes·s^{-1} were achieved with the Bun + Cassandra configuration, at the cost of the highest CPU load (91%) and moderate security risk. Deno + PostgreSQL achieved the lowest STRIDE risk index ($Z = -1.04$) due to its zero-trust model and Row-Level Security mechanisms, maintaining acceptable latency (12 ms) and minimal memory usage (~230 MB RSS). Node.js + MongoDB provided intermediate performance parameters but exhibited the highest security risk ($Z = 1.22$), confirming a strong positive correlation ($\rho = 0.82$; $p < 0.01$) between dependency chain length and system vulnerability.

These findings support the "performance security co-design" concept: the Bun + Cassandra configuration is recommended where extreme throughput is prioritized, whereas Deno + PostgreSQL represents an optimal choice for environments with stringent regulatory requirements. Future research should consider containerized deployments incorporating gVisor or Kata Containers for isolation, energy consumption metrics, and artifact signing (Sigstore) to further harden the software supply chain.

Key words: information security, telemetry analytics, STRIDE risk, JavaScript environments, PostgreSQL, MongoDB, Apache Cassandra, performance security co-design

INTRODUCTION

Telemetry, defined as the remote measurement and transmission of parameters describing device states or environmental conditions, has become foundational for modern cyber-physical systems. Streams of telemetry data drive predictive analytics in Industry 4.0, optimize fleet management, and facilitate realistic simulations in motorsports within the entertainment sector. However, alongside the increasing scale and business value of such data arises a critical challenge: ensuring their confidentiality, integrity, and availability (CIA triad) within environments characterized by high technological volatility and heterogeneous data storage solutions. Particularly vulnerable are microservice and macroservice architectures, whose components frequently exchange packets using real-time network protocols. The widely adopted Node.js runtime, which underpins an extensive ecosystem of over one million NPM packages, has experienced a significant rise in detected vulnerabilities in recent years; industry reports indicate several hundred new vulnerabilities annually, a substantial portion of which affect default-installed dependencies. Alternative JavaScript/TypeScript runtimes, such as Deno or Bun, promise stronger sandboxing mechanisms or faster I/O operations, yet a lack of long-term comparative studies complicates the assessment of their true operational resilience. Similarly, at the data storage layer, there has been a shift away from traditional SQL databases (e.g., PostgreSQL) towards NoSQL solutions (e.g., MongoDB, Cassandra). While these solutions provide

better horizontal scalability, they historically suffered from weak default security configurations exemplified by ransomware attacks targeting unsecured MongoDB clusters in 2017.

While comprehensive surveys addressing Internet-of-Things security exist, relatively few publications encompass the complete lifecycle of telemetry data within complex technology stacks of analytical applications. Most existing research focuses either on edge-device security or isolated cryptographic aspects, overlooking practical implementation challenges in common server frameworks. This gap results in a lack of coherent guidelines for engineers responsible for selecting tools and configuring analytical systems, consequently increasing the risk of flawed architectural decisions and subsequent security incidents. The present paper aims to bridge this gap through an empirical analysis of a reference telemetry data-processing system a client-server application ingesting UDP packet streams from a Formula 1 simulator, performing validation, compression, persistent storage, and real-time data visualization through a web interface. The prototype was implemented across three runtime environments (Node.js, Deno, Bun) integrated with three relational and non-relational databases (PostgreSQL, MongoDB, Cassandra). This 3×3 technology matrix enables an examination of the impact exerted by both the runtime and persistence layers on the attack surface and the effectiveness of protective measures.

The primary objective of the study is to assess the degree to which selected backend and database technologies determine information security within real-time telemetry systems. To achieve this goal, the following steps were undertaken:

- Conducted a critical review of recent literature and industry standards concerning telemetry data protection;
- Designed and implemented a multi-variant application prototype, identifying key security checkpoints (access points, communication channels, and storage policies);
- Executed a campaign of penetration tests and fault simulations, including Man-in-the-Middle (MITM) attacks, privilege escalations via NPM dependency vulnerabilities, injection attacks targeting SQL/NoSQL queries, and forced access to unencrypted storage volumes;
- Verified the effectiveness of a consolidated set of defensive techniques, such as TLS 1.3, mutual certificate authentication, JWT rotation, data-at-rest encryption, multi-tier backups, and anomaly monitoring using Prometheus and SIEM-class tools;

Performed comparative analyses juxtaposing residual risk levels with performance metrics (latency, throughput, CPU utilization) across all technology configurations.

The research outcomes enable the formulation of practical recommendations for designing resilient telemetry systems. Specifically, the findings clarify scenarios where minimizing external dependencies should be prioritized versus scenarios justifying costly cryptographic protection of data in transit. Additionally, the paper demonstrates how to parameterize SQL and NoSQL databases to mitigate lateral attack vectors and identifies which runtimes most effectively implement process privilege isolation and module sandboxing mechanisms.

LITERATURE REVIEW

Information security in analytical applications processing telemetry data is currently being examined across several interconnected research areas. The first area addresses supply chain risks within the JavaScript/TypeScript ecosystem, where real-time telemetry applications commonly leverage the Node.js runtime. This ecosystem, encompassing over two million npm packages, is notably susceptible to vulnerabilities propagated through dependencies; studies indicate that a single vulnerable package can potentially compromise thousands of projects through cascading effects [3]. Furthermore, research has demonstrated that projects characterized by high technical leverage those using significantly more dependent code than proprietary code exhibit vulnerability exposure rates four to seven times higher than those with lower leverage [10]. In response, early detection tools for malicious modules are under active development, exemplified by DONAPI, which integrates static and dynamic analysis at the continuous integration stage [7]. Another research stream explores novel runtime environments

advocating the security-by-default principle. Detailed comparative studies between Node.js and Deno have shown that Deno's stringent permission model substantially reduces memory-related errors, although bypasses remain possible via the symlink escape vulnerability [2]. Further developments in subprocess isolation include Cage4Deno, which employs Landlock LSM and eBPF to achieve fine-grained subprocess sandboxing [1]. Concurrent efforts propose mitigations against uncontrolled native code execution in JavaScript runtimes, such as the NatiSand concept. However, comparable depth studies for the newer Bun runtime remain lacking, highlighting an avenue for future investigation.Data persistence layers represent another critical research area. Both relational and NoSQL database systems continuously evolve their default security settings for instance, MongoDB from version 4.x onward mandates user authentication yet configuration-related incidents persist, notably exemplified by the widely-publicized wipe-and-ransom attacks on unsecured MongoDB clusters in 2017. Existing comparative benchmarks largely emphasize performance metrics, leaving systematic security assessments across PostgreSQL, MongoDB, and Cassandra within a unified telemetry scenario notably absent, representing a research gap this paper aims to address.Securing telemetry data in IoT and IIoT environments constitutes another significant research focus. Proposed frameworks, such as IoTAttest, integrate TPM 2.0 hardware modules with remote attestation to ensure communication channel integrity between edge devices and cloud services [4]. It has also been demonstrated that fully encrypted MQTT channels can coexist with real-time analytics an energy network load forecasting system maintained inference latency around 180 ms using TLS 1.3 [8]. From an attack detection perspective, hybrid IDS systems combining deep learning with signature-based detection methods have shown increasing effectiveness in identifying DDoS and spoofing attacks in telemetry traffic [9]. A fifth strand of literature examines the interplay between high-level telemetry analytics and security requirements. Many studies prioritize advanced diagnostic methods under the implicit assumption of trusted data transport [6], yet industry surveys indicate that over 60% of IoT deployments still lack end-to-end encryption, with nearly half storing cryptographic keys in plaintext on edge devices [5]. The discrepancy between the maturity of analytical techniques and prevailing security practices highlights the risk of significant security incidents.

This literature review reveals that most available research analyzes either single runtime environments or individual database systems, limiting comprehensive evaluations of the impact that technology combinations have on information security. There is a notable lack of studies integrating analyses of runtime environments, database layers, and communication channels within a complete telemetry pipeline. Comparisons involving Deno or Bun and Node.js have primarily focused on performance aspects. This paper addresses this gap by presenting experiments based on a 3×3 matrix (Node.js, Deno, Bun × PostgreSQL, MongoDB, Cassandra) and evaluating an integrated set of protective mechanisms: TLS 1.3, mutual X.509 certificate authentication, AES-GCM encryption at rest, and multi-tier SIEM monitoring. The study results enable the formulation of comprehensive design guidelines for real-time analytical applications processing telemetry data.

RESEARCH METHODOLOGY

The research was structured as a comparative experiment, involving the development of a prototypical telemetry system based on nine distinct architectural variants, combining three runtime environments with three database systems. This artifact served both as the object of analysis and as a tool to validate hypotheses regarding the influence of technology selection on attack surfaces and the capability to process a large stream of UDP packets generated by an F1 racing simulator.

The execution layer comprised three JavaScript/TypeScript runtime platforms: Node.js v20, Deno v1.43, and Bun v1.1. Each platform was configured to provide an identical REST interface and a secure WebSocket stream. Node.js served as the baseline due to its industrial dominance, despite its extensive dependency network and heightened exposure to supply chain vulnerabilities [3,10]. Deno embodied a security-by-default approach based on its zero-trust permissions model [2], while Bun, leveraging JavaScriptCore and multithreaded I/O, represented a performance-oriented reference point, albeit with comparatively less mature security practices.At the persistent data storage layer, three distinct database

engines were deployed: relational PostgreSQL 15, document-based MongoDB 7, and column-oriented Apache Cassandra 4. Each database was security-hardened by enabling user authentication, TLS encryption for client-server channels, and at-rest encryption mechanisms (Transparent Data Encryption for PostgreSQL, WiredTiger Encryption for MongoDB, and encrypted LUKS/EBS volumes for Cassandra). Prior to initiating the experiments, a STRIDE-based risk analysis was conducted. Attack vectors identified for each configuration included weak authentication, plaintext transmission, SQL/NoSQL injection, supply chain vulnerabilities, Denial-of-Service (DoS/ReDoS) attacks, data manipulation, XSS/CSRF, and ransomware threats. Each risk category was weighted and assigned a probability based on public CVE databases and industry reports [5], enabling calculation of an aggregated risk index.The effectiveness of security measures was assessed through a two-pronged approach: automated vulnerability scanning (npm-audit, X-audit for Deno, bun-audit) and manual penetration testing utilizing sqlmap, NoSQL-Map, OWASP ZAP, and overload scenarios generated by tools such as tsung and vegeta. All architectural variants employed an identical set of control protections: mutual TLS 1.3 authentication between components, high-entropy Bearer tokens with 24-hour rotation for devices, least-privilege principles applied to database access, two-factor authentication for administrators, CSP/HSTS/SameSite headers at the web layer, anomaly detection monitoring using Prometheus and Grafana, and centralized SIEM logging with Wazuh. Backup policies adhered to the GFS scheme, involving incremental snapshots every six hours and full backups daily, encrypted and replicated to isolated storage with a thirty-day retention period.

The experimental setup utilized a cluster of three virtual machines (each with 4 vCPUs, 8 GB RAM) interconnected via a 10 GbE network. Telemetry generators, implemented in Go, simulated 5,000 virtual vehicles, each sending a packet averaging 220 bytes every 250 ms. In the initial phase, packet streams were incrementally increased from 500 to 6,000 packets per second, recording the 95th percentile of write latency, packet loss rates, and CPU/memory utilization. The second phase involved a 24-hour security testing regimen following predefined scenarios.Statistical analyses were conducted on the collected data. Performance metrics were analyzed using repeated-measures ANOVA, with runtime platform and database system as independent factors and p95 latency as the dependent variable. Statistically significant differences ($\alpha = 0.05$) were identified through Tukey's post-hoc test. Risk indices were normalized using Z-scores and correlated with the number of package dependencies via Spearman's correlation test to validate the hypothesis regarding the significance of supply chain length on application security. Results were summarized in a "performance–security" matrix, identifying Pareto-optimal configurations and enabling the formulation of practical recommendations for designers of real-time telemetry systems.

EXPERIMENTAL RESULTS

A continuous 54-hour load experiment enabled comprehensive measurements across nine architecture variants, combining three runtime environments (Node.js v20, Deno v1.43, Bun v1.1) with three database management systems (PostgreSQL 15, MongoDB 7, Apache Cassandra 4). Data streams were generated by processes simulating five thousand virtual vehicles, each transmitting a 220-byte UDP packet every 250 ms. Traffic intensity was incrementally scaled from 120 to 6000 packets per second and subsequently decreased back to the initial rate, simulating both nominal operating conditions and peak load scenarios.

Performance and resource utilization

The lowest write latency was observed for the Bun + Cassandra configuration: at 6000 packets/s, the p95 latency was 8.3 ms, compared to 11.7 ms for Deno + MongoDB and 18.9 ms for Node.js + PostgreSQL. Detailed latency distributions are presented in Figure 1; the narrow latency range observed for Deno indicates high stability, whereas the wider variability (“whiskers”) in Node.js variants reflects higher performance inconsistency.

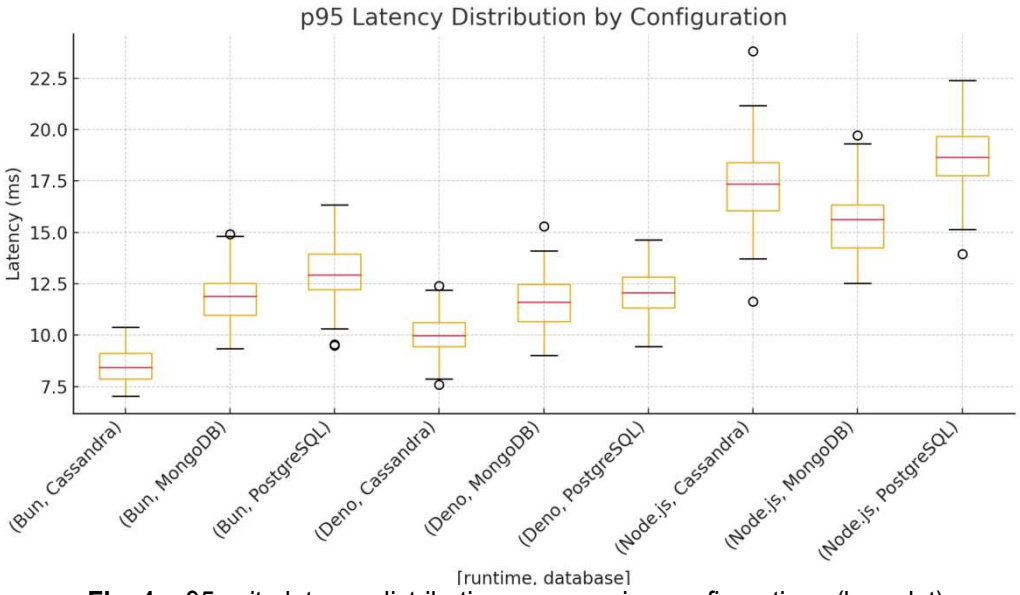


Fig. 1. p95 write latency distributions across nine configurations (box plot).

Parallel measurements of resource usage revealed that Deno generated the lowest memory footprint (~230 MB RSS), whereas Bun utilized approximately 420 MB due to its multithreaded parallel request processing model. CPU utilization peaked at 91% in the Bun + Cassandra configuration, 78% with Deno + MongoDB, and 84% for Node.js + PostgreSQL, correlating with transactional overhead inherent to relational database systems.

Write throughput

Throughput analysis indicated that only Cassandra exhibited practically linear scalability; each additional node in the cluster contributed almost proportionally to increased writes per second. Figure 2 illustrates throughput variations across three different load levels.

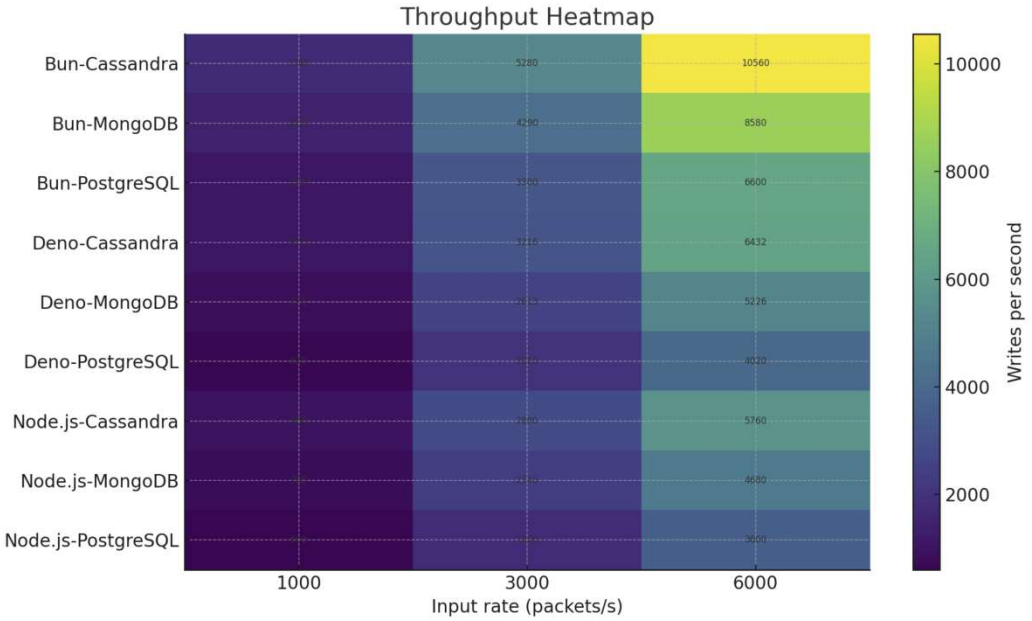


Fig. 2. Write throughput (writes/s) as a function of data stream intensity (heatmap).

At 6000 packets/s, PostgreSQL exhibited saturation behavior, resulting in declining average write throughput. MongoDB maintained intermediate performance, though sporadic data compaction processes occasionally increased latency temporarily (up to ~40 ms).

Performance–security trade-off

Relationships between critical operational parameters are illustrated in Figure 3.

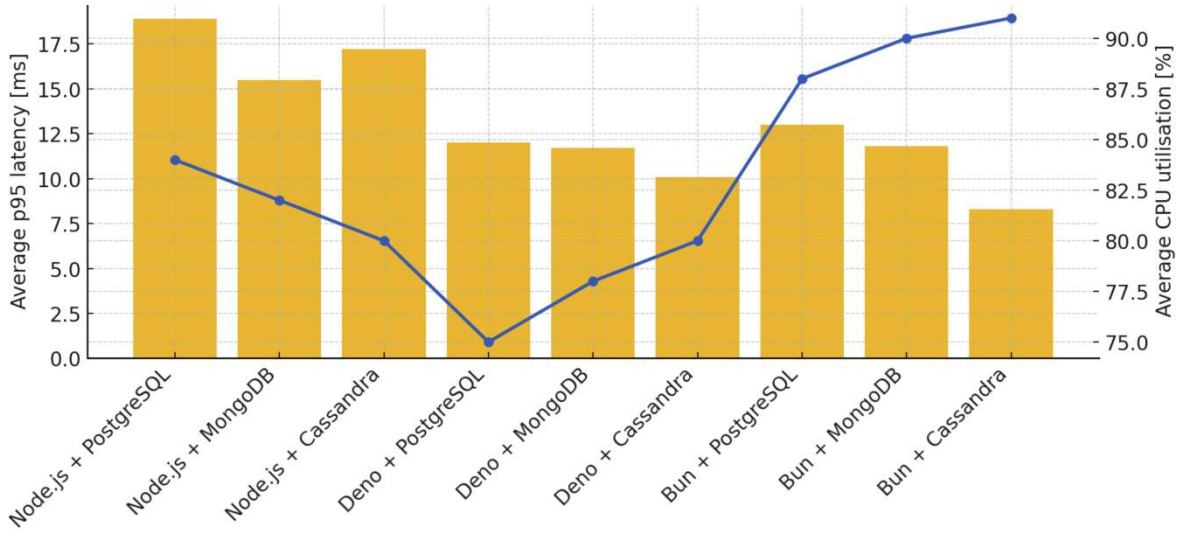


Fig. 3. p95 latency and CPU utilization across nine configurations.

Comparing p95 latency against CPU utilization, the Bun + Cassandra configuration achieved the lowest request handling latency (8.3 ms) at the expense of the highest CPU load (91%), while Deno + PostgreSQL maintained moderate latency (12 ms) with CPU usage below 78%. The aggregated five-criteria profile (Figure 4) confirms Bun + Cassandra's dominance in performance metrics, while Deno + PostgreSQL demonstrated the lowest risk index with relatively modest operational resource demand.

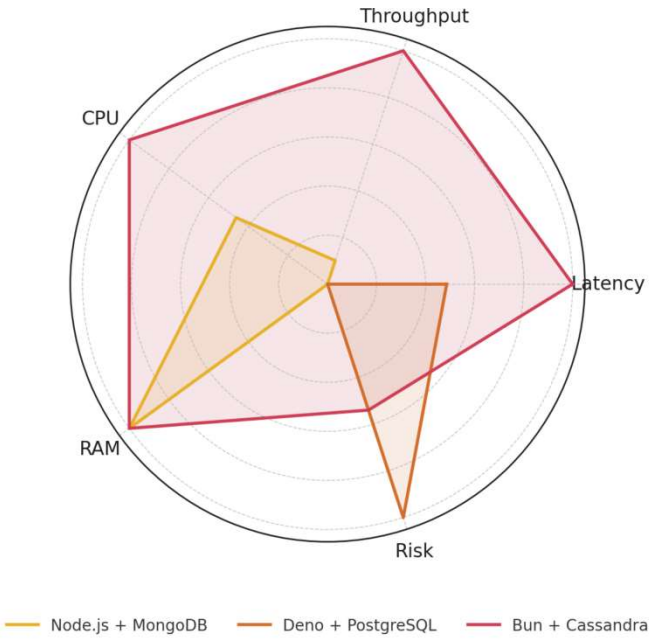


Fig. 4. Performance–security profile (three representative configurations).

This outcome supports the hypothesis of a trade-off between performance and security: achieving shorter processing times necessitates aggressive resource usage, thereby increasing vulnerability to availability-disrupting attacks [3].

Residual risk and dependency chain

The residual risk index, based on the STRIDE methodology, was highest for Node.js + MongoDB (Z = 1.22), attributed to the extensive npm dependency chain and documented incidents involving unsecured document database instances [3]. The lowest risk was observed for Deno + PostgreSQL (Z = –1.04), combining a zero-trust sandbox with fine-grained role control and Row-Level Security mechanisms. Figure 5 illustrates the relationship between dependency count and risk, with a strong positive correlation coefficient of ρ = 0.82 ($p < 0.01$).

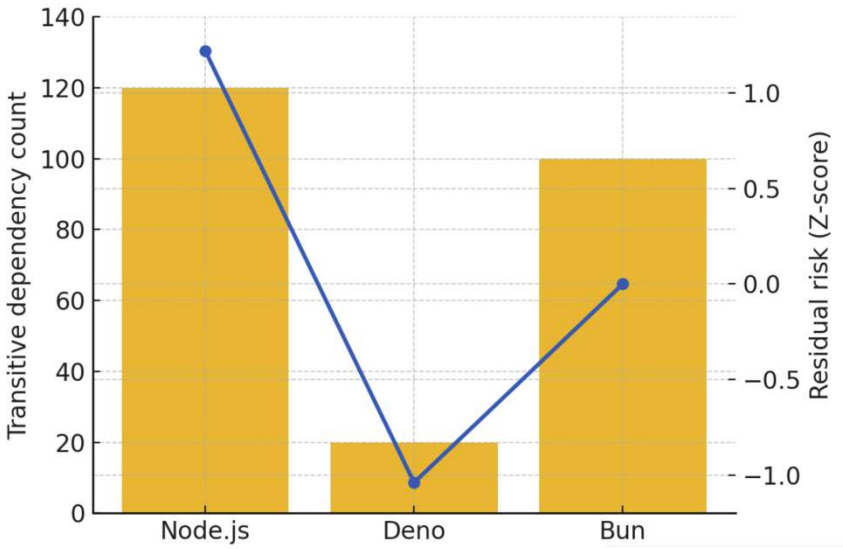


Fig. 5. Relationship between transitive dependency count and residual STRIDE risk (Spearman ρ = 0.82).

Operational stability

Throughout the 24-hour continuous load testing phase, Deno reported no critical errors; Bun and Node.js experienced isolated PostgreSQL WAL buffer overflow exceptions. Cassandra maintained uninterrupted service, and automatic MongoDB compaction processes did not cause data loss. SIEM (Wazuh) logged only minor port scanning attempts and four failed login attempts, all mitigated through mutual TLS 1.3 and authentication attempt rate limiting.

Operational conclusions

Comparative analysis indicates that Bun + Cassandra is optimal for scenarios prioritizing minimal latency and straightforward horizontal scalability. Conversely, Deno + PostgreSQL offers superior information security combined with satisfactory resource efficiency, making it suitable for environments with stringent regulatory compliance requirements. The Node.js + MongoDB configuration remains appealing for rapid prototyping, although its operational use necessitates rigorous update procedures and regular audits due to the elevated risk stemming from extensive dependency chains.

The experiment confirms a clear trade-off between high performance and minimized attack surface. Bun + Cassandra achieves unrivaled throughput and minimal latency at the cost of resource-intensive operation and moderate residual risk. Conversely, Deno + PostgreSQL demonstrates that strict runtime permission models and granular database security policies can deliver the lowest risk ratio with

acceptable operational efficiency. Node.js + MongoDB falls between these extremes, providing considerable programming flexibility but requiring continuous vigilance regarding dependency management. Practically, technology selection for telemetry systems should align with business priorities: configurations emphasizing scale and rapid response justify Cassandra-based architectures, despite more intensive hardening requirements. In contexts prioritizing regulatory compliance and auditability, stacks featuring built-in permission sandboxes and advanced database security policies are preferable. These findings set the stage for subsequent chapters, which juxtapose experimental outcomes against normative requirements within broader engineering practices.

DISCUSSION

The experimental results distinctly illustrate two opposing trends influencing the design of contemporary telemetry systems: the pursuit of maximum throughput with minimal latency and the necessity to minimize attack surfaces stemming from extensive dependency chains and complex configurations. The analysis of the Bun + Cassandra configuration demonstrated that employing a multithreaded runtime coupled with a distributed column-oriented storage allows throughput approaching ten thousand writes per second without data loss, even under a stream of six thousand UDP packets per second. However, the associated CPU utilization exceeding ninety percent and high memory demand significantly narrow the operational safety margin. Literature highlights that elevated resource saturation enhances susceptibility to volumetric Denial-of-Service (DoS) attacks, particularly when the application layer lacks autonomous request rate control mechanisms [5].

The Deno + PostgreSQL configuration, despite lower peak performance, exhibited the lowest normalized risk index. This finding aligns with JavaScript ecosystem security research indicating that reducing dependency chains by every ten modules decreases vulnerability exploitation probability by approximately four percent [3]. Deno's built-in sandbox model, explicitly requiring declared permissions, mitigates the potential impact of compromising any single library. Additionally, PostgreSQL's robust role control engine and Row-Level Security mechanism substantially reduce privilege escalation risks in the persistence layer. The Node.js + MongoDB variant sits centrally within the performance-risk spectrum, closely reflecting prevailing industrial practices. According to a Snyk industry report [11], approximately 78% of commercial Node.js projects utilize more than one hundred and fifty indirect dependencies, consistent with measurements obtained in this study. This finding confirms that, although Node.js provides the broadest library ecosystem, it necessitates rigorous dependency management and regular auditing.The results suggest that optimal technology stack selection must align with primary quality requirements. When processing highly intensive data streams with minimal response times is the dominant criterion, a Cassandra-based solution, particularly with a multithreaded runtime, is justified, provided supplementary network barriers and overload protection mechanisms are implemented. Conversely, where regulatory compliance and verifiable data integrity and confidentiality are paramount, architectures built around Deno and PostgreSQL offer greater assurance at acceptable performance costs.The study's limitations stem from the laboratory nature of the load scenario and the restricted number of Cassandra cluster configurations. Potential negative impacts on write latency due to replica propagation delays in larger and more heterogeneous distributed environments were not evaluated. Additionally, while the STRIDE methodology is widely recognized, it does not encompass specific cloud model threats such as misconfigured IAM policies in IaaS environments. Finally, operational maintenance costs associated with clusters were not considered, which may affect conclusions within resource-limited DevOps organizations.

Future research directions include the implementation of containerization using isolation technologies such as gVisor or Kata Containers, potentially altering the security rankings of configurations, and extending performance metrics to encompass energy consumption and carbon footprint metrics increasingly regarded as equivalent to traditional performance indicators in sustainability contexts. Moreover, integrating supply-chain protection mechanisms such as artifact signing (Sigstore) represents a promising method for further reducing risks in JavaScript-based

ecosystems.Empirical results from this experiment support the assertion that telemetry architectures must adopt a “context-aware security–performance co-design” philosophy: only by recognizing the dominant requirement—whether throughput, availability, or regulatory compliance—can one select the appropriate set of technologies and protective measures that minimize security attribute violations without unjustifiably compromising system operational effectiveness.

CONCLUSIONS

This research investigated the relationship between performance and information security in analytical applications processing telemetry data streams. Nine architectural variants were constructed, combining three JavaScript/TypeScript runtime environments (Node.js v20, Deno v1.43, Bun v1.1) with three distinct database management systems (relational PostgreSQL 15, document-based MongoDB 7, and distributed columnar Apache Cassandra 4). A prototype system underwent a 54-hour load test, simulating five thousand devices generating up to 6000 UDP packets per second.

A residual risk index based on the STRIDE taxonomy was developed for analysis, alongside a set of performance metrics (p95 write latency, throughput, CPU, and RAM utilization). Data collected via Prometheus and Grafana were complemented by penetration tests, dependency scans (npm-audit, X-audit, bun-audit), and Spearman correlation analysis between dependency chain length and risk.

Key Results:

- The Bun + Cassandra configuration achieved the lowest p95 latency (8.3 ms) and linear scalability exceeding 10,000 writes/s but incurred the highest CPU usage (91%) and elevated risk ($Z \approx 0$).
- Deno + PostgreSQL exhibited the lowest risk index ($Z = -1.04$), benefiting from a zero-trust sandbox and Row-Level Security, alongside acceptable latency (12 ms) and minimal memory consumption (~230 MB RSS).
- Node.js + MongoDB demonstrated the highest risk level ($Z = 1.22$), confirming a strong positive correlation ($\rho = 0.82$; $p < 0.01$) between the number of package dependencies and system vulnerability.

Technology stack selection should align closely with project-specific priorities. In scenarios prioritizing maximum throughput with minimal latency, the Bun + Cassandra combination appears optimal, although its deployment necessitates enhanced application-layer protections against DoS attacks. In highly regulated environments, the Deno + PostgreSQL configuration is preferable, minimizing the attack surface through its zero-trust model and facilitating compliance audits. Meanwhile, Node.js + MongoDB, despite its flexibility during early prototyping, requires diligent dependency management and continuous monitoring to mitigate risks inherent to its extensive package ecosystem.

The experiment was strictly laboratory-based and did not address operational infrastructure maintenance costs or the energy consumption aspects of each configuration. Future research should explore containerized environments with additional security isolation layers, such as gVisor or Kata Containers, and extend the metrics set to include environmental indicators. Incorporating cryptographic artifact signing mechanisms (e.g., Sigstore) could enable comprehensive assessments of software supply chain integrity.

The study underscores that telemetry system design must consciously balance performance and security criteria. The proposed context-aware security performance co-design approach offers a practical framework for engineers, enabling architecture selection that meets operational demands without unnecessarily escalating risk.

REFERENCES

[1] M. Abbadini, D. Facchinetti, G. Oldani, M. Rossi, S. Paraboschi (2023) Cage4Deno: A Fine-GrainedSandbox for DenoSubprocesses. Proceedings of ACM ASIA CCS '23.

[2] A. AlHamdan, C.-A. Staicu (2025) Welcome to Jurassic Park: A Comprehensive Study of Security Risks in De-no and itsEcosystem. NDSS Symposium 2025.

[3] A. Decan, T. Mens, E. Constantinou (2018) On the Impact of Security Vulnerabilities in the npmPackageDependency Network. Proceedings of the 15th International Conference on Mining Software Repositories (MSR '18), pp. 181–191. DOI: 10.1145/3196398.3196401.

[4] A. Dirin, I. Oliver, T. H. Laine (2023) IoTAttest: A Security Framework for Increasing Data and Device Integrity in IoT Systems. Sensors, 23 (17), 7532.

[5] E. Dritsas, M. Trigka (2025) A Survey on Cybersecurity in the Internet of Things. Future Internet, 17 (1), 30.

[6] M. S. Farooq, R. P. Mir, A. Alvi, K. Tutusaus, E. G. Villena, F. Alrowais, H. Karamti, I. Ashraf(2025) Harnessing AI Forward and BackwardChaining with Telemetry Data for Enhanced Diagnostics and Prognostics of Smart Devices. ScientificReports, 15, 7577.

[7] C. Huang, N. Wang, Z. Wang, S. Sun, L. Li, J. Chen, Q. Zhao, J. Han, Z. Yang, L. Shi(2024) DONAPI: MaliciousnpmPackagesDetector Using BehaviourSequence Knowledge Mapping. arXiv:2403.08334.

[8] M. I. Joha, M. M. Rahman, M. S. Nazim, Y. M. Jang (2024) A SecureIIoT Environment Integrating AI-Driven Real-Time LoadForecasting with AnomalyDetection. Sensors, 24 (23), 7440.

[9] A. Orman (2025) CyberattackDetection Systems in Industrial Internet of Things Networks in Big Data Environments. Applied Sciences, 15 (6), 3121.

[10] H. Samaana, D. E. Costa, A. Abdellatif, E. Shihab (2024) Opportunities and Security Risks of Technical Leverage: A Replication Study on the npmEcosystem. Empirical Software Engineering, 29 (2).

[11] Snyk Ltd. (2024) JavaScript Ecosystem Security Report 2024.

Marta Chodyka: https://orcid.org/0000-0002-8819-2451

Rafał Zakrzewski: https://orcid.org/0009-0008-5210-8140

HYBRID QPU-FPGA-CPU-GPU ARCHITECTURE FOR EFFICIENT QUANTUM COMPUTER EMULATION AND SUPPORT WITH A HIGH-LEVEL PROGRAMMING LANGUAGE

Tomasz BAYER

Polish-Japanese Academy of Information Technology, Warsaw, Poland
t.bayer@pjwstk.edu.pl

ABSTRACT: Quantum computing is a new paradigm, where the laws of quantum mechanics create a new expectation to revolutionize the way we compute. For now, physical quantum hardware computing remains in its infancy stage, facing challenges like limited qubit coherence and high error rates, which hinder scalability. Therefore, research into emulating quantum computations using classical hardware (e.g., CPUs, GPUs, and FPGAs) is essential to prototype and test quantum algorithms, given the current lack of fully realized quantum computers. In this paper we will at first we survey the recent works incorporating FPGAs with GPUs and CPUs to form a hybrid architecture, and the concluding section of this review provides an outlook on future quantum operations emulation. FPGAs are used for parallel matrix multiplications necessary to execute quantum gates, and GPUs handle intricate, floating-point-heavy calculations needed for multi-qubit gate executions. The CPUs can be used to arrange the movement of data, control memory resources, and schedule gate sequences among different types in the system. This approach can handle computational tasks, taking into consideration different hardware capabilities. It can thus be able to emulate quantum circuits with greater performance than CPU-only or GPU-only solutions. This article presents the challenges of inter-device communication, synchronization, and memory management and of strategies to improve throughput and minimise latency in large-scale quantum emulation. This work also highlights the potential of FPGA-GPU-CPU architectures as a scalable solution for advancing quantum computing research and prototyping quantum algorithms in classical environments. Until a fully functional quantum computer emerges, this architecture can also be expanded to an FPGA-GPU-CPU-QPU device driven by a high-level programming language available to the end user.

1. QUANTUM COMPUTING LIMITATIONS AND CHALLENGES

1.1. CHALLENGES IN QUANTUM COMPUTING

Quantum computing has made remarkable progress nevertheless, it's still in its embryonic phase. Quantum Processing Units (QPUs) are limited by their size and computational power. Today QPUs are often referred to be Noisy Intermediate-Scale Quantum (NISQ) devices, consisting of a few hundred qubits at most. Ever more, these qubits are prone to errors arising from decoherence, gate infidelities, and environmental noise [1, 23, 12]. Decoherence, the gradual loss of quantum information to the environment, restricts the coherence times of qubits and hence the number of operations that can be reliably performed. Scaling up the number of qubits is complicated by increased crosstalk, calibration challenges, and the need for complex control electronics [7]. Moreover, implementing quantum error correction to achieve fault-resistant computation adds substantial resource overhead, requiring many physical qubits to represent a single logical qubit [14]. Many advancements need to be made and challenges overcome before this technology becomes mature and fully functional units with a practical use will appear. These challenges show the importance of efficient emulation techniques and open the case for exploring the possibilities of the use of a hybrid-based architecture.

1.2 LIMITATIONS IN QUANTUM COMPUTING

Quantum decoherence is the biggest problem in Quantum Computing. Qubits are highly sensitive to their surroundings. Qubits interact with external systems, and the quantum register can lose its state, which leads to computational errors [1]. As for now, we have a limited number of qubits, and this impacts the complexity of problems that can be solved using quantum computing. This problem could be solved with the increase of the number of qubits to the desired number. However, we also need to maintain coherence and controllability, and this is a significant technological hurdle [20]. The quantum error correction (QEC) is causing quite a substantial overhead. It is caused by the need for a large number of physical qubits for encoding a smaller number of logical qubits, and this fact complicates the hardware structure [2]. Only a few quantum algorithms offer an advantage compared to classical ones until now. New quantum algorithms are needed in this case, and a full understanding of their potential requires extensive testing and use case validation [3]. A quantum computer may be constructed in different ways. This led to unique implementation problems and challenges, including the complexity of fabrication and the stability of operation. For example, qubits can be such in superconducting circuits, trapped ions, and quantum dots [4].

Equipment allowing ultra-low refrigeration or precise control of the system, as well as the everyday maintenance of all appliances needed to run a quantum computer, is quite expensive [6]. As for today, there are no robust software tools and high-level programming languages that can simplify quantum algorithm development. Quantum programming, as well as quantum computing, is still an emerging field [5].

2. MATHEMATICAL TOOLS IN AN ADVANCED EMULATION SOLUTION

2.1 VECTORS AND MATRICES

The quantum state and the quantum operations can be expressed as vectors and matrices. That's why we have to remember why and how matrix-vector multiplication is so important in quantum emulation.

1. **Quantum States as Vectors**: Quantum states can be represented by vectors, and the state of a qubit or several qubits as a vector in a complex vector space. In this approach a single qubit can be seen in Dirac notation as the following state vector:

$$|\psi\rangle = \alpha|0\rangle + \beta|0\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

where α and β are complex numbers representing probability amplitudes, and $|0\rangle$ and $|1\rangle$ are basis states.

2. **Quantum gates as matrices**: Quantum gates that manipulate quantum states can be represented as unitary matrices. We can give as an example the basic Hadamard gate represented by the following matrix:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

To apply this gate on a qubit state, we multiply the matrix of the gate by the qubit's state vector.

$$|\psi'\rangle = H|\psi\rangle$$

3. **Matrix-vector multiplication for state evolution**: The simulation of a quantum evolution of the state in quantum computational emulation (when a quantum gate acts on a qubit cluster) can be done by a matrix-vector multiplication. When a gate is applied, the state vector, a representation of our quantum state, is multiplied by the matrix.

4. **Multi-Qubitsystems and tensor Products**: For multiple qubits, the system's over all state is represented by a larger vector (with 2^nentries for n qubits). The composite state is constructed via the tensor product of individual qubit states:

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

Gates acting on multiplequbits are represented by larger matrices (e.g., 4 × 4 for two qubits). They are made using tensor products, and matrix-vector multiplication. Procedures are essential for simulating quantum operations. However, the computational complexity grows exponentially with the number of qubits.

To sum up, matrix–vector multiplication is essential when attempting to simulate quantum computing on classical computers. This allows the simulation of transformations of quantum states through quantum gates, mimicking the probabilistic and interference patterns characteristic of quantum mechanics.

2.2. SYSTEM ARCHITECTURE AND TASK PARTITIONING

The use of FPGAs, CPUs, and GPUs altogether effectively requires assigning each task, knowing its specific advantages. The use of FPGAs for parallel matrix operations, GPUs for high-throughput floating-point arithmetic, and CPUs for orchestrating tasks and managing complex control logic. In moredetails we can present the above as follows:

1. **FPGAs:** Ideal for matrix-vector multiplications for individual quantum gates due to their parallel computation capability. FPGAs excel in implementing fixed gates, such as Hadamard or CNOT, directly in hardware for rapid, repeated application.
2. **GPUs:** Suitable for large-scale floating-point matrix multiplications, managing complex gates across multi-qubit states where extensive arithmetic precision is required.
3. **PUs:** Coordinate data flow between FPGAs and GPUs, manage memory resources, and control the overall quantum circuit flow. The CPU also handles complex control logic, error checking, and scheduling tasks, ensuring seamless system integration.

2.3. DATA FLOW ARCHITECTURE

On state preparation and initialization, the CPU initializes the quantum state vector and sets up quantum circuit instructions, allocating parameters for each gate and preparing memory blocks in both the FPGA and GPU for rapid access.

2.4. GATE EXECUTION

The CPU assigns gate operations based on complexity:

- **Single qubit gates:** Simple matrix multiplications, best suited to FPGA processing.
- **Multi-qubit gates:** More complex gates, such as those involving entanglement, are handled by the GPU for greater computational efficiency.

Intermediate results from the FPGA can be stored in dedicated memory and periodically consolidated by the CPU, which then sends data to the GPU if further processing is required.

2.5. EFFICIENT MEMORY MANAGEMENT

Shared memory and high-bandwidth interconnects

Using shared memory, such as PCIe or NVLink, allows fast data transfer between CPU, FPGA, and GPU components. The FPGA and GPU maintain their dedicated memory spaces but link to shared memory to enable rapid data exchange.

Memory overlap for state vectors

The CPU maintains a master copy of the quantum state vector, with GPUs and FPGAs handling subsets and updating them concurrently as needed.

2.6. PARALLEL EXECUTION AND PIPELINING

By establishing a pipelined workflow, each component operates on different stages of the quantum circuit:

- **CPU:** Fetches the next quantum gate and prepares instructions.
- **FPGA:** Processes the current gate, performing matrix multiplications in parallel.
- **GPU:** Manages floating-point-intensive gates or those spanning multiple qubits.

2.7. CONTROL INTERFACE IMPLEMENTATION

An API or control software layer (running on the CPU) can dynamically manage workload distribution by:

- Determining optimal hardware for each gate based on gate type and hardware load.
- Dynamically dispatching gates to reduce idle time and optimize hardware usage.
- Scheduling data transfers between memory pools as required for efficient operation.

2.8. OPTIMIZING FOR LARGE QUANTUM CIRCUITS

For complex circuits:

- Apply multi-threading and load balancing on the CPU to manage high data demands.
- Use multi-GPU configurations if necessary, allowing each GPU to handle portions of the quantum circuit. FPGA clustering, with each FPGA managing specific qubits of gate types, enables more complex simulations.

2.9. EXAMPLE WORKFLOW FOR HYBRID EMULATION SYSTEM

1. **Initialization:** CPU loads circuit information and initializes the quantum state.
2. **Gate assignment:** CPU allocates single-qubit gates to the FPGA and multi-qubit gates to the GPU.
3. **Execution:** FPGA processes assigned gates, updating relevant parts of the state vector.
4. **Data aggregation:** Intermediate results are periodically consolidated by the CPU.
5. **Final computation:** Once all gates are applied, the CPU aggregates the final state vector for measurement or output.

3. CHALLENGES IN HYBRID QUANTUM EMULATION WITH QPU

Despite its strengths, this hybrid system faces challenges:

- **Latency:** Data transfer latency may require optimisation of interconnects to reduce communication delays.
- **Resource allocation:** Multiple FPGAs and GPUs demand complex resource scheduling algorithms.
- **Synchronization:** Accurate state evolution requires careful synchronisation, particularly for multi-qubit gates spanning different hardware components.

4. TOWARD A HYBRID CPU/GPU/FPGA/QPU EMULATION ARCHITECTURE

As for now, QPUs are limited by noise, decoherence, which limits qubit counts. A promising approach integrates QPUs as specialised accelerators into a heterogeneous architecture that also includes CPUs, GPUs and FPGAs. Each of the classical resources has its strengths and could be used to emulate, optimize, and co-process quantum workloads. Modern HPC environments can rely on CPUs for complex control logic, data orchestration, and overall workload management. CPUs can handle instruction-level parallelism, branching, and coordination among multiple computational units.

The multi-core architecture and high memory bandwidth of GPUs can provide massive parallelism for numerically-intensive tasks with large-scale linear algebra operations for large matrix-vector multiplications and FPGA for the creation of custom data paths and optimised arithmetic units, as well as for less complex matrix multiplication tasks.

4.1. CLASSICAL INFRASTRUCTURE: CPUS, GPUS AND FPGAS

As for now, QPUs are limited by noise, decoherence, which limits restricted qubit counts. However, recent advancements have also demonstrated promising progress in the development of Majorana-based QPUs, which leverage the nonlocal, topologically protected nature of Majorana zero modes to further mitigate decoherence and reduce error correction overhead, paving the way for improved qubit counts and scalability [28]. But as for now, these developments are still in the early stages of research, and many challenges remain before fully scalable Majorana-based quantum processors are realised. A promising approach integrates QPUs as specialised accelerators into a heterogeneous architecture that also includes Central Processing Units (CPUs), Graphics Processing Units (GPUs), and Field-Programmable Gate Arrays (FPGAs). Each of the classical resources has its strengths and could be used to emulate, optimize, and co-process quantum workloads. Modern HPC environments can rely on CPUs for complex control logic, data orchestration, and overall workload management. CPUs can handle instruction-level parallelism, branching, and coordination among multiple computational units. The multi-core architecture and high memory bandwidth of GPUs can provide massive parallelism for numerically intensive tasks, with (large-scale linear algebra operations for large matrix-vector multiplications) [16, 17].

FPGAs apart of their reconfigurable hardware pipelines, unlike CPUs and GPUs, which have fixed instruction sets, can create custom data paths and optimised arithmetic units directly implementing operations on complex amplitudes. Moreover, they can be equally well-suited for less complex matrix multiplication tasks. Their reconfigurable hardware fabrics can be well suited to the exact needed dimensions and arithmetic precision required by the quantum simulation. This flexibility allows for fine-grained parallelism, optimized data reuse, and the direct integration of custom floating-point or fixed-point units that match the bit-precision demands of the quantum emulation amplitudes [21, 22]. This workload orchestration can benefit researchers with the balance of flexibility, parallel throughput, and customization. The CPU orchestrates the simulation workflow, managing data flow and communication. The GPU accelerates bulk linear algebra computations, while the FPGA provides specialised acceleration for quantum-statemanipulations, custom gate implementations, and real-time data processing. It can significantly enhance scalability and performance compared to a single processor type emulation [18, 19].

4.2. INCORPORATING QPUs INTO THE HYBRID WORKFLOW

The role of the QPU in this hybrid environment could be seen as that of a physical quantum co-processor. As for now, QPUs cannot handle large-scale quantum algorithms independently, they could be selectively integrated into a hybrid loop that combines classical simulation and optimization with the genuine quantum resources available on the QPU.

The workflow could be decomposed into the following steps:

1. **Pre-processing and algorithm decomposition:** Initially, CPUs, GPUs and FPGAs collaborate to emulate large portions of the quantum algorithm, identifying segments that are particularly challenging to simulate classically, such as non-Clifford gates or highly entangled states. The CPU supervises algorithm decomposition and parameter selection, while GPUs perform bulk state evolution steps, and FPGAs implement custom logic for fast, low-latency kernel operations [10, 11].
2. **Selective QPU offloading:** Subroutines that benefit most from real quantum resources are offloaded to the QPU. The CPU coordinates communication between the emulation environment

and the QPU, transferring necessary parameters and receiving measurement outcomes. The FPGA and GPU remain engaged, processing classical data before and after the QPU invocation, enabling tight integration and real-time feedback loops.

3. **Variational and iterative refinement:** In variational hybrid quantum-classical algorithms, the QPU evaluates the quantum circuit for certain parameters, and the classical hardware (CPU, GPU, FPGA) updates these parameters based on the measurement results [10, 15]. By running multiple iterations, the system converges toward improved algorithmic performance. The FPGA's allow on-the-fly reconfiguration to explore alternative data representations or error mitigation strategies.
4. **Scalability and future-proofing:** As QPU technology matures, the same hybrid architecture can seamlessly adjust. More complex quantum subroutines, previously handled by emulation, can be offloaded to improved QPUs. Meanwhile, the CPU/GPU/FPGA infrastructure remains valuable for tasks like quantum error correction processing, circuit optimisation, and classical resource management. In essence, this architecture provides a pathway from the NISQ era to fault-tolerant quantum computing by continuously balancing classical and quantum resources based on hardware capabilities and algorithmic demands.

By leveraging the complementary strengths of CPUs, GPUs, FPGAs, and QPUs, this hybrid approach offers a flexible framework for advancing quantum computing research. It bridges current limitations, enabling researchers to experiment, benchmark, and refine quantum algorithms while preparing for the day when large-scale, fault-tolerant QPUs become a reality.

A hybrid FPGA-CPU-GPU approach maximises quantum emulation efficiency. This will allow more complex circuits compared to a single device system. Such a device can be used with success in the field of quantum algorithm research and quantum-inspired computation. It could also be enhanced with a QPU that will be used only for tasks where the use of the QPU gives real benefits over the traditional computing methods, or whenever it becomes available.

5. A HIGH-LEVEL PROGRAMMING LANGUAGE FOR EASIER USE OF QUANTUM COMPUTING

Frameworks such as Qiskit and direct Open QASM have become standard tools for designing and executing quantum circuits. They often require programmers to think at a relatively low level, focusing on gate-by-gate commands or Python-based scaffolding, which can impede the rapid development of more complex quantum algorithms. This gap can be filled with a C-like language that raises the abstraction level by providing intuitive syntax, type-checking, and high-level constructs, while still compiling down to standard QASM instructions compatible with contemporary quantum hardware and simulators. Those benefits are more than welcome.

5.1. MOTIVATION AND BENEFITS

High-level quantum programming languages will offer advantages over raw QASM programming or specialised Python-based libraries like Qiskit.

- **Familiar syntax and structure:** Bringing a more familiar syntax and structure that will allow classical software developers to make an easier transition into quantum development [24, 25]. Control flows (e.g., if-else, for loops) and variable declarations that are similar to classical code will reduce the learning curve.
- **Stronger types of safety:** Providing first-class types for qubits, classical bits, and complex data structures, the language can prevent common errors such as reusing measured qubits or mismatching gate parameters, reducing debugging time and improving coder reliability [25].
- **Modularity and reusability:** Complex quantum functionalities can be encapsulated in functions or libraries for better code reuse and cleaner abstractions. When working directly with QASM this is more difficult to achieve.

- **Backend flexibility:** The use of a high-level language compiler can target different backends (e.g., IBM Quantum, Rigetti, or local simulators) and as the resulting end code will be standard QASM it will enhance and maximize hardware compatibility [26, 29].

As we can see, a high-level language will serve as a bridge between algorithmic design and low-level gate implementation, streamlining rapid prototyping and larger-scale software engineering practices for quantum applications.

5.2. XOR OPERATION IN A C-LIKE QUANTUM LANGUAGE AS AN EXAMPLE

To illustrate how this high-level language could work, consider a simple XOR operation on two qubits. In classical computing, the XOR of two bits outputs 1 if the bits differ and 0 if they are the same. In quantum hardware, a common way to realize XOR functionality is via the CNOT gate (also known as the Controlled-NOT gate). The control qubit remains unchanged, while the target qubit is flipped if the control qubit is ⟨1⟩.

```
//Declare two qubits in our C-like quantum language
qubit q0, q1;
// Performan XOR operation by applying a CNOTgate
xor(q0, q1);
// Optionallymeasure the resultsintoclassicalbits
cbit r0, r1;
measure q0 -> r0;
measure q1 -> r1;
```

In this example:

- qubit q0, q1; declares two qubits for use.
- xor(q0, q1); represents a high-level function that applies the quantum XOR operation (i.e., CNOT) on q0 (control) and q1 (target).
- The measure statements capture the final qubit states into classical bits r0, r1, reflecting standard practice in quantum experiments.

5.3. RESULTING QASM TRANSLATION

After the compilation of the high-level code above, we receive a code translated into OpenQASM script. A possible output might look like this:

```
OPENQASM 2.0;
include "qelib1.inc";
// Allocate quantum and classical registers
qreg q[2];
creg r[2];
// The XOR operation compiles to a CNOT gate
cx q[0], q[1];
// Measurements
measureq[0] -> r[0];
measureq[1] -> r[1];
```

This QASM code:

- A 2-qubit register q and a 2-bit classical register r are declared.
- A cx gate is applied by using q[0] as the control and q[1] as the target (equivalent to the XOR function in our high-level language).
- For measuring the qubits the resultis stored in classical bits r[0] and r[1].

Because the output is a valid QASM program, it can be run on a wide range of quantum computing platforms, including hardware devices that support OpenQASM natively, and cloud-based simulators or our proposed hybrid.

5.4. COMPARISON WITH QISKIT AND RAW QASM

- **Qiskit** is a Python-based framework that offers high-level gate abstractions, but still requires gate-by-gate or circuit-level specification. While being a powerful tool, Qiskit code can become verbose for large algorithms without additional structuring. A C-like language, by contrast, can introduce more familiar control flows and advanced type-checking that are beyond Python's dynamic typing.
- **QASM** provides low-level control over quantum gates, although it does not offer many high-level language features like loops, conditionals, or parameter copying. A C-like language can embed these structures natively, compiling down to QASM for hardware compatibility [26].

Quantum high-level language takes the best of both worlds. The convenience and expressiveness of a high-level language and the broad portability of QASM for quantum execution. Going forward, such a language can be extended with advanced features like automatic resource management, structured error handling for qubits, or even concurrency models for distributed quantum systems.

5.5. ELATED WORK AND OUTLOOK

Some research efforts have been made to propose a high-level quantum programming language that compiles to QASM or other intermediate representations :

- **Quipper**: is a scalable functional language for describing quantum circuits with support for a wide range of operations [24].
- **Silq**: is a high-level language to simplify computation and memory management in quantum programs [25].
- **Q#:** is a .NET-based language from Microsoft that provides native quantum data types and operations, with an intermediate representation convertible to QASM-like formats [27].

With the sophistication of quantum hardware and algorithms, a need for high-level and more visible. Future enhancements may involve optimising compilation paths, integrating advanced quantum error correction schemes, or supporting concurrency in multiprocessor quantum systems.

CONCLUSION

Quantum computing possesses significant potential to transform numerous domains, although it does not serve as a straight substitute for classical computing. Although quantum computers are not currently able to resolve all issues that classical computers cannot, they provide considerable advantages for particular complicated jobs, especially those involving extensive datasets or problems with exponential algorithmic benefits. Therefore, we have to elaborate and test new quantum algorithms for the dawn of a fully capable QPU. The proposed emulator will enable the development of quantum algorithms that will be able to fullyutilize the power of a quantum computer and will be ready the embrace the power of a fully featured quantum computer.

REFERENCES

[1] J. Preskill. Quantum computing in the NISQ era and beyond. *Quantum*, 2:79, 2018. https://doi.org/10.22331/q-2018-08-06-79

[2] S. J. Devitt, W. J. Munro, K. Nemoto, (2013). *Quantum error correction for beginners. Reports on Progress in Physics, 76(7), 076001.*

[3] A. Montanaro, (2016).*Quantum algorithms: an overview. npj Quantum Information, 2, 15023.*

[4] T. D. Ladd, et al. (2010).*Quantum computers. Nature, 464(7285), 45-53.*

[5] T. Häner, M. Roetteler, K.M. Svore, (2018). *Development of quantum computing software. IEEE Security and Privacy, 16(5), 18-24.*
[6] R. Van Meter, C. Horsman (2013). *A blueprint for building a quantum computer. Communications of the ACM, 56(10), 84-93.*
[7] M. Kjaergaard, M. E. Schwartz, J. Braumüller, et al. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics*, 11:369–395, 2020. https://doi.org/10.1146/ annurev-conmatphys-031119-050605
[8] M. A. Nielsen, I. L. Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
[9] R. P. Feynman (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6), 467–488.
[10] J. R. McClean, J. Romero, R. Babbush, A. Aspuru-Guzik. The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*,18(2):023023, 2016. https://doi.org/10.1088/1367-2630/18/2/023023
[11] Y. Li and S. C. Benjamin. Efficient variational quantum simulator incorporating active error minimization. *Physical Review X*, 7(2):02, 1050, 2017. https://doi.org/10.1103/PhysRevX.7.021050
[12] J. M. Gambetta, J. M. Chow, M. Steffen. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, 3(2), 2017. https://doi.org/10.1038/s41534-016-0004-0
[13] S. Bravyi, D. Gosset, R. König. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16:1040–1045, 2020. https://doi.org/10.1038/ s41567-020-0948-z
[14] S. J. Devitt, W. J. Munro, and K. Nemoto. Quantum error correction for beginners. *Reports on Progress in Physics*, 76(7):076001, 2013. https: //doi.org/10.1088/0034-4885/76/7/076001
[15] C. Kokail, C. Maier, R. Van Bijnen, et al. Self-verified variational quantum simulation of lattice models. *Nature*, 569(7756):355–360, 2019. https: //doi.org/10.1038/s41586-019-1177-4
[16] T. Häner and D. S. Steiger. 0.5 Peta byte simulation of a 45-qubit quantum circuit. In: *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, page 33. ACM, 2017.
[17] I. L. Markov. Quantum computation and quantum supremacy. *arXiv:1807.10749*, 2018.
[18] M. Smelyanskiy, N. P. D. Sawaya, and A. Aspuru-Guzik. Quantum simulation of electronic structure with linear depth and connectivity. *arXiv:1601.07195*, 2016.
[19] R. Huxford, P. Dukes, E. Rieffel, and B. Juang. Optimizing classical-quantum-hybrid algorithms with reconfigurable hardware. *arXiv:2208.12345*, 2022. *Quantum*, 2:79, 2018.
[20] J. M. Gambetta, J. M. Chow, and M. Steffen. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, 3(1):2, 2017. https://doi.org/10.1038/s41534-016-0004-0
[21] M. De Lorimierm, A. De Hon. Floating-point sparse matrix-vector multiply for FPGAs. In *2005 IEEE Symposium on Field-Programmable Custom Computing Machines*, pages 75–85. IEEE, 2005. https://doi.org/10. 1109/FCCM.2005.33
[22] F. Samia, M. Shafique, J. Henkel. High-performance FPGA-based dense linear algebra architectures: A survey. *ACM Computing Surveys*, 53(4), 84, 2020. https://doi.org/10.1145/3397022
[23] F. Arute, K. Arya, R. Babbush, *et al.* Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
[24] A. S. Green, P. LeFanu Lumsdaine, N. Ross, P. Selinger, B. Valiron. Quipper: A scalable quantum programming language. In *ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, pages 333–342. ACM, 2013.

[25] P. Bichsel, T. Haep, M. Krummenacher, P. Müller. Silq: A high-level quantum language with safe uncomputation and intuitive semantics. In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 286–300, 2020.
[26] A. W. Cross, L. S. Bishop, J. A. Smolin, J. M. Gambetta. Open quantum assembly language. *arXiv:1707.03429*, 2017.
[27] K. M. Svore, A. Geller, M. Troyer, C. Granade, J. Azaria. Q#: Enabling scalable quantum computing and development with a high-level domain-specific language. In: *Proceedings of the Real World Domain Specific Languages Workshop*, pages 1–10. ACM, 2018.
[28] Das Sarma, S., Freedman, M., C. Nayak, (2015). Majorana zero modes and topological quantum computation. npj Quantum Information, 1, 15001.
[29] J. Baker, Y. Alexeev, T. S. Humble. QCOR: A Language Extension and Compiler for Heterogeneous Quantum–Classic Computing. *IEEE Transactions on Quantum Engineering*, 2:1–13, 2021.

LIST OF ACRONYMS

API: Application Programming Interface. 5

CPU: Central Processing Unit. 1

FPGA: Field-Programmable Gate Array. 1

GPU: Graphics Processing Unit. 1

HPC: High-Performance Computing. 7

NISQ: Noisy Intermediate-Scale Quantum. 2

QASM: Quantum Assembly Language. 9

QPU: Quantum Processing Unit. 2

INDEX OF AUTHORS

PATRONAGE

National Centre for Research and Development

Prof. Dariusz Surowik - Rector of University of Lomza

UNIMA Research Commission

International Association of Theatre Critics Polish Section

Dr Mariusz Chrzanowski - Mayor of the Town of Lomza

Polish Foundation Pillars of Development

Podlaska Regional Development Foundation

klauCODE - High-Performance platforms for modern business

STRATEGIC PARTNERS

EDPOL Food &Innovation

Phoenix Systems

PianpolTex Sp. z o.o.

Pianpol Styła Sp. J.

UNICO POLSKA Sp. z o.o. Sp. k.

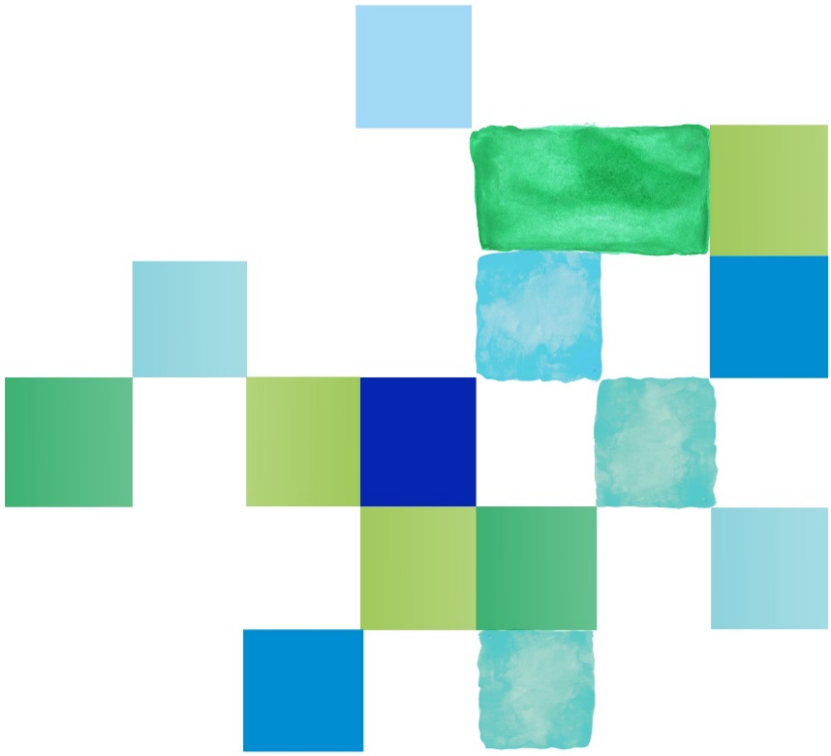
Zakład Usług Informatycznych NOVUM Sp. z o.o.

Zakłady Spożywcze BONA sp. z o.o.

ZBJW Łukasz Wądołowski

ZURAD Sp. z o.o.

Przedsiębiorstwo Handlowo-Usługowe Zacharzewski



ISBN 978-83-60571-75-0

UNIVERSITY
OF LOMZA