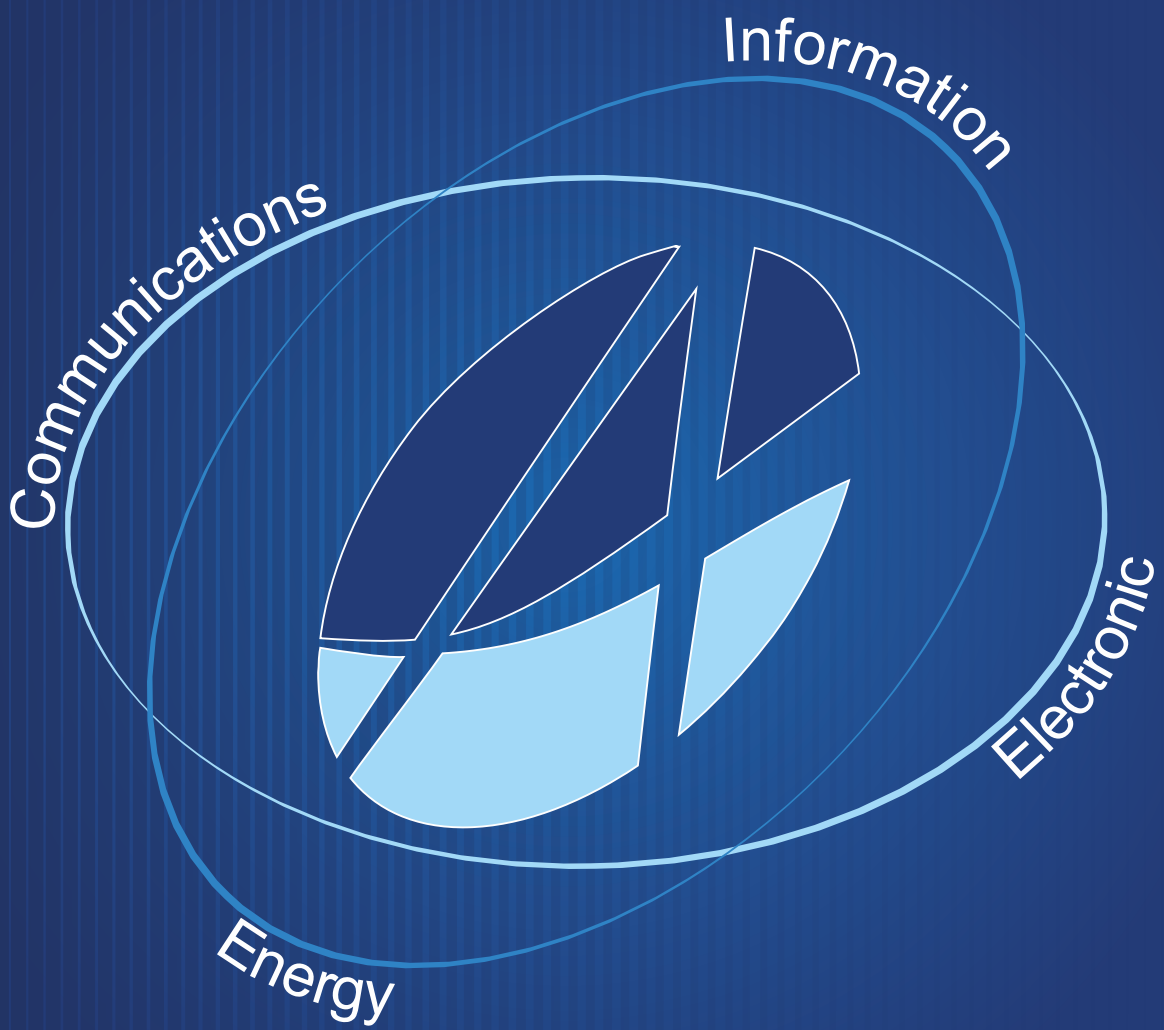
The Journal of CIEES

Communications, Information, Electronic & Energy Systems

Print ISSN: 2738-7283
Online ISSN: 2738-7291

Year 2024
Volume 4 (1)



CIEES Association Press

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

No liability is assumed by the editorial staff for the content of scientific papers and opinions published in this volume. They represent the author's point of view.

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

Editorial

As a result of widening the spectrum of communication, dissemination and implementation of scientific research results, in 2020 was founded the association journal (magazine), issued under the name The Journal of CIEES appearing both in print (ISSN: 2738-7283), and online (ISSN: 2738-7291) format with DOI: https://doi.org/10.48149/jciees.

The Journal of CIEES is published in English and it is open access, peer-reviewed international scientific journal publishing papers submitted by authors themselves for publishing and invited by the Editorial Board. The Journal of CIEES covers all the essential branches of theories, technologies, systems, tools, applications, work in progress, and experiences on all theoretical and practical issues arising in telecommunications, electronics, signal processing and applications, information technologies, energy systems and etc.

As always, many people have contributed to this issue including all authors, the anonymous reviewers, the Associate Editors, the Editorial Advisory Board and, of course, our outstanding production team. We wish to acknowledge each individual's contributions, and to also express our gratitude for everyone's commitment. We hope you enjoy this first issue of The Journal of CIEES.

We have had the privilege to publish truly outstanding, quality manuscripts that, judging by the response of our reviewers and readers, are important contributions to their respective fields of research. We want to take this moment to thank all of our reviewers and authors for entrusting us with their discoveries.

Editors-in-Chief:

Prof. TEODOR ILIEV, PhD
University of Ruse, Bulgaria

&

Prof. IVAYLO STOYANOV, PhD
University of Ruse, Bulgaria

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

MANAGING EDITORIAL BOARD

Editors-in-Chief:

Prof. Teodor ILIEV, PhD
University of Ruse
Bulgaria

Prof. Ivaylo STOYANOV, PhD
University of Ruse
Bulgaria

Associate Editor-in-Chief:

Prof. Grigor MIHAYLOV, PhD
University of Telecommunications and Post
Bulgaria

Chairman of the Editorial Advisory Board:

Prof. RENATO FILJAR, PhD
Krapina University of Applied Sciences
Croatia

Editorial Advisory Board:

Prof. Iliya ILIEV, PhD - University of Ruse, Bulgaria
Assoc. Prof. Bogdan POPA, PhD - University POLITEHNICA of Bucharest, Romania
Assoc. Prof. Gani BALBAYEV, PhD - Academy of logistics and transport, Kazakhstan
Prof. Felipe PENARANDA-FOIX, PhD - Universidad Politécnica de Valencia, Spain
Assoc. Prof. Angel TERZIEV, PhD - Technical university of Sofia, Bulgaria
Prof. Goran DJORDJEVIC, PhD - University of Nis, Serbia
Assoc. Prof. Selahattin KOSUNALP, PhD- Bandirma Onyedi Eylul University, Turkey
Assoc. Prof. Stanimir SADINOV, PhD - Technical university of Gabrovo, Bulgaria
Assoc. Prof. Marko HORVAT, PhD - University of Zagreb, Croatia
Assist. Prof. Danijela EFNUSHEVA, PhD - University "Ss. Cyril and Methodius", Republic of North Macedonia
Lecturer Irena POPOVIC - Krapina University of Applied Sciences, Croatia

Web Design Editor:

Assoc. Prof. Yordan DOYCHINOV, PhD
University of Ruse
Bulgaria

English Language Editor:

Assoc. Prof. Diana ILIEVA, PhD
University of Telecommunications and Post
Bulgaria

The Journal of CIEES

Volume 4, Issue 1 / 2024

Print (ISSN: 2738-7283) & Online (ISSN: 2738-7291)

http://journal.ciees.eu E-mail: publication@ciees.eu

Published by: CIEES Association Press, Bulgaria

Copyright: Association on Communications, Information, Electronic and Energy Systems

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

CONTENTS

Determination of the parameters of a DC motor with parallel excitation by a genetic algorithm 7
Anka Krasteva, Donka Ivanova, Vyara Ruseva

Stages of Development of Speech Signal Processing, Problems and Algorithms 11
Berdanov Ulugbek Abdumurodovich, Azamov Temur Narzullayevich,
Makhmudova Shakhzoda Yorkinovna

Investigation of a Precise Positioning System for Earth-moving and Construction Machines 20
Tatyana Golubeva

Design and Simulation of a PV System under Different Operating Conditions 24
Todor Todorov

Analysis of modern approaches to security in IoT networks 29
Marieta Haka

Homomorphic Encryption for Secure Federated Learning: A PRISMA-Based Systematic Review 37
Dinko Dinkov

AMSA: An Adaptive ML-Based Synchronization Arbiter for Resilient Time Distribution in 5G and Beyond Networks 48
Ivelin R. Penkov

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.1

Determination of the Parameters of a DC Motor with Parallel Excitation by a Genetic Algorithm

Anka Krasteva[1,*], Donka Ivanova[2], Vyara Ruseva[3]
[1]Department of Electric Power Engineering, "Angel Kanchev" University of Ruse, Bulgaria
[2]Department of Automatics and Mechatronics, "Angel Kanchev" University of Ruse, Bulgaria

*Corresponding author: akrasteva@uni-ruse.bg

Abstract: This paper presents a method of determining the parameters of a DC motor with parallel excitation by the use of a genetic algorithm. An approach is described for determining the mutual induction coefficient, the equivalent moment of inertia of the motor armature, the coefficient of friction and the friction torque based on the transient response graphs of the armature current and the rotational frequency of the motor. The measured resistance and inductive reactance of the armature and field windings of the motor are used as input data in the optimization procedure. The determined correlation coefficient, mean deviation error and mean square error between the experimentally taken and model-derived transient response graphs of the armature current and rotational frequency of the motor confirm the applicability of the presented approach.

Received 8 May 2024
Accepted 28 June 2024
Published 26 September 2024

Keywords: DC motor, Matlab, Genetic Algorithm.

1. Introduction

DC motor drives are used in industry because they are easy to model and control. The problem is that some of the parameters of the DC motor, such as the armature winding resistance, armature winding inductance, field winding resistance and inductance can be measured while others, such as the coefficient of mutual induction, the equivalent moment of inertia of the armature, the friction coefficient and friction torque, are unknown. Therefore, an accurate mathematical model of the motor cannot be built and appropriate control cannot be implemented.

The determination of motor parameters is a subject of research. Various optimization techniques [1] are used, as well as model searching algorithms [2], the method of moments [3], the regression method [4]. There is an increasing use of evolutionary methods, among which is the GA [5,6,7,8]. It is a stochastic method for solving optimization problems with or without constraints, based on natural selection - the process determining biological evolution. The GA changes the population of individuals at each step, selecting those from the current generation that will continue their evolution, i.e., they will be used for the next generation. The best individuals are selected on the basis of a functional or functionals (objective functions) that provide an estimate of the fitness of the individual for the desired solution. The advantage of the GA over classical optimization methods is that it generates a population of individuals (points) at each iteration, and the optimal solution is reached by the fittest point in the population, as opposed to classical methods where one point is generated at each iteration, and the optimal solution is reached by a sequence of points.

The genetic algorithm can be applied to solve a number of optimization problems for which standard optimization methods are not suitable, including those where the objective function is discontinuous, non-differentiable, stochastic, or strongly nonlinear.

The aim of this paper was to use a genetic algorithm to determine the parameters of a DC motor, i.e., the coefficient of mutual induction, the equivalent moment of inertia of the armature, the coefficient of friction and the friction torque, using as input data the transient response graphs of the speed and armature current as well as the measured values of the resistance and inductive reactance of the armature and field windings.

2. Explanation

The object of study was a model of a DC motor with parallel excitation with rated power $P_r = 3$ kW, rated voltage $U_r = 220V$ and rotational frequency $n = 1500\ \mathrm{min}^{-1}$ [9].

The stages required to achieve the objective of this paper were as follows:

- Building a virtual model of a DC motor in Simulink;
- Measuring the resistance and inductive reactance of the armature and field windings;
- Experimentally obtaining data of the transient response graphs of the angular speed and armature current during idling of the DC motor;
- Determining the parameters of the motor under study by a genetic algorithm;
- Comparing the experimentally obtained transient response graphs of the angular speed and armature

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

current of the motor with those obtained by the virtual model whose motor parameters were determined by a GA.

The motor model shown in Figure 1 was synthesized in Simulink [10, 11]. The model was built using the blocks from the SimPowerSystems library, namely DC Voltage Source – a DC voltage source supplying the armature and field windings of the motor respectively; DC_Machine – a model of a DC machine; Constant – used to set the motor shaft load (resistive torque); Demux – measurement block; Scope 1, Scope 2, Scope 3, Scope 4 – used to take the respective readings of the motor shaft angular speed (ω), the armature current value (i_a), the field current value (i_f), and the electromagnetic torque of the motor (M_e).

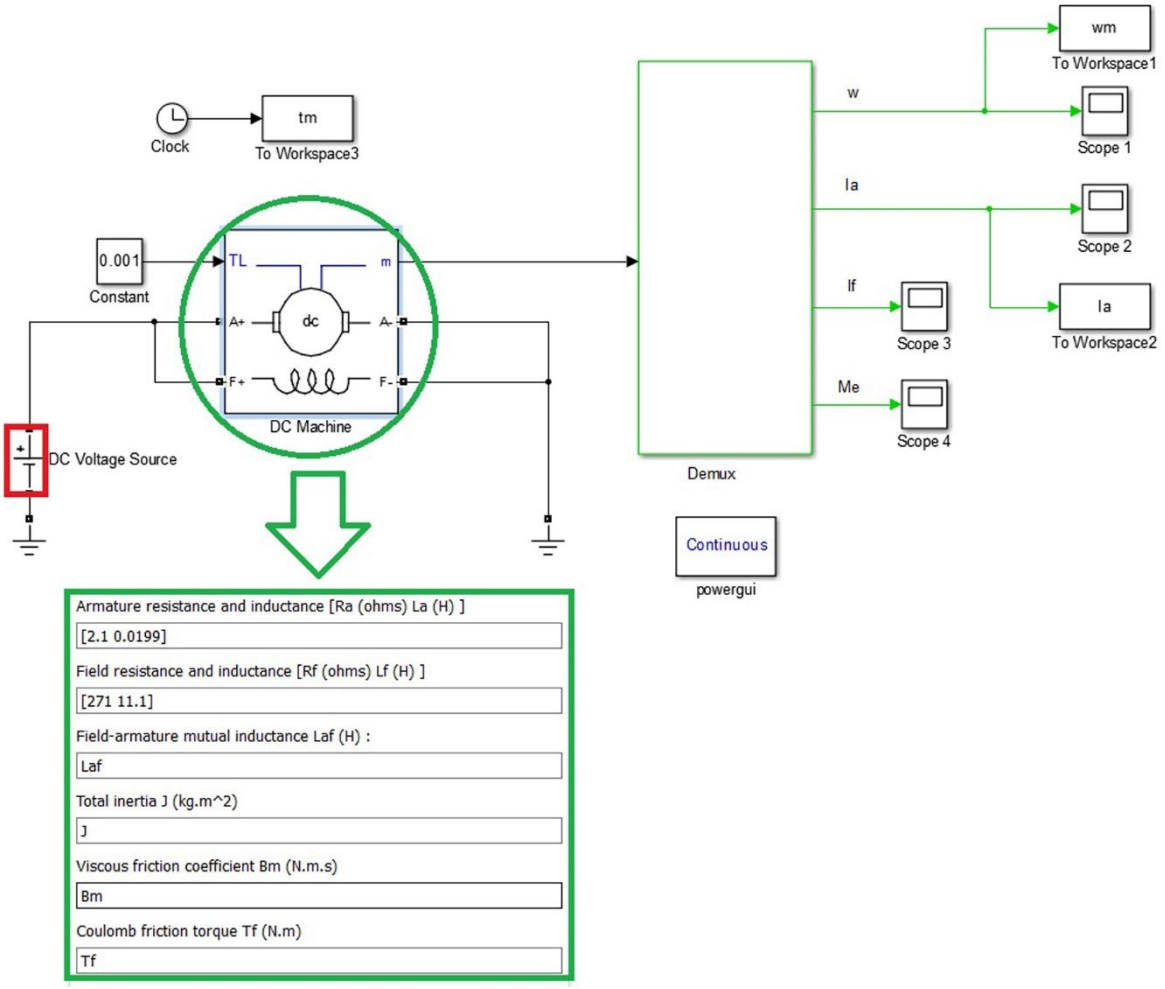


Fig. 1. Virtual model of study of a DC motor with parallel excitation.

The mathematical model that described the dynamics of an electric DC motor drive consisted of the following differential equations describing the electrical and mechanical processes in the drive:

$$U = E + Ri + L\frac{di}{dt}; \quad (1)$$

$$M - M_c = J\frac{d\omega}{dt}, \quad (2)$$

where U is the voltage of the armature winding of the motor, V; E – the armature electromotive force (EMF), V; i – the armature current, A; Φ – the magnetic flux in the air gap, Wb; M – the motor electromagnetic torque, N. m; M_c – the resistive torque, N. m; ω – the rotational speed of the motor shaft, $rad.s^{-1}$; R – the resistance of the armature circuit, Ω; L – the inductance of the armature circuit, H; J – the total moment of inertia of the armature and load, $kg.m^2$.

The following motor parameters had to be entered in the respective setting fields (DC_Machine block in Fig.1): R_a- resistance of the armature winding; L_a- inductance of the armature winding; R_f and L_f–resistance and inductance of the field winding. They were measured and their values are shown in Table 1.

Table 1. Parameters of the motor under study.

R_a, Ω	L_a, H	R_f, Ω	L_f, H
2.1	0.0199	271	11.1

The experimentally obtained transient response graphs of the angular speed of the motor shaft ω_s and the armature current i_s are shown in Figure 2 and Figure 3.

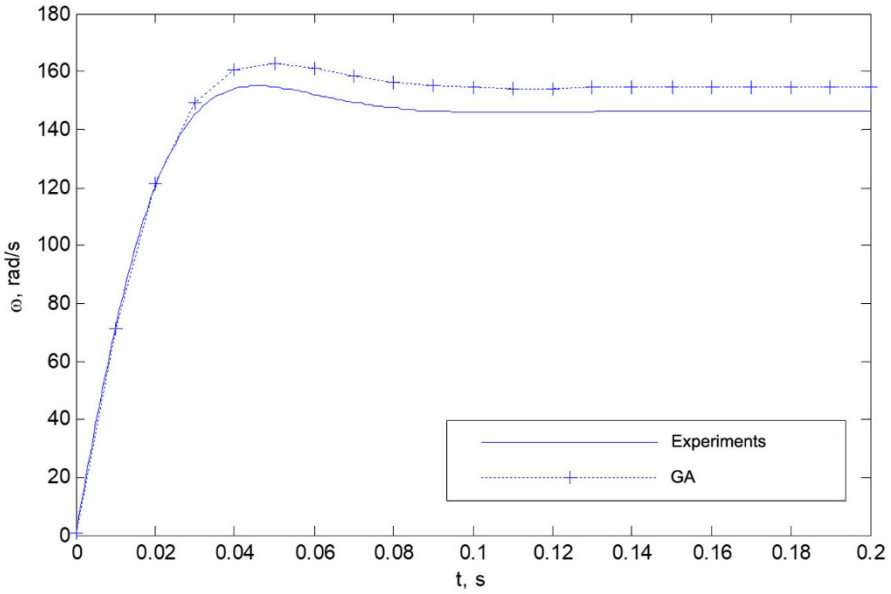


Fig. 2. Transient response graph of the angular speed of the DC motor with parallel excitation under study.

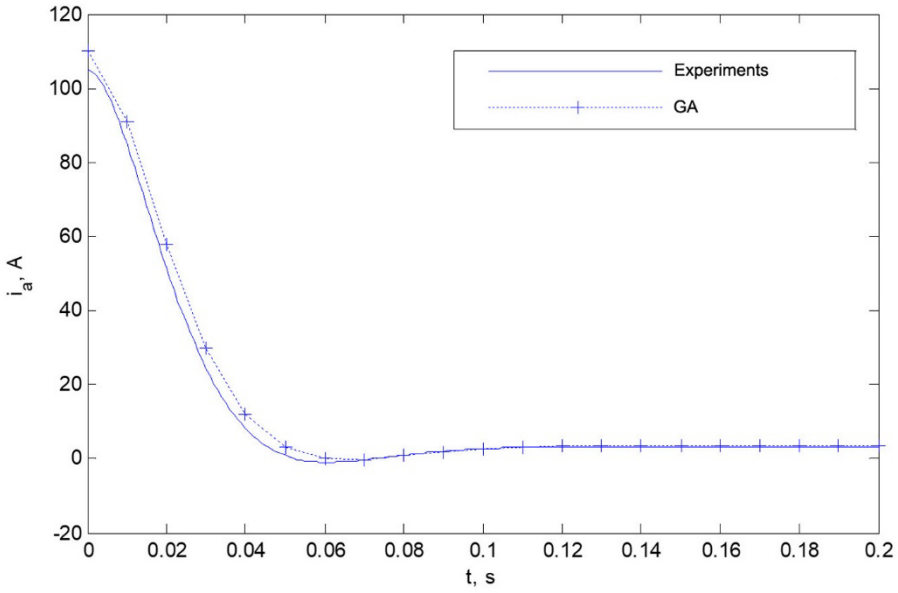


Fig. 3. Transient response graph of the armature current of the DC motor with parallel excitation under study.

In order to determine the parameters of the DC motor under study by a GA, the values of the resistance and inductive reactance of the armature and field windings were entered in the DC_Machine block in Fig. 1. The wanted parameters were the mutual induction coefficient, the equivalent moment of inertia of the motor armature, the coefficient of friction and the friction torque. When simulating the operation of the motor under study using the model in Fig. 1, the obtained data (in Scope 1) for the armature current i_{GA} and the rotational speed of the motor shaft ω_{GA} were sent to the MATLAB workspace. The experimentally obtained data for the armature current i_s and the rotational speed of the motor shaft ω_s were also present in the workspace. The F function that computed the optimization criterion was recorded in the M-file. It contained the declared global variables L_{af}, J, B_m, T_f, i_s and ω_s. The **sim** command was used to call the SIMULINK model and compute the corresponding objective function.

$$F = \frac{1}{N}\sum_{i=1}^{N}\left(\left(\frac{i_{GA}-i_S}{i_{S,max}}\right)^2 + \left(\frac{\omega_{GA}-\omega_S}{\omega_{S,max}}\right)^2\right), \quad (3)$$

The genetic algorithm was run using the **gamultiobj** command. The vectors defining the lower and upper bounds of the optimization parameters L_{af}, J, B_m *and* T_f, were set within bounds that included their expected values.

The optimization procedure was terminated when the set accuracy level was reached. The transient response graphs of the angular speed and armature current of the DC motor with parallel excitation under study (Figure 2 and Figure 3), as well as the parameters of mutual induction

coefficient $L_{af} = 1{,}8$, the equivalent moment of inertia of the motor armature $J = 0{,}02$, the coefficient of friction $B_m = 0{,}0295$ and the friction torque $T_f = 0{,}0058$, were obtained by a GA.

In this work, the correlation coefficient R was calculated by the formula

$$R = \frac{N\sum_{i=1}^{N} Y_{M,i}Y_{e,i} - \sum_{i=1}^{N} Y_{M,i}\sum_{i=1}^{N} Y_{e,i}}{\sqrt{\left(N\sum_{i=1}^{N} Y_{M,i}^2 - \left(\sum_{i=1}^{N} Y_{M,i}\right)^2\right)\left(N\sum_{i=1}^{N} Y_{e,i}^2 - \left(\sum_{i=1}^{N} Y_{e,i}\right)^2\right)}} \quad (4)$$

where $Y_{e,i}$ represented the i-th measurement, $Y_{M,i}$ represented the armature current (angular speed) for the corresponding measurement, N was the number of observations.

The obtained values for the coefficient of correlation for the angular velocity and the armature current were as follows: $R_\omega = 0.9990$, $R_i = 0.9991$.

The mean bias error MBE and the mean squared error $RMSE$ were calculated by the following formulas:

$$\mathrm{MBE} = \frac{1}{N}\sum_{i=1}^{N}\left|Y_{e,i} - Y_{M,i}\right|; \quad (5)$$

$$\mathrm{RMSE} = \left[\frac{1}{N}\sum_{i=1}^{N}\left(Y_{e,i} - Y_{M,i}\right)^2\right]^{\frac{1}{2}} \quad (6)$$

The obtained error values for the angular speed were: $\mathrm{MBE}_\omega = 6.9833$, $\mathrm{RMSE}_\omega = 6.5488$, and for the armature current: $\mathrm{MBE}_i = 1.6757$, $\mathrm{RMSE}_i = 2.7024$.

The correlation coefficient was close to one, while the mean bias error and mean squared error between the experimentally taken and the model-derived transient response graphs of the armature current and rotational frequency of the motor were less than 7%.

3. Conclusion

This paper presents an approach for determining the parameters of DC motors when such parameters are unknown. A genetic algorithm was used with the following input data: the resistance and inductive reactance of the armature and field windings of the motor, the transient response graphs of the armature current and the angular speed. The output (wanted) data were the mutual induction coefficient, the equivalent moment of inertia of the motor armature, the coefficient of friction and the friction torque.

The study was conducted on a DC motor with parallel excitation. The motor parameters and the transient response graphs of the angular speed and armature current were determined using a genetic algorithm.

The determined correlation coefficient, mean bias error and mean squared error between the experimentally taken and model-derived transient response graphs of the armature current and rotational frequency of the motor confirm the applicability of the presented approach.

References

[1] Adewusi, S. (2016). Modeling and Parameters Identification of a DC Motor Using Constraint Optimization Technique. *IOSR J. Mech. Civ. Eng*. vol. 13, pp. 46–56.

[2] Avoda, M. L. & Ramzy, S. A. (2019). Parameter Estimation of a Permanent Magnets DC motor. *Iraqi J. Electr. Electr. Eng.*, vol. 15, pp. 28–36.

[3] Hadef, M., Bourouina, A. & Mekideche, M. R. (2008). Parameters Identification of DC Motor via Moments Method. *Iran. J. Electr. Comput. Eng.* vol. 7, pp. 159–163.

[4] Shanmuga, N. B., Mythile, A., Pavithra, S. & Nivetha, N. (2020). Parameter Identification of a DC Motor. *Int. J. Sci. Technol. Rese*. Vol. 9, pp. 5746–5755.

[5] Amiri, M. S., Ibrahim & M. F., Ramli, R. (2020). Optimal parameter estimation for a DC motor using genetic algorithm. *Int. J. Power Electr. Drive Syst*. Vol. 11, pp. 1047–1054.

[6] Lankarany, M. & Rezazade, A. (2007). Parameter Estimation Optimization Based on Genetic Algorithm Applied to DC Motor, In Proceeding of the International Conference on Electrical Engineering, Lahore, Pakistan, 2007, pp. 1-6, doi: 10.1109/ICEE.2007.4287313.

[7] Jesenik, M., Hamler, A., Trbušić, M. and M. Trelep. (2000). The Use of Evolutionary Methods for the Determination of a DC Motor and Drive Parameters Based on the Current and Angular Speed Response. Faculty of Electrical Engineering and Computer Science, University of Maribor, Koroška cesta 46, 2000 Maribor, Slovenia, 2020. https://doi.org/10.3390/math8081269

[8] Amiri, M., Ibrahim, M. & Ramli, R. (2020). Optimal parameter estimation for a DC motor using genetic algorithm. *International Journal of Power Electronics and Drive Systems*, Vol 11, June, pp.1047-1054, http://doi.org/10.11591/ijpeds.v11.i2.pp1047-1054.

[9] Ruseva V., A. Krasteva. (2023). Using the Matlab Programming Environment in the Course of Student Training in the Electrical Machines Discipline. In Proceeding of the 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, IEEE, 2023, pp. 1561-1566.

[10] Chernykh I. V. (2008). Modelling of Electrotechnical Devices in MATLAB, SimPowerSystems and Simulink, DMK Press, Moscow.

[11] Bebikhov Y.V., A.S. Semenov, M.N. Semenova, I.A. Yakushev. (2019). Analysis of Methods of Simulation Modelling of Technical Systems in the Matlab Environment. Modelling, *Optimisation and Information Technologies. Scientific Journal*, vol. 7, No. 3, 2019.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.2

Stages of Development of Speech Signal Processing, Problems and Algorithms

Berdanov Ulugbek Abdumurodovich[1], Azamov Temur Narzullayevich[1], Makhmudova Shakhzoda Yorkinovna[2]

[1] Department of introduction ICT and digitization, Innovative Development Agency, Tashkent, Uzbekistan
[2] Department of Artificial Intelligence, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

*Corresponding author: u.berdanov@ilmiy.uz

Abstract: This article develops mathematical methods of learning and decision-making in speech recognition, when extracting informative properties from speech signals, intelligent algorithms based on a data set consisting of properties. Effective ways to isolate features from speech signals are explained in sequential steps. These sequences are reflected in the database of several solutions (HMM, CNN and DTV) based on their comparative analysis, and the results are presented in the form of a table. In the experiments, sounds, syllables and words of speech were evaluated based on familiar intelligent algorithms, and a high result was achieved using the CNN mode.

Keywords: Hidden Markov models, convolutional neural networks, Dynamic Time Wrapping, artificial intelligence algorithms, informative properties.

Received 11 September 2024
Accepted 17 October 2024
Published 4 December 2024

1. Introduction

The importance of processing and analyzing speech signals in the Uzbek language is growing in today's world. Speech recognition technologies are commonly utilized in different fields, especially in domains like virtual assistants, voice control systems, text-to-voice conversion, etc. To excel in these domains, comprehending the intricate structure of the speech signal and devising methods for its analysis is crucial.

The focus of this study is on utilizing artificial intelligence algorithms to process and analyze speech signals in the Uzbek language. The primary aim of the research is to identify essential parameters in speech signals and then utilize intelligent algorithms to enhance the decision-making process [1].

The research examines commonly utilized algorithms in artificial intelligence like dynamic programming, implicit Markov models, and neural networks. A study is conducted on their abilities and restrictions in handling speech signals, and a broad model is suggested. Experiments are carried out using the speech signal of the Uzbek language to assess the performance of this model. The examination of the findings provides new opportunities for structuring speech signal parameters, enhancing the effectiveness of smart algorithms, and advancing Uzbek language speech recognition technologies.

Contemporary systems employ three primary categories of techniques to compute speech cognition. Hidden Markov models are part of the initial group. They analyze if an opening speech can be seen as a series of specific phonemes and the likelihood of transitioning between them. Recognition involves searching for the most probable sequence of phonemes for a given input signal [3]. The next method relies on comparing to the standard. Each word in the dictionary is compiled in a certain manner as per the standard. In the process of recognition, the closest word to the standard input signal is chosen. The artificial neural networks form the foundation of the third set of techniques. The core of the techniques is discovering a key function from the input signal that can identify if it fits into a specific class. Artificial neural networks are constructed based on the organization of biological neural networks and effectively handle various tasks [2].

Methods utilizing neural network technology play a unique role in the field of speech recognition. The outcome of recognition in these techniques is influenced by how a specific neural network type is structured and operates. Neural networks consist of connected basic processors that carry out simple tasks.

2. Stages of development of speech signal processing, problems and algorithms

The main goal of the research work is to develop speech recognition algorithms based on a limited

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

vocabulary, the results of which are carried out to this day, processing speech signals. This, algorithms are selected that process speech signals based on algorithms and models developed by scientists. The results of the analysis show that there are several algorithms that process speech signals. Based on the results of the study, the process of processing speech signals can be carried out in three stages [4]. The general guide structure of the algorithms of these steps is presented Figure1.

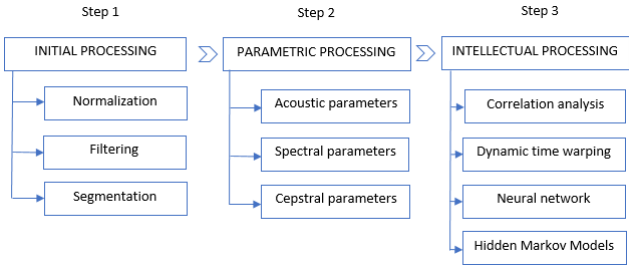


Fig. 1. The stages of processing speech signals.

The possibility of these stages can be used to get acquainted with the sounds, syllables and words of speech. Based on the task set based on the algorithms specified at these stages, the primary processing of the speech signal takes place at the first stage [5]. After that, the speech signal is divided into parameters and information about the speech signal is extracted using intelligent processing algorithms. At each stage, there are several algorithms for processing speech signals. Based on the problem statement, it is necessary to select algorithms. That is, based on a perfect analysis of the task, parameters are selected and the potential of intelligent algorithms is used. At these stages, there are several types of algorithms, of which one or more types can be used simultaneously [6].

The formation of speech signals is described as depending on the characteristics of the speaker. The algorithms of these stages can also be used in the process of processing speech signals. These stages form a set of several algorithms in their working mode. Each stage is organized based on the sequence of algorithm changes depending on the task statement. These steps are described below.

2.1. The stage of primary processing.

During the primary processing of speech signals, the speech signal is converted from analog to digital form. This task is performed by analog to digital converters. At the same time, discrete quantization and encoding are performed. This is often a speech signal converted to WAV file format, the sampling rate is quantized in the range of 8 kHz – 19.2 kHz, and the recording channel is selected mono. In real-time speech signal processing tasks, the speech signal is quantized at a sampling frequency of 22 kHz. These parameters are standard when selecting a speech signal. The reason for this is the voice signal [7]. The WAV file format is an expression of a speech signal in an uncompressed state, and the sampling rate of 22 kHz is the standard sampling rate chosen by scientists when processing speech signals. After the speech signal is presented in digital form, it is processed by the following initial processing algorithms.

Normalization. The digital expression of the speech signal is adjusted to the standard margin at different intervals. Such normalization intervals for speech signals [0:1], [-1:1], [-3:3], [-128:128], [-256:256], [-512:512] there are intervals. These intervals ensure that the values of the speech signal fall within one standard interval. When processing speech signals, the interval [-1:1] is often chosen.

Filtering. Speech signal filtering is used to clear the speech signal from interference and eliminate external influences. To do this, you can use filters with finite pulse characteristics and filtering algorithms with infinite pulse characteristics. After the filtering process, the silence states in the speech signal are lost [8].

Segmentation. Segmentation is the process of dividing the values of a speech signal into frames of a given size. Currently, in modern speech signal processing systems, speech signal frames include 64, 128, 256, 512, 1024, 2048 accepts the coefficients of the speech signal. When processing speech signals, one of these segmentation intervals is selected, depending on the formulation of the question. As a result, the speech signal is divided into frames.

The process of mirroring a segmented speech signal performs the task of approximating the initial and final values of the frame being determined to zero. The main reason for this is that with parametric processing, spectral values do not tend to infinity [9]. There are such types of mirroring algorithms as rectangular mirror, Hannah mirror, Hemming mirror, Blackman mirror, Kaiser mirror. The Hemming mirror for speech signals is one of the most commonly used types of mirrors by scientists.

2.2. The stage of parametric processing.

At the stage of parametric processing, acoustic, spectral, formant frequency, and cepstral parameters of the speech signal are determined. In the general account, the choice of a specific parameter is selected depending on the formulation of the question. Each parameter has its own mathematical algorithm. At the same time, the completeness of the parameters is checked.

The spectral density of speech signals is calculated using mirror functions. Here the mirror size changes without stripes. This approach characterizes the activity of the human auditory system. The first MFCC algorithm was S.B. Davis and P. Mermelstein proved that speech can be used to solve the dating problem. The MFCC algorithm is calculated in the following sequence.

A discrete cosine transforms (DCT) and discrete fourier transform (DFT) more information about these converters is described in this source [22].

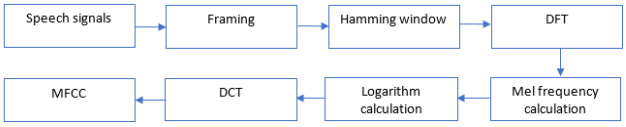


Fig. 2. Algorithm for obtaining MFCC values

The algorithm for obtaining MFCC values consists of several successive stages, the algorithm for calculating the Mel-frequency is shown above.

2.3. The stage of intelligent processing.

The intelligent processing stage is an important stage. At this stage, the grouped set of parameters is processed based on decision-making algorithms. Dynamic programming algorithms, Markov chains, and neural network algorithms can be attributed to this group of stage algorithms. The results of the intelligent processing stage are summarized [10]. That is, the results of the processed frames are analyzed and a final conclusion is made about the state of the speech signal.

Parametric characteristics of speech are important when processing speech signals. That is, as a result of processing the parameters of human speech based on intelligent algorithms, a conclusion is made about the speech signal. The state of the conclusion depends on the formulation of the question. We will fully familiarize ourselves with the general theory of intelligent algorithms below.

3. Application of artificial intelligence algorithms in speech recognition

Uzbek language based on the analysis of the above algorithms for processing speech signals, speech signals were divided into parameters. Based on these parameters, it is necessary to determine the speech signal. The decision-making process is carried out by intelligent algorithms. Artificial intelligence algorithms come in several types, depending on the tasks they are used for. Their algorithms, which are currently widely used in speech signals, include dynamic programming algorithms, implicit Markov models, and neural network algorithms. These artificial intelligence algorithms are used to make decisions based on the parameters of speech signals. The main purpose of the research work is to organize a parametric set of speech signals and propose a generalized model that allows making decisions based on these parameters as a result of the effective use of intelligent algorithms and evaluating its effectiveness. As a result of the experiments, a set of parameters was formed on which spectral analysis processing speech signals was based [11]. As a result of selecting the necessary parameters from this set of parameters, a general structure based on dynamic programming algorithms, implicit Markov models and neural networks was created. This structure is shown in Figure 2. Based on this question, the use of all parameters and decision-making algorithms in the structure is not required. That is, based on the task, parameters are selected and the possibility of decision-making algorithms is used.

More about fast-Fourier transform (FFT) is described in this source [22].

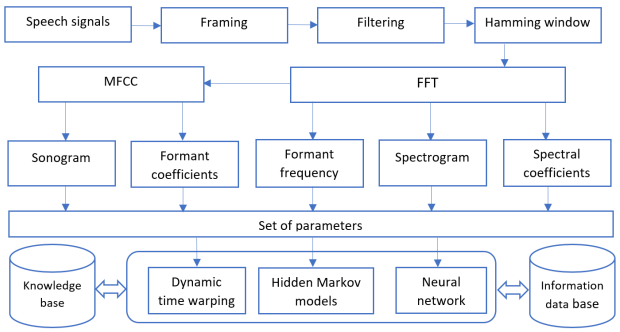


Fig. 3. Speech processing as a general structure.

A user familiar with the speech of the Uzbek language, this general structure was the first to apply the process of shredding a recorded speech signal. Using the above algorithm of the grinding filter [12]. After that, the smoothed signal is segmented. Segmentation is used to divide the speech signal into frames. After that, the task of extracting parameters from each frame is displayed. A discrete Fourier transform is performed from spectral algorithms with parametric decomposition. Using spectral algorithms, spectral distortions, formant frequencies and spectrograms of the speech signal can be returned as a signal parameter. In addition, spectral algorithms can help to obtain MFCC parameters and return as signal parameters in the MFCC algorithm utility. These parameters are used for general parameters.

The solution of the problem is determined from the selected parameters with the addition of the basics of the artificial intelligence algorithm. Artificial intelligence algorithms dynamic programming algorithm, hidden Markov models and neural network algorithm were analyzed during the study. This method is able to solve a number of practical issues that call into question the processing of human speech. An example is the definition of personality based on human speech, the content of human speech and use in the management system in order.

3.1. Speech recognition solutions based on Dynamic Programming

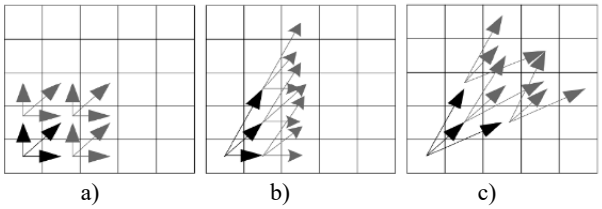
DTW (Dynamic Time Warping) - this algorithm is considered a kind of dynamic programming algorithms. It is used to compare the algorithm with the parameters of speech signals. There are several types of algorithms for comparing the parameters of speech signals, each of which requires that the parameters be of the same length during the comparison process. Unlike other comparison algorithms, it allows you to compare two vectors of different lengths. An effective aspect of the DTW algorithm is that this algorithm itself is able to determine the difference between vectors of different lengths. Therefore, this algorithm is widely used in the processing of speech signals.

When using this algorithm to recognize speech sounds, syllables and words, MFCC signal parameters were obtained. It is known that the MFCC values in one frame of a given speech signal are 12. When organizing an ad database for a given speech M frame, a sum of MFCC winds of 12xm is generated. As a result, a reference database is formed for a given speech signal [13]. The main problem is comparing the incoming anonymous voice signal with the database of ads. The number of MFCC values of the incoming speech signal frames is 12, and the number of frames is N. The result is an unknown speech signal, which is 12xn, and the signal, which is 12xm, requires comparison with some data. The DTW algorithm is effective when comparing signals with different resolutions. The DTW algorithm builds the path of the least action from the sequence when solving such problems. There are several types of computing speech signal information using the DTW algorithm:

- symmetrical, classic (Figure 4, a);

- asymmetric (Figure 4, b);
- fast (Figure 4, в).

Each variant of this type of calculation of the DTW algorithm has a different speed and different effect, depending on the parameters of the speech signals.



a) b) c)

Fig. 4. Types of DTW algorithm.

The DTW algorithm, based on MFCC parameters, compares an unknown speech signal of 12XN with a standard data of 12xm with some of the unknown speech signal X ($x_1, x_2, ..., x_n$) and standard data some are absorbed into E ($e_1, e_2, ..., e_m$). As a result, vectors of length of two different sequences are formed. This is calculated using the following formula.

This is followed by the calculation of local deviations between the two sequences. Local deviation is the distance between the I - frame of an unknown speech signal and the j – frames in the standard database. The most common method of calculating local deviations is the method of calculating the absolute deviation between the values of the two elements, that is, the Euclidean distance. This is calculated using the following formula [14].

$$D_l(x_i, e_j) = \|x_i - e_j\| = \sqrt{\sum_{k=1}^{N}(x_{ik} - e_{jk})^2} \quad (1)$$

In addition, there are several types of calculation of local deviations. They are calculated using the formula [14]:

- Manhattan distance;

$$D_l(x_i, e_j) = \|x_i - e_j\| = \sum_{k=1}^{N}|x_{ik} - e_{jk}| \quad (2)$$

- Minkowski distance;

$$D_l(x_i, e_j) = \|x_i - e_j\| = \sqrt[m]{\sum_{k=1}^{N}(x_{ik} - e_{jk})^m} \quad (3)$$

- Chebyshev distance;

$$D_l(x_i, e_j) = \|x_i - e_j\| = \max_{k\in 1,N}|x_{ik} - e_{jk}| \quad (4)$$

As a result, a deviation matrix Ωnm is constructed, consisting of n rows and m columns. Using the deviation matrix Ωnm, a path W of length K is constructed. This path indicates the correspondence between the vectors X and E. The element k of the path W is defined as wk=(i, j), D(wk) with $D_l(x_i,e_j)$ is considered as an equivalent formula. The length of the K-path is determined by the following condition.

$$\min(m, n) \le K < m + n - 1 \quad (5)$$

The W path is determined as a result of the following three conditions. There are many ways to fulfill these three conditions, but the optimal definition of this path is carried out using the following formula [15]:

$$DTW(X, E) = min\left\{\frac{1}{K}\sqrt{\sum_{k=1}^{K} D(wk)}\right\} \quad (6)$$

The algorithm used to recognize sounds, syllables and words of the Uzbek language by the DTW method is shown in Figure 5 below.

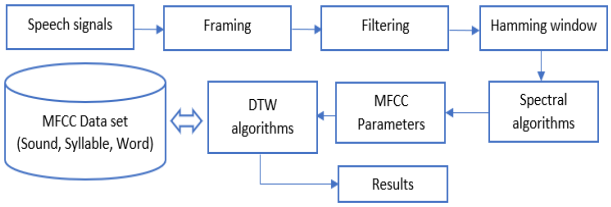


Fig. 5. Speech recognition algorithm based on the DTW algorithm DTW.

In this structure of the speech signal processor, the MFCC parameters of sounds, syllables, and words are stored in the announcement database. During processing of the incoming speech signal, the MFCC parameters of the signal are compared with the MFCC parameters in the ad database using the DTW algorithm. As a result, the process of recognizing the incoming speech signal takes place. When creating an ad database using the DTW algorithm, it is recommended to group the database. Therefore, the algorithm creates a separate database of sounds, syllables and words. This is due to a reduction in the calculation time during the comparison process. In the issue of speech recognition based on the DTW algorithm-based speech recognition method, the results of the ban for a single speaker gave a minimum accuracy of 70% to 99%. These results are presented in Table 1 below in the context of speech sounds, grouped into groups.

Table 1. Results of sound recognition using the DTW algorithm.

Classification of speech sounds (Uzbek language)		Result based on DTW algorithm (%)	
		Min	Max
Vowel sounds	A, O, O‘, U E, I	92	99
Crawling noises	S, Z, SH, J, CH	76	82
Sonar sounds	R, L, M, N	83	92
Tongue back sounds	K, G, X	97	96
Deep tongue sounds	Q, G‘, H	73	86
Sonorous sound	B, V, Z, D, J, G, G‘, Y, P, F	82	94
Muted sounds	S, T, SH, CH, K, Q, X, H	77	95

Like any decision-making algorithm, DTW has a number of disadvantages. In this algorithm, the number of simple calculations increases depending on the size of the computational matrix [16]. This creates computational complexity. The large number of columns I and rows J of the deviation matrix generates the following disadvantages:

- the complexity of the process of studying large digital matrices and searching in them;
- calculating a large number of deviations takes a long time;
- to increase small calculations in the matrix.

Due to the above disadvantages, the DTW algorithm has generally proven itself well in determining sounds and syllables. In addition to the slippery and deep language, the error in the background sounds was found unsatisfactory. Thus, the DTW algorithm can serve well mainly for correcting learning and speech disorders.

3.2. The Markov model speech recognition process

Based on the implicit Markov model, NFCC parameters are taken as an input parameter when solving the problem of familiarity of sounds, syllables and words of speech. To build an implicit Markov model using these parameters, it is necessary to select a sequence of states.

Experiments show that using the hidden Markov model, it is necessary to determine the number of hidden cases when recognizing sounds, syllables and words of speech. The number of hidden states depends on mass spectrometry. The hidden Markov model is the most effective solution for recognizing speech sounds, syllables and words, it is necessary to select the number of hidden cases. There are 29 sounds in the Uzbek language, each of which allows you to express one hidden state in a hidden Markov model.

The solution to the problem is to determine the highest probability of the existence of each frame of a given speech signal (MFCC frame parameters) in these 29 hidden states. This decision determines which sound the given frame of the speech signal belongs to. As a result of sequential frame processing, the sequence of sounds in the speech signal is determined. Based on the identified sequence of sounds, it is possible to artificially determine syllables and words in a speech signal [17]. To do this, an implicit Markov model of a sequence consisting of n-states is first constructed. In solving the problem, N=29 is considered.

The implicit Markov model is based on modeling processes consisting of implicit N-states. The transition between states is carried out in the time interval t according to Probst's law, and the transition probability matrix is described by ANN. A schematic representation of the transition scheme between the hidden states of the hidden Markov model is shown in Figure 6.

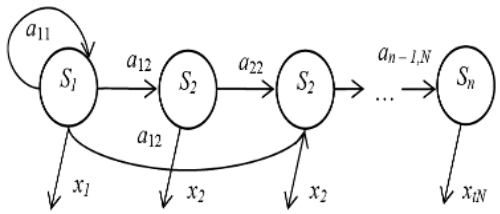


Fig. 6. Hidden cases of the Hidden Markov model.

The presence of the model in a given state i corresponds to a certain stationarity of the observed signal in a given time interval. A simple physical interpretation of the hidden Markov model arises: sometimes it is considered a process that gradually changes its properties.

Multidimensional probability distribution function $f_j(x)$at the next transition to a new state i, at time t, an output vector is formed, called the parametric vector xt. As a result of the hidden Markov model, the length the parameter is a sequence of vectors [x_1, x_2, ..., x_t] [16].

The advantage of the Hidden Markov model over other intellectual algorithms is that it has different lengths and the ability to work with sequences and parameters.

$$f_j(x) = \sum_{i=1}^{M} w_i p_i(x) \quad (7)$$

where M is the number of components in the model; w_i is the weight of the component; $p_i(x)$ is the normal distribution of the event measure D. The $p_i(x)$ function is defined by the expression:

$$p_i(x) = \frac{1}{2\pi^{\frac{D}{2}}|\sigma_i|^{\frac{1}{2}}} + exp\left\{-\frac{1}{2(x-\mu_i)^T\sigma_i^{-1}(x-\mu_i)}\right\} \quad (8)$$

where D is the size of the vector; μ_i is the expectation vector; σ_i is the covariance matrix.

Hidden Markov models the analysis process, as in any other expert system, when processing speech information is carried out in two stages.

1) Training - concealment the Markov model of the Baum-Welch algorithm is used in the training of speech signals. Scientists have proved that this algorithm is one of the optimal algorithms for learning speech signals

2) Definition - a sequence of vectors for determining the probabilities observed in S_i [x_1, x_2, ..., x_T] probability maximization is determined using the Viterbi algorithm. A certain probability determines the outcome. The following is a brief description of the above algorithms [19].

The process of learning a hidden Markov model consists in determining the following parameters using a set of training samples:

- A matrix of probabilities of transition between A_{NN} states is constructed;
- For each case, using the Gauss algorithm, the parameters in the A_{NN} matrix are determined: mathematical expectation, covariance matrix and weight.

When constructing a probability matrix and determining parameters using the Gauss algorithm, the forward-backward algorithm is used to solve these problems using two iterative forward-backward algorithms and the Baum-Welch algorithm. in the forward-backward algorithm, $a_j(t)$ is the correct probability distribution, and $\beta_j(t)$ is the inverse probability distribution. the solution $a_j(t)$ with certain values consists in finding the state j of the hidden Markov model at time t [x_1, x_2, ..., x_T] gives a probability distribution [17].

$$a_j(t) = P(x_1, x_2 \ldots . x_t | state_t = j) \quad (9)$$

where $a_j(t)$ i $a_j(t-1)$ the quantities are related to an iterative expression:

$$a_j(t) = \left[\sum_{i=2}^{N-1} a_i(t-1)A_{i,j}\right] f_j(x_t) \quad (10)$$

where A_{ij} is the probability of transition from state i to state j, $f_j(x_t)$ is the probability of observing vector x in state j.

In the implicit Markov model, the inverse function βj(t) is the time t of the state j in [x_{t+1}, x_{t+2}, ..., x_T}] allows us to determine convergence in the sequence of observations and is determined by the formula[17]:

$$\beta_j(t) = P(x_1, x_2 \ldots . x_t | state_t = j) \quad (11)$$

where $\beta_j(t)$ va $\beta_j(t+1)$ the amounts are related in a similar way:

The values of $a_j(t)$ i $\beta_j(t)$ are equal to [x_1, x_2, ..., x_t]makes it possible to determine the state of the hidden Markov model at time t when observing the sequence and is calculated using the following formula.

$$L_j(t) = \frac{1}{P} a_j(t)\beta_j(t) \quad (12)$$

At the next stage of training, the Baum-Welch recovery algorithm allows you to overestimate the model parameters using the above expressions. Let R be a training sample, then the probability of transition from state i to state j is defined as [18]:

$$\tilde{A}_{i,j} = \frac{\sum_{r=1}^{R} \frac{1}{P_r} \sum_{t=1}^{Tr-1} a_i^r(t) A_{ij} f_j(x_{t+1}^r) \beta_j^r(t+1)}{\sum_{r=1}^{R} \frac{1}{P_r} \sum_{t=1}^{Tr} a_i^r(t) \beta_j^r(t)} \quad (13)$$

Each state J and each component M of the Gaussian mixture, the mathematical expectation, the covariance matrix and the weight are determined by the following expressions:

$$\hat{\mu}_{j,m} = \frac{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t) x_t^r}{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t)}$$

$$\hat{\sigma}_{j,m} = \frac{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t) x_t^r - \hat{\mu}_{jm}^r \left([(x)]_t^r - \hat{\mu}_{jm}^r\right)^T}{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t)} \quad (14)$$

$$\hat{w}_{j,m} = \frac{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t)}{\sum_{r=1}^{R} \sum_{t=1}^{Tr} L_{jm}^r(t)}$$

For high-quality training of the hidden Markov model, many samples of speech signal frames (MFCC parameters) in the amount of several tens or even hundreds of copies are required. It is also necessary to monitor the state of linear independence of the training samples, otherwise the covariance matrix will be violated in the learning process, which will lead to a complete failure of the model. To avoid this condition, it is advisable to constantly monitor the learning process[19]. When processing speech signals with hidden Markov models developed on the basis of these mathematical algorithms, the following requirements must be met:

- The choice of kepstral coefficients (MFCC) as parametric vectors in speech signal recognition.
- Development of an algorithm for normalization of parametric vectors;
- Choosing the number of m states of the N model and the components of the Gaussian algorithm.

It should be noted that the implicit Markov model does not have a universal algorithm for determining the above parameters, and each case has a high recognition accuracy depending on the problem being solved, many experiments may be required to achieve the result.

The MFCC parameters of each detected frame are set to ready for processing in an implicit Markov model, and processing is performed based on the underlying structure (Figure 7).

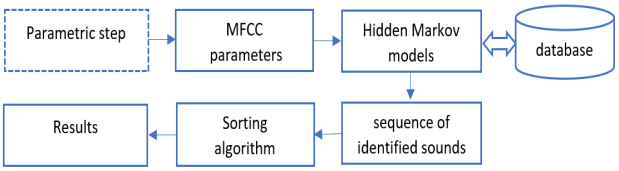


Fig. 7. An algorithm for recognizing speech information based on the Hidden Markov model.

In the structure, the MFCC parameters of each frame of the speech signal are entered as parameters into the Markov model. To increase the accuracy in this structure, the frames were worn 60% apart. This, of course, leads to an increase in the number of processing frames in the speech signal and an increase in processing time. It is proved that such sorting of frames gives high accuracy of experimental results [20]. The Markov algorithm performs the task of determining the correspondence of the obtained parameters to the parameters in the database and determines in which of the 29 specified states the MFCC parameters of the frame have the highest probability. As a result of algorithmic processing of the parameters of the MFCC, a certain sequence of sounds is formed (in the form of text).

These sound sequences are summarized using sorting algorithms. There are certain types of sounds in this that are discarded if their sequence is less than 15. If the number of frames exceeds 15, this set of sound sequences is returned as a result.

Of the 20 two-syllable words selected for the study, 16 were found clearly, and 4 were found indeterminately. There is one mistake in each of the vaguely defined words.

The MFCC parameters of each detected frame are set to ready for processing in an implicit Markov model, and processing is performed based on the underlying structure (Fig.7).

4. Speech recognition based on CNN

Convolutional Neural Networks (CNN) is also used in speech recognition systems. Convolutional neural networks are mainly designed for speech recognition and processing, and are also widely used in natural language processing and other fields. CNN networks allow you to maintain and effectively analyze the spatial structure of the input data.

- Convolutional layer: performs convolutional operations with input data. This layer analyzes the input data using small filters (cores).
- Activation Function: After each convolution, an activation function (for example, Relu) is applied, which introduces zero linearity.
- Pool layer: After convolution, layers of the maximum pool or average pool are usually applied, which reduces the spatial resolution and reduces the computational complexity of the model.
- Fully Connected (FC) layer: One or more fully connected layers are added after convolution, these layers are used to classify the results.
- Dropout: The method of accidental disconnection (dropout) of some neurons of the network is used to prevent overvoltage.

The principle of operation of a convolutional neural network is implemented in the following sequence.

1. Input data: CNN is usually designed for image processing, but can be processed as speech signal spectrograms or in other forms.
2. Convolutional layers: Each convolutional layer defines local properties by maintaining small filters for the input data. Filters slide over the image, creating dot multiplication and sums at each location.
3. Activation functions: After each convolution, an activation function (for example, ReLU) is applied, which adds zero linearity to the property map.
4. Pool Layers: Pool layers reduce spatial resolution and extract the most important features. For example, the max-pooling layer takes the highest value in a small area.
5. Fully connected layers: One or more fully connected layers are applied at the end, and these layers act as classifications.
6. Output layer: The last layer usually supports the SoftMax function, providing the classification result.

Convolutional neural networks (CNNs) are one of the main components of modern artificial intelligence and machine learning. They are highly accurate in performing many complex tasks such as image processing and speech recognition. CNN's work has a wide range of applications due to the effective analysis of spatial objects [21].

A neural network with two architectures is built in a speech recognition algorithm based on a convolutional neural network. The first architecture is based on the MFCC parameter of a speech signal with 12 input vectors and the FFT parameters of a speech signal with 128 input vectors. The neural network principle of the algorithm checks the result based on the MFCC parameter of the first speech signal. If the result meets the specified requirement i.e., above 90%, the result will be printed. Otherwise, it performs the computational process of a neural network based on the parameters of the FFT of the speech signal. Here the result is printed if it is 35% higher. Otherwise, the information in the form of "file error" will be printed.

These algorithms can be used not only to recognize children's speech pronunciation, but also to solve problems of recognizing Uzbek speech sounds, syllables and word content. The wide range of tasks solved by neural networks today limits the possibility of developing a functional, powerful, universal network with various algorithms.

Because each neural network uses different resources that do not match in the problems being solved. Therefore, when designing neural networks, the structure is developed depending on the type of problem being solved, as well as the scope of application. When developing this structure, the following approach was created.

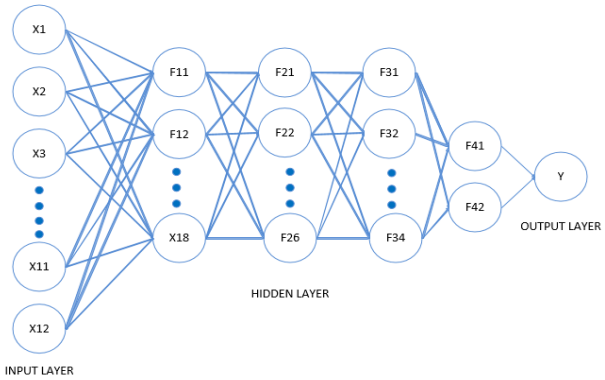


Fig. 8. The general structure of the neural network.

Speech word recognition used a multilayer perceptron neural network with a classical multilayer structure with the above-mentioned sequential connections and activation functions of a sigmoid neuron. The input layer of the network consists of 12 elements (MFCC parameters) $X_1,X_2....X_{12}$ has four hidden layers and consists of one output layer.

The first hidden layer is F_{1n}=8 elements, the second hidden layer is F_{2n}=6 elements, the third hidden layer is F_{3n}=4 elements, the fourth hidden layer is F_{4n} N=2 elements. These dimensions are determined based on experiments, and the size Y of the output layer always consists of 1 element. The output layer, equal to 1, is based on the fact that the child pronounces one word during the speech.

In the structure of a neural network, each synapse has its own synaptic connection or its weight. The current state of a neuron is determined by a randomly found sum of values at its input [19].

$$F_{i,N} = \sum_{i=1}^{n} x_i w_i \quad (15)$$

At the output of the neuron there is a function for its state:

$$Y = f(F_{i,N}) \quad (16)$$

One of the most common of these functions is a nonlinear function, that is, a logistic function in the form of F(X) or a sigmoid function

$$f(x) = \frac{1}{1+e^{-\alpha x}} \quad (17)$$

Reduction in the indicator α, the sigmoid moves to a position as if it is stretched, at α = 0 a horizontal line is formed, all points of which are equal to 0.5. and with an increase in the value of the pointer α, the function X = 0 at point T makes it possible to convert one into a function of a jump variable.

This activation function has the following advantages:

- this function is bipolar, and, accordingly, all signals in the neural network will also be bipolar, which will reduce the number of repetitions of the learning algorithm of this network;
- the hyperbolic tangent function is quickly calculated on a computer, which allows you to speed up the work of neural networks both in speech recognition mode and in learning mode.

The mathematical model of the neural network used in this paragraph is presented as follows [20]:

$$Y = f\left[\sum_{N=1}^{2} F_{4,N} f\left(\sum_{N=1}^{4} F_{3,N} f\left(\sum_{N=1}^{6} F_{2,N} f\left(\sum_{N=1}^{8} F_{1,N} X_1^{12}\right)\right)\right)\right] \quad (18)$$

where $F_{1,N}$, N are the neural cells of the hidden layer, X_1^{12}- are the MFCC coefficients , f is the activation function, y is the outgoing neural cell.

In the general structure of recognition of children's speech pronunciation, we can see that the spectra obtained on the basis of the Fourier transform algorithm are sent directly to the neural network. To do this, the structure of the neural network is based on the model below.

$$Y = f\left[\sum_{N=1}^{2} F_{4,N} f\left(\sum_{N=1}^{4} F_{3,N} f\left(\sum_{N=1}^{6} F_{2,N} f\left(\sum_{N=1}^{8} F_{1,N} X_1^{128}\right)\right)\right)\right] \quad (19)$$

where $F_{I,N}$ are the neural cells of the hidden layer, X_1^{128}- are the spectral coefficients, f is the activation function, Y is the outgoing neural cell.

In this formula, we see that the number of spectral coefficients is 128. This is due to the fact that the speech signal contained 256 values when divided into frames. When spectral values are obtained by the Fourier transform, 128 real frequencies and 128 abstract frequencies are obtained from each frame. When the spectral coefficients were aimed at the neural network, only the actual frequencies were obtained [21].

We can see the decision-making process in their neural network by taking the MFCC coefficients from each frame of the speech signal. Spectral values can also be determined by neural networks on this basis.

Based on the sequence of these algorithms, it is possible to determine how correctly the speech signal is recognized in the speech development of children (Table 2)

Table 2. the result of comparing artificial intelligence algorithms.

№	Speech signal type	DTW	HMM	NN
1.	Sound	73	77	87
2.	Syllable	74	81	95
3.	Word	82	85	91

The sequence of algorithms consists in making decisions on neural networks based on the distribution of the speech signal by parameters (MFCC and spectral parameters). At the same time, the probability that the speech signal will be correctly pronounced is 90% higher. This means that the sequence of algorithms for processing Uzbek speech characterizes the correct organization.

5. The effectiveness of speech recognition algorithms based on intelligent algorithms

It can be seen from the results of the analysis that the use of the Markov model is considered productive when recognizing words in Uzbek speech. The principle of word recognition based on parameterization of two- and three-syllable words of the Uzbek language is implemented. The work on the parameters of the speech signal was carried out in the Markov model as destructive values. When determining two-syllable words, out of 20 selected words, 4 were found vague, and the remaining 16 were clear. There is one mistake in each of the four words found ambiguously. No error was found in the three-syllable words. The degree of determination in processing Uzbek words based on the hidden Markov model gave an accuracy of 80-85%. Thus, the proposed model of processing Uzbek words can be assessed as effective. But the calculation takes a long time, and constant monitoring is necessary when learning speech information. Otherwise, this will lead to incorrect formation of the covariance matrix. This characterizes a high error rate.

6. Conclusion

According to the results of the analysis, it can be seen that from the artificial intelligence algorithms used to recognize Uzbek speech, neural networks turned out to be effective based on experimental results. It is also efficient with computational time from other artificial intelligence algorithms with the simplicity of the computational process in neural networks.

The accuracy of comparative indicators of artificial intelligence algorithms conducted in the research work was estimated as a percentage. This is due to the fact that the main goal was to determine the type of analyzed artificial intelligence algorithms that provide high accuracy. The main purpose of comparing the Markov chain, the DTW algorithm and neural networks is to check the correspondence of pointers to complexity:

- accuracy (must be above 90%);
- real-time compatibility;
- occupied memory capacity;
- simplicity of the algorithm.

Experiments have shown that there are certain requirements for the learning and testing process when working with neural networks. Therefore, this algorithm is more efficient than other artificial intelligence algorithms. Speech signals it is advisable to use neural network algorithms in solving field problems.

Acknowledgment

This paper was carried out at the Tashkent University of Information Technologies named after Muhammad al-Khorazmi in BV-Atex-2018-134—"Analysis and creation of software for speech signal recognition algorithms in digital signal processors" and 24/19-F "In the rehabilitation of speech defects in preschool and school-aged children" thanks for using the results of scientific research projects "development of computer programs".

References

[1] Abdullaeva, M., I. Khujayorov and M. Ochilov (2021). Formant set as a main parameter for recognizing vowels of the Uzbek language, International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2021, pp. 1-5.

[2] M. M. Mahmudovich, A. M. Ilkhamovna and T. B. Shukhrat Ogli, (2022). Image Approach to Uzbek Speech Recognition, IEEE 22nd International Conference on Communication Technology (ICCT), Nanjing, China, 2022, pp. 1201-1206.

[3] Musaev M., Abdullaeva M., Ochilov M. (2022). Advanced Feature Extraction “Method for Speaker Identification

Using a Classification Algorithm". AIP Conference Proceedings, 2022, pp 256-265.

[4] W. Chan (2016). Speech recognition with attention-based recurrent neural networks, US Patent 9,990,918, 2018.

[5] W. Chan (2016). Listen, attend and spell: A neural network for large vocabulary conversational speech recognition, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).— IEEE. 2016, pp. 4960—4964.

[6] W. Xiong, J. Droppo, X. Huang, F. Seide, M. Seltzer, A. Stolcke, D. Yu, and G. Zweig (2016) Achieving human parity in conversational speech recognition, Technical Report MSR-TR-2016 pp.71.

[7] O. Abdel-Hamid (2014) Convolutional neural networks for speech recognition, IEEE/ACM Transactions on audio, speech, and language processing. Vol. 22, 2014, pp. 1533––1545.

[8] Lama, P. (2010) Speech recognition with dynamic time warping using MATLAB, Project Report, CS 525, Spring 2010.

[9] B. W. Gawali. (2010) Marathi isolated word recognition system using MFCC and DTW features, Proc. of Int. Conf. on Advances in Computer Science. Vol. 1, Citeseer. 2010, pp. 21—24.

[10] Y. LeCun, Y. Bengio (1995). Convolutional networks for images, speech, and time series, The handbook of brain theory and neural networks Vol. 3361, no. 10, 1995.

[11] P. Ahmadi and M. Joneidi (2014). A new method for voice activity detection based on sparse representation, 2014 7th International Congress on Image and Signal Processing, Dalian, 2014, pp. 878-882.

[12] V. A. Volchenkov and V. V. Vityazev (2016) Development and testing of the voice activity detector based on use of special pilot signal, 5th Mediterranean Conference on Embedded Computing (MECO), Bar, 2016, pp. 108-111.

[13] Z. Fan, Z. Bai, X. Zhang, S. Rahardja and J. Chen (2019). AUC Optimization for Deep Learning Based Voice Activity Detection, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019, pp.

[14] Mirco Ravanelli, Philemon Brakel, Maurizio Omologo, and Yoshua Bengio, (2018) Light gated recurrent units for speech recognition, IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, pp. 92–102.

[15] D. Palaz, M. Magimai.-Doss, and R. Collobert (2015). Convolutional neural networks-based continuous speech recognition using raw speech signal, in Proc. of ICASSP, April 2015.

[16] S. M. Mon and H. M. Tun (2015). Speech-to-text conversion (STT) system using hidden Markov model (HMM), International Journal of Scientific & Technology Research, vol. 4, no. 6, Jun. 2015 pp.349-352.

[17] Savchenko V. V. (2017). Study of the stationarity of random time series using the principle of the information-divergence mini mum, Radiophysics and Quantum Electronics, vol. 60, no. 1, 2017, pp. 81—87.

[18] Pahini A. Trivedi (2014). Introduction to Various Algorithms of Speech Recognition: Hidden Markov Model, Dynamic Time Warping and Artificial Neural Networks, International Journal of Engineering Development and Research, Volume 2, Issue 4, 2014.

[19] G. Harsha Vardhan, G. Hari Charan (2014). Artificial Intelligence & its Applications for Speech Recognition, International Journal of Science and Research (IJSR) Volume 3 Issue 8, August 2014.

[20] Weng C., Yu D., Seltzer M. L., Droppo J. (2014). Single-channel mixed speech recognition using deep neural networks, IEEE ICASSP. 2014, pp. 5632-5636.

[21] Geoffrey Hinton, Li Deng, Dong Yu, George Dahl, Abdel-rahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Tara Sainath, and Brian Kingsbury, (2012). Deep Neural Networks for Acoustic Modeling in Speech Recognition" - IEEE, Signal Processing Magazine, 2012.

[22] Shaw Talebi. (2020). The Fast Fourier Transform (FFT)", Published in The Startup 7 min read Dec 4, 2020.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.3

Investigation of a Precise Positioning System for Earth-moving and Construction Machines

Tatyana Golubeva

Institute of Information Technologies AUPET named after G.Daukeyev, Baitursynuly 126/1, 050013, Almaty, Kazakhstan,

e-mail: t.golubeva@aues.kz.

Abstract: The paper discusses a precise positioning model for earth-moving and construction machines (ECM) based on differential correction techniques. The proposed algorithm incorporates both a least squares approach and an iterative method. An opportunity of system implementation is illustrated by the case of an iron ore mine in Kazakhstan, including the selection of the base station and repeater locations.

Received 3 September 2024
Accepted 12 October 2024
Published 9 December 2024

Keywords: earth-moving, construction machines, precise positioning system.

1. Introduction

At first glance, precise positioning of earth-moving and construction machines may seem like a straightforward task. However, due to ionospheric and tropospheric errors, the problem becomes non-linear, leading to significant positioning inaccuracies. For ECMs operating in open-pit mines and for surveyors, centimeter-level precision is required, with differential correction methods being employed [1]. A dedicated base station (or multiple) is installed alongside the mine at a location with known coordinates. The correction data from this station is then incorporated into the navigation solution for precise positioning of ECMs. To ensure real-time high-precision positioning of ECMs, a math model based on fundamental principles is considered [2].

Precise positioning of ECMs for the system to be investigated is carried out by applying the specialized satellite receivers designed to measure both the signal propagation time from multiple satellites to the receiver and the signal phase at a carrier frequency. The receiver based on a unidirectional measurement method is implemented. Multiple receivers installed on closely located ECMs can operate simultaneously, each receiver measuring signals independently.

Higher precision is provided by multiple receivers obtaining the same signal from each visible satellite with differences in phase. If any receiver is placed stationarily at a location with known coordinates, positioning of the remaining ones can be performed relative to this stationary receiver with an accuracy of up to several millimeters [3].

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

2. Material and methods

Pseudorange (code-based) measurements are characterized by the ability of a receiver to directly determine the signal propagation time based on knowledge of the signal transmission time and the determination of the signal reception time [4]. Multiplying signal propagation time by the signal propagation speed, i.e. the speed of light, yields the desired unambiguous pseudorange value. To obtain the geometric distance between the satellite and receiver, appropriate corrections are applied to the recorded pseudorange value. Since code signals are transmitted from the satellite through a carrier wave modulation, they are characterized by a group propagation speed. This factor must be taken into consideration when determining the time delays of radio signals as they propagate through a dispersive medium such as the ionosphere.

Based on the fundamental equations of pseudorange and actual range in satellite navigation [5] further analysis is conducted:

- the pseudorange equation for the i-th satellite differs from the actual range by an error term (satellite clock error, receiver clock error, signal propagation deviation etc):

$$P_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} + D, i$$

$$P_i = \overline{1, M} \quad (1)$$

- the corresponding actual range equation is given as follows:

$$R_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} \quad (2)$$

To determine coordinates, at least four satellites are required, yielding a system of four equations with four unknowns. Since this system is nonlinear due to the fact that the error (D) is unique for each satellite, the least squareы method is applied [6]. The least squareы objective function is formulated as follows:

$$F = \sum_{i=1}^{M} f_i^2 = \sum_{i=1}^{M} (R_i + D - P_i)^2 \to min \quad (3)$$

To find the minimum, first derivative is taken with respect to each variable, yielding:

$$\begin{cases} 2\sum_{i=1}^{M}(R_i + D - P_i)\frac{1}{R_i}(x - x_i) = 0 \\ 2\sum_{i=1}^{M}(R_i + D - P_i)\frac{1}{R_i}(y - y_i) = 0 \\ 2\sum_{i=1}^{M}(R_i + D - P_i)\frac{1}{R_i}(z - z_i) = 0 \\ \sum_{i=1}^{M}(R_i + D - P_i)\frac{1}{R_i} = 0 \end{cases} \quad (4)$$

Further, a system of nonlinear algebraic equations, comprising four equations for a single satellite is considered. For solving the system an initial approximation is defined, and the equations are expanded in Taylor series around the chosen initial approximation, yielding the following:

$$\sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(x^k - x_i) + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(x^k - x_i) + (R_i(x^k, y^k, z^k, D^k) + D - P_i))\Delta x + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(y^k - y_i)(x^k - x_i)\Delta y + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)(x^k - x_i)\Delta z + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)}\Delta D = 0 \quad (5)$$

$$\sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(y^k - y_i) + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(y^k - y_i)\Delta x + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(y^k - y_i)(y^k - y_i) + (R_i(x^k, y^k, z^k, D^k) + D - P_i))\Delta y + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)(y^k - y_i)\Delta z + \sum_{i=1}^{M}\frac{(y^k - y_i)}{2R_i(x^k, y^k, z^k, D^k)}\Delta D = 0 \quad (6)$$

$$\sum_{i=0}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(z^k - z_i) + \sum_{i=0}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(z^k - z_i)\Delta x + \sum_{i=0}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(y^k - y_i)(z^k - z_i)\Delta y + \sum_{i=0}^{M}\left(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)(z^k - z_i) + (R_i(x^k, y^k, z^k, D^k) + D - P_i)\right)\Delta z + \sum_{i=0}^{M}\frac{(z^k - z_i)}{2R_i(x^k, y^k, z^k, D^k)}\Delta D = 0 \quad (7)$$

$$\sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i) + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)\Delta x + (\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(y^k - y_i)\Delta y + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)\Delta z + \sum_{i=0}^{M}\frac{(z^k - z_i)}{2R_i(x^k, y^k, z^k, D^k)}\Delta D = 0, \quad (8)$$

where "k" denotes the approximation index, and Δx, Δy, and Δz represent differences between the coordinate values from the previous and current iterations of the system's solution.

To simplify the system of equations, matrix form is employed, namely:

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix} \begin{bmatrix} \Delta x \\ \Delta y \\ \Delta z \\ \Delta D \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}, \quad (9)$$

where:

$$a_{1,1} = \sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(x^k - x_i) + \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(x^k - x_i) + (R_i(x^k, y^k, z^k, D^k) + D - P_i));$$

$$a_{1,2} = \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(x^k - x_i);$$

$$a_{1,3} = \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)(x^k - x_i);$$

$$a_{1,4} = \frac{(x^k - x_i)}{2R_i(x^k, y^k, z^k, D^k)};$$

$$a_{2,1} = \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(x^k - x_i)(y^k - y_i);$$

$$a_{2,2} = \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(y^k - y_i)(y^k - y_i) + (R_i(x^k, y^k, z^k, D^k) + D - P_i));$$

$$a_{2,3} = \sum_{i=1}^{M}(\frac{1}{2R_i(x^k, y^k, z^k, D^k)} 2(z^k - z_i)(y^k - y_i);$$

etc.,

$$b_1 = \sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(x^k - x_i);$$

$$b_2 = \sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(y^k - y_i);$$

$$b_3 = \sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i)(z^k - z_i);$$

$$b_4 = \sum_{i=1}^{M}(R_i(x^k, y^k, z^k, D^k) + D - P_i);$$

The solution of the system is performed by an iterative method via successive approximations until the deltas become less than 0.001.

The algorithm is as follows: an initial approximation is set, then the elements of matrix A and vector b are calculated, and finally the next approximation is determined.

$$x^{k+1} = x^k + \Delta x; \quad (10)$$

$$y^{k+1} = y^k + \Delta y; \quad (11)$$

$$z^{k+1} = z^k + \Delta z; \quad (12)$$

$$D^{k+1} = D^k + \Delta D. \quad (13)$$

3. Results and discussion

Based on the conducted mathematical modelling, a feasibility of precise positioning system implementation for earth-moving and construction machines is illustrated by the case of an iron ore mine in Kazakhstan.

In the light of current study, a site alongside an iron ore mine must be selected and a continuously operating base station must be installed onsite to perform differential correction. This stage is essential for the comprehensive implementation of automation in the operation of ECM and other users. An installation of a base station will substantially enhance both the precision and timeliness of determining ECM's position in real time. The continuously operating base station will collect both code and phase data from satellite navigation systems and transmit data to the receivers of ECMs and other users.

Moreover, the existing local coordinate system at the iron ore mine should be taken into account, which has previously served as the basis for large-scale surveys of the quarry at various scales. The shape of the iron ore quarry at the surface is roughly circular with a diameter of 3 km and depth of 700 meters.

Taking into account the terrain and the existing buildings and structures adjacent to the iron ore quarry, to establish the high-precision positioning system, comprising three primary network stations for ECM is expedient, with one station being the base. This number of network stations is considered to be sufficient for both the establishment and subsequent operation of the positioning system over an area of approximately 7.6 square kilometers at the iron ore quarry.

Further, the station layout is examined in detail. The base station should be located at the only viable option - the existing ore management building. This placement is optimal, as the ore management building is the only site within the quarry that is secured continuously (24/7). In addition to providing security, this location will reduce costs associated with the installation and operation of the sensitive and expensive equipment within the base station. The second and third network stations should be placed at the existing points of the local geodetic network within the iron ore quarry. Furthermore, all three stations should be positioned at a considerable distance from one another and, preferably, at approximately equal intervals, since satellite navigation measurements rely on a network adjustment method for the precise determination of coordinates [7]. Accordingly, the second and third stations should be placed at two points of the local geodetic network within the iron ore quarry, as shown in Figure 1.

All three stations satisfy the requirements for satellite geodetic network stations, as each offers an unobstructed view of the sky for satellite reception.

In Fig. 1, the base station of the precise positioning system for ECM is represented by a small triangle, the two remaining network stations are denoted by squares, and the existing points of the local geodetic network within the iron ore quarry are indicated by circles.

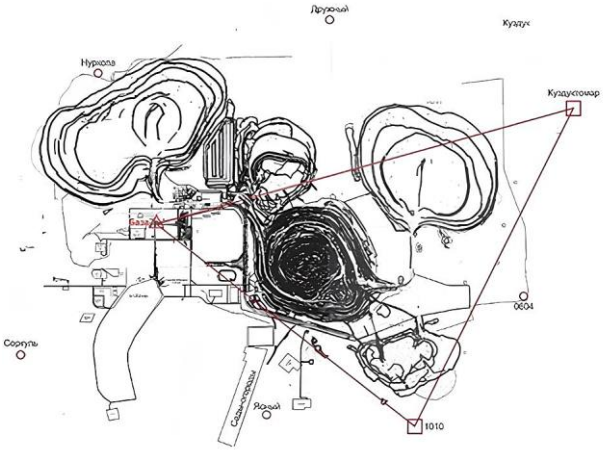


Fig. 1. Placement of network stations.

Mounting the base station tower on the ore management building complies fully with the recommendations [8, 9]. The ore management building is a reinforced concrete structure built more than 15 years ago. No visible signs of foundation damage or wall cracks are observed in the building. It's worth mentioning that the ore management building is ideally located, being suited at a considerable distance from both the quarry blasting sites and the railway tracks.

Within the ore management building itself, when installing the base station, a number of requirements should also be taken into account. To reduce measurement errors in pseudoranges caused by noise in the base station receiver's signal path, antenna cable length must be minimized. The receiving antenna must be positioned in an area free from obstructions for clear satellite signal reception and must be installed at an elevation of more than 10° above the horizon—for instance, on the building's roof. At the same time, convenient access to the antenna for operation and maintenance should be ensured. Based on these requirements, mounting the antenna on the load-bearing wall of the ore management building is proposed, taking into account the placement of the satellite receiving equipment, as shown in Fig. 2.

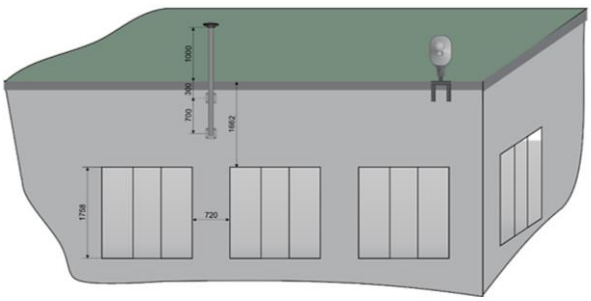


Fig. 2. Mounting the base station on the ore management building.

However, the ore management building is located at a considerable distance from the edge of the quarry, and the same applies to the two other network stations. Moreover, to maintain continuous communication with ECMs at the lower part of the quarry and to refine the differential

correction signals they receive, a repeater at the quarry's edge should be installed to retransmit these signals. The repeater may be placed on the dispatch building situated at the quarry's edge [10]. Frequent blasting operations at the iron ore quarry forbid installation of the base station's navigation unit alongside the quarry's edge, as the resultant soil vibrations significantly disrupt the relative determination of the phase center's coordinates in the receiving antenna at the ground station. The existing antenna mast of the dispatch building is considered optimal for installing the repeater, as it facilitates high-precision satellite measurements on the slopes and floor of the iron ore quarry and ensures the transmission of differential corrections via signals retransmitted by GSM and VHF repeater antennas from the quarry's edge.

When placing the repeater at the edge of the quarry, the repeater's receiving antenna must be oriented toward the dispatch tower by tilting it. A secondary radio communication zone should be provided by the transmitting antenna. Additionally, the repeater must be installed at an elevated position if it is located at a considerable distance from the dispatch tower, as shown in Fig. 3.

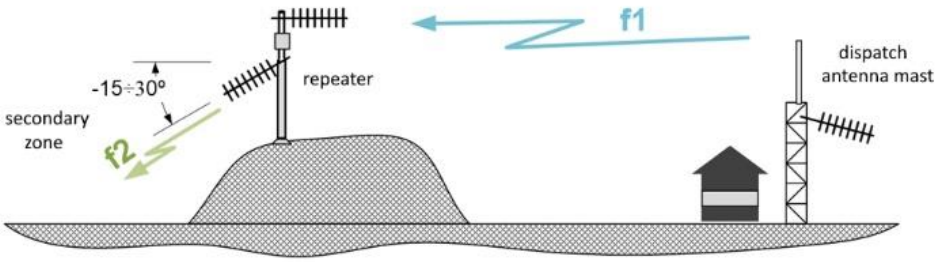


Fig. 3. Orientation of the repeater antennas when installed on spoil heaps.

When installing the repeater at the edge of the iron ore quarry, the antennas should be set with an inclination of approximately +30° (for frequency f1) and –30° (for frequency f2), respectively. (Fig. 4).

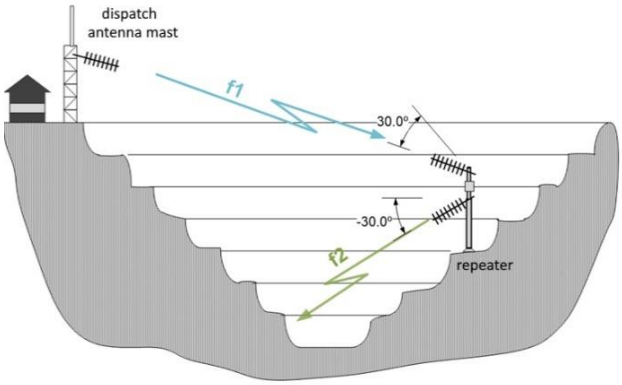


Fig. 4. Orientation of the repeater antennas when installed within the quarry.

4. Conclusion

The results of mathematical modlling demonstrate the feasibility of developing an effective and precise positioning system for ECMs based on differential correction. The proposed system will enhance both the accuracy and timeliness of ECM control, thereby increasing productivity and operational safety.

References

[1] Yehuda Bock and Diego Melgar (2016). Rep. Prog. Phys. 79 106801, DOI 10.1088/0034-4885/79/10/106801.

[2] Seeber, Günter (2003). Satellite Geodesy, Berlin, New York: De Gruyter. https://doi.org/10.1515/9783110200089.

[3] Pearlman, M., Arnold, D., Davis, M. et al. (2019). Laser geodetic satellites: a high-accuracy scientific tool. J Geod 93, 2181–2194. DOI: 10.1007/s00190-019-01228-y.

[4] Ahmadi, S. A., Mohammadzadeh, A., Yokoya, N., & Ghorbanian, A. (2024). BD-SKUNet: Selective-Kernel UNets for Building Damage Assessment in High-Resolution Satellite Images. Remote Sensing, 16(1), 182. https://doi.org/10.3390/rs16010182.

[5] Theurl, F., Schmied, C., Reitbauer, E., & Wieser, M. (2023). Automated Route Planning from LiDAR Point Clouds for Agricultural Applications. Engineering Proceedings, 54(1), 54. https://doi.org/10.3390/ENC2023-15448.

[6] Pupillo, G., Righini, S., Orosei, R., Bortolotti, C., Maccaferri, G., Roma, M., Mastrogiuseppe, M., Pisanu, T., Schirru, L., Cicalò, S., Tripodo, A., Harju, J., Penttilä, A., Virkki, A. K., Bach, U., Kraus, A., Margheri, A., Ghiani, R., Iacolina, M. N., ... Sessler, G. (2024). Toward a European Facility for Ground-Based Radar Observations of Near-Earth Objects. Remote Sensing, 16(1), 38. https://doi.org/10.3390/rs16010038.

[7] Verdu-Candela, A., Femenia-Ribera, C., Mora-Navarro, G., & Sierra-Requena, R. (2023). Implementation of Web Map Services for Old Cadastral Maps. ISPRS International Journal of Geo-Information, 12(10), 413. https://doi.org/10.3390/ijgi12100413.

[8] Špoljar, D., Štajduhar, I., Lenac, K., & Filjar, R. (2021). A Predictive Model of Multipath Effect Contribution to GNSS Positioning Error for GNSS-based Applications in Transport and Telecommunications. The Journal of CIEES, 1(2), 7–13. DOI:10.48149/jciees.2021.1.2.1.

[9] T. A. Herring (1999). Geodetic applications of GPS, in Proceedings of the IEEE, vol. 87, no. 1, pp. 92-110, Jan. 1999, DOI: 10.1109/5.736344.

[10] W. S. Parker and R. G. Bartholomew, "Mapping, charting, and geodesy in the DoD standard GPS receivers," IEEE PLANS '88.,Position Location and Navigation Symposium, Record. 'Navigation into the 21st Century'., Orlando, FL, USA, 1988, pp. 145-152, doi: 10.1109/PLANS.1988.195477.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.4

Design and Simulation of a PV System under Different Operating Conditions

Todor Todorov
AC DC ENERGY LTD, 1 Nikola Gabrovski Str., 1000 Sofia, Bulgaria

tn_todorov@abv.bg

Abstract: Over the past few years, the installed power of wind and photovoltaic power plants in Bulgaria has been significantly increased. The aim of this article is to proposes a methodology for the design and construction of a stationary 75kWp photovoltaic power plant, connected to the public grid at the MV level through a CSS (0.4/21 kV). The proposed design methodology is convenient and easy to implement, and the results of practical construction show that the difference between the estimated and the obtained electricity production is less than 5%. It has been found that two main factors have the strongest impact on the electricity production - the pollution of the surface of the modules (i.e. field dust, bird droppings etc.) and the ambient temperature. Reducing their impact can be achieved by using a cleaning and cooling system with temperature feedback, which would lower the operating temperature of the modules from 80-85°C to 47°C /NOCT/. The results of the simulation studies performed show that this would increase electricity production by about 20%, which would compensate for the degradation of the photovoltaic modules.

Keywords: PV systems, power plant, Operating Conditions, MPPP, electricity production.

Received 23 August 2024
Accepted 10 October 2024
Published 20 December 2024

1. Introduction

Over the past decade, photovoltaic systems (PV) have entered the energy market and have established themselves as the preferred technology for decentralized power generation in more and more countries and regions due to their modularity and flexibility. The share of solar electricity in the energy resource portfolio has been steadily increasing due to the possibility of free use of the available solar resource, the minimal costs of operation and maintenance of photovoltaic plants, and clean and safe electricity generation [1]. The dynamic growth of the photovoltaic (PV) sector in the United Europe over the past decade has been largely supported by the favorable regulatory framework and incentive mechanisms applied to renewable energy sources. Despite the rapid development of the solar industry in recent years and technological innovations in this area, PV projects are still associated with significant capital investments, and because the results of the investment are realized over a long period of time, the future efficiency of the systems largely depends on the precise assessment of the investment idea and good planning and management of the project initiatives. Regardless of Europe's priority goal of creating a competitive, sustainable, and secure energy supply, economic reasons force the Bulgarian government to frequently change its regulatory framework related to renewable energy sources and to strive to limit the more expensive energy solutions, including PV, despite their long-term beneficial effect [2]. This circumstance further emphasizes the need for a detailed assessment and quality investment analysis of PV projects, to achieve the investor's goals and achieve the desired economic result in conditions of uncertainty.

Regardless of the relevance and importance of the issues related to the assessment, planning, and management of capital investments in solar power installations, some of their theoretical and practical aspects remain insufficiently studied and investigated, due to the relative novelty of technological solutions for the Bulgarian scientific and applied reality. The features of PV and the trends in solar electricity production, which define this type of solar installation as a specific object of management, have not been systematized and clarified in detail. The main problems related to the assessment and planning of PV projects have not been identified, and there are no specific guidelines for solving them. No scheme has been developed to present the sequence and connections between the activities for organizing the preparation and implementation of the variety of projects for electricity production from PV [3]. The issues related to models for forecasting the amount of electricity produced have not been studied in a sufficiently comprehensive manner. The methods and tools for analyzing and assessing the economic efficiency of capital investments in PV are not sufficiently adapted to practice [4]. At this stage, there are no comprehensive methodological guidelines that would describe the sequence of analytical and evaluation actions

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

preceding the implementation of a PV project, which would enable entrepreneurs to improve management and increase the effectiveness of the project initiative.

2. Methodology

In order to achieve maximum electricity production from photovoltaic modules, it is necessary to calculate the optimal installation angle [5]. An algorithm calculated with the MathCAD program is used:

$$J(D) = 360.\frac{D}{365}, \quad (1)$$

where: D is the day of the year.

Declination of the Sun:

$$\delta j = (0.3948 - 23.2559\cos(J + 9.1) - 0.3915\cos(2.J + 5.4) - 0.1764\cos(3.J + 105.2). \quad (2)$$

Time equality:

$$Zglj = [0.0066 + 7.3525\cos(J + 85.9) + 9.9359\cos(2.J + 108.9) + 0.3387\cos(3.J + 105.2). \quad (3)$$

From the mean European time MEZ and the longitude λ of the location, the mean time of the location is determined:

$$MOZ = MEZ - 4.(15° - \lambda), \text{ min} \quad (4)$$

where:

MOZ is the mean time of the location [min];

MEZ is the mean European time [min];

λ=42.18o- longitude.

The astronomical time of a place is determined by the:

$$WOZ = MOZ - Zglj \quad (5)$$

φ=25.13° is the latitude.

With the latitude φ of the location and the hour angle ω, given by:

$$\omega = (12 - \frac{WOZ}{60}).15 \quad (6)$$

The Sun's altitude γs and the solar azimuth αs are obtained:

$$\gamma s = \arcsin(\cos\omega.\cos\varphi.\cos\delta + \sin\varphi.\sin\delta), ^o \quad (7)$$

$$\alpha s1 = 180 - \text{acos}\,(\frac{\sin(\gamma_s).\sin(\Phi) - \sin(\delta_j)}{\cos(\gamma_s).\cos(\Phi)}) \quad (8)$$

$$\alpha s2 = 180 + \text{acos}(\frac{\sin(\gamma_s).\sin(\Phi) - \sin(\delta_j)}{\cos(\gamma_s).\cos(\Phi)}) \quad (9)$$

Formula (8) gives us the change in the solar azimuth for the time before 12 hours, and formula (9) gives us the change for the time after 12 hours [6]. Using the MathCAD software and the "if" function in it, this calculation is performed automatically according to formula (10):

$$\alpha s = \text{if}(WOZ < 12, \alpha s1, \alpha s2). \quad (10)$$

There are two angles of tracking the movement of the Sun: θ_{sl1} and θ_{sl2}. θ_{sl1} is determined by the rotation of the Earth around its axis and changes by 15° per hour. θ_{sl2} is determined by the height of the Sun according to the formula:

$$\theta_{sl2} = 90 - \gamma s, \quad (11)$$

Where γs is the altitude of the Sun, determined by (7).

Since the photovoltaic park will be built with fixed panels, we perform optimization based on the height of the Sun γs for 12 o'clock, when the intensity of solar radiation reaches its maximum. The photovoltaic modules will be installed with their working surface facing south, and at 12 o'clock the deviation from θsl1 is zero and the panel is perpendicular to the Sun. Fig 1. presents the change in γs for each day of the year.

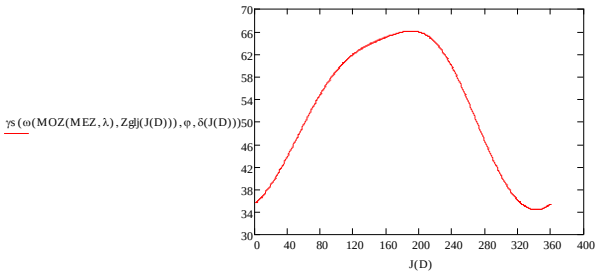


Fig.1. Deviation of γs during the year -at 12h.

Based on the data obtained from Fig. 2. we can determine the average angle at which the photovoltaic module should be fixed at 12h for each of the months of the year.

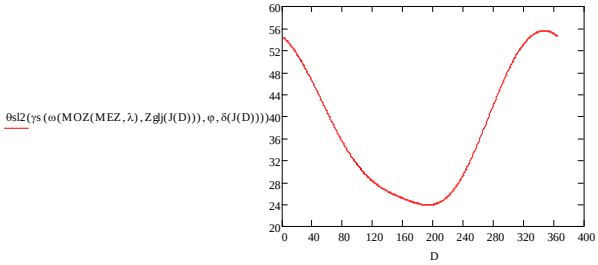


Fig.2. Deviation of Θ_{sl2} during the year- at 12h.

This angle is given by the formula:

$$\Theta sl1n - av. = \frac{\sum_1^m \Theta sl1}{\sum_1^m D} \quad (11)$$

Where:

$\Theta_{sl1n\text{-}av}$ is the average angle at which the photovoltaic module should be fixed,

n is the the number of the month of the year, n takes values from 1 to 12;

m is the number of days in the month, m takes values from 1 to 31;

D is the day of the year.

The simulated results are presented in Table 1.

Table 1. Results for $\Theta_{sl1n\text{-}av}$ for the months.

Month	$\Theta_{sl1n\text{-}av}$	Month	$\Theta_{sl1n\text{-}av}$
January	51.76	July	24.13
February	44.63	August	27.13
March	36.68	September	35.03
April	30.24	October	45.13
May	26.69	November	52.94
June	24.75	December	55.29

Table 2 presents meteorological data on direct and diffuse irradiation by month for the area where the photovoltaic park will be built.

Table 2. Direct (Edir) and diffuse (Ediff) irradiation.

Month	Edir (kWh/m^2)	Ediff (kWh/m^2)
January	51	29
February	64	36
March	97	57
April	140	68
May	167	88
June	172	88
July	175	96
August	160	77
September	123	56
October	85	45
November	50	30
December	44	24

Using the data from Table 1. and Table 2, the optimal angle for mounting the modules is determined - Θmont. =33º.

2.1. Determining the minimum distance between rows

The distance between the strings is determined using the formula:

$$h = l\sin(\Theta\text{mont.}) \quad (12)$$

where:

h is the height between the plane of the lower and upper ends of the module

l is the the length of the photovoltaic module; l=1.957m.

Θmont. =33º angle at which the panels are mounted.

h=1.957.sin(33)=1.067 m

$$h = l1.sin(\gamma s - av.) \quad (13)$$

where: $l1$ is the distance from the top of the panel to the end of the shadow that is produced at an angle γs-av;

$$l1=\frac{h}{\sin(\gamma_{s-av})} \quad (14)$$

Consequently, the minimum distance X between the strings can be determined by the formula:

$$X = l1.\cos(\gamma s - av.). \quad (15)$$

Thus:

$$X = \frac{h.\cos(\gamma_{s-av})}{\sin(\gamma_{s-av.})} = h.\text{cotg}(\gamma s - av.) \quad (16)$$

Table 3 presents the values of γs-av. For 12h for each of the months, and Table 4 for minimum distance X.

Table 3. Mounty results for γs-av.

Month	γs-av.
January	38.245
February	45.371
March	53.402
April	59.796
May	63.308
June	65.251
July	65.867
August	62.875
September	54.975
October	44.875
November	37.060
December	34.709

Table 4. Mounty results for minimum distance X.

Month	X, m
January	1.354
February	1.053
March	0.792
April	0.621
May	0.5365
June	0.492
July	0.478
August	0.547
September	0.748
October	1.072
November	1.413
December	1.482

Therefore, the minimum row spacing calculated for angle γs-av at 12h is 1.482 m. A spacing of 2.66 m is chosen to allow the use of mechanized equipment between the rows.

2.2. Determination of the annual production from the photovoltaic park

The production of electricity from PV systems depends on a number of factors that must be considered before starting the design: solar radiation, type of modules, operating temperature, V-A characteristic, pollution, optical losses, etc.

The initial approximate analysis in the design of PV systems is based on the peak solar power hours (PSH) indicator [7], which represents the equivalent of one day. This approach is used in the preliminary estimation of the parameters of PV systems that do not have solar concentrators.

The meaning of PSH for one day is equal to the amount of solar radiation accumulated throughout the day relative to the accepted standard value of 1000W/m^2. This parameter measures time and when expressed in hours it has the same numerical value as the total daily radiation measured in kWh/m^2 [8].

Thus, the approximate annual energy production from the PV system can be forecasted as:

$$X = \frac{h.\cos(\gamma_{s-av})}{\sin(\gamma_{s-av.})} = h.\text{cotg}(\gamma s - av.) \quad (17)$$

$$EA = \sum_{i=1}^{365}(PSH)_i \,.\, P0 \quad (18)$$

where:

(PSH)i- the value of the parameter PSH for the i-th day of the year

P0- nominal installed power of the system under standard conditions.

For systems operating at the maximum power point MPP, the instantaneous output power relative to the maximum $\frac{P_A}{P_{max}}$ depends on temperature and solar radiation, and therefore equation (18) is only an approximate estimate. A more accurate prediction can be made using a model that takes into account the ambient temperature, the temperature of the modules through the NOCT parameter (normal operating cell temperature) and the temperature coefficient of the modules.

2.Results and analysis

The photovoltaic modules chosen by the investor are CNBM Solar Polycrystalline Series III -260 W. Photovoltaic panels can be connected in parallel or in series depending on the requirements of the device to which they will be connected.

Up to 5 strings can be connected to each inverter. In the inverter, all incoming strings are connected in parallel to common buses – bus "+" and bus "-", using standard MC-4 type connectors. A mandatory condition for the normal operation of the inverter is that all strings have the same number of photovoltaic modules, that they are of the same type with the same unit nominal power, voltage and current and that they are mounted at the same angle to the ground. If possible, the wires connecting the individual strings to the inverter should have the same parameters.

To protect the wires and photovoltaic modules on the DC side, a string box is installed. One, two or more strings can be combined in the string box, depending on the installed power and the selected configuration. It installs a DC disconnector, two DC fuses with a fusible silver insert, respectively for "+" and "-", and a cathode arrester.

Conventional means of automatically shutting down the power supply in emergency mode rely on maximum current protection. Since PV systems are current limited, this makes conventional protections difficult to apply. The short-circuit current is slightly higher than the maximum operating current, so in this case the protection will not work.

Ground leakage can be caused by a number of reasons: damaged insulation, faulty installation, corrosion, etc. In PV systems where the negative is not grounded, a fault will only occur when both conductors leak to ground or the structure on which the modules are mounted. With appropriate placement of the conductors, this type of damage can be minimized.

Significant differences in the voltages of the individual strings at idle, when the inverter is off, can cause equalizing currents to flow. The most common reasons are: shading, partial covering of the modules with snow, damaged module.

Figure 3 shows an example of a ground fault. Three parallel strings connected to common poles "+" and "-" are shown. Under normal operating conditions, the maximum current in each string conductor is equal to the I_{sc} of the modules used.

In this system, which is not grounded by principle, we consider a case when a connection occurs between the negative pole and ground. We assume that this is the first failure and this does not affect the operation of the string. After some time, when a second leakage occurs to ground / in t. x / - which is at a potential different from that of the negative pole, a short-circuit current will flow.

In the diagram shown in Fig. 3, a reverse current flow through some of the PV modules in the damaged string. The magnitude of this current is the same as that of the current flowing through the string cable:

$I_R=(n-1).I_{sc}$, where n is the number of parallel connected strings.

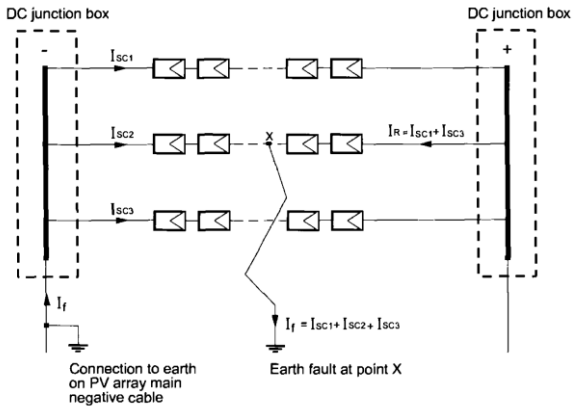


Fig.3. Ground fault.

The reverse current flowing through the modules can cause damage to them and increases the risk of fire. The high temperatures due to the reverse current lead to desoldering and delamination of the individual cells of the PV module.

The estimated yields (Table 4) assumed in the design of the power plant (Fig. 4) are presented in the tables below.



Fig.4. The designed PV system.

Table 5. Mounty estimated yields in the designed PVS.

Month	PSH/h	Electricity produced kWh
January	51	3818.88
February	64	4792.32
March	97	7263.36
April	140	10483.20
May	167	12504.96
June	172	12879.36
July	175	13104.00
August	160	11980.80
September	123	9210.24
October	85	6364.80
November	50	3744.00
December	44	3294.72
Annually		99440.64

Using the SolarLog 500 control and monitoring system, the actual production for the observed period was recorded (Table 6 and Table 7).

Table 6. Actual electricity generation.

Month	Generated energy for the month kWh/kWp	Electricity produced kWh
January	52.07	4165.50
February	83.72	6697.93
March	101.64	8130.87
April	106.31	8504.89
May	143.43	11474.59
June	132.87	10629.75
July	143.89	11511.35
August	147.83	11829.69
September	110.29	8823.24
October	76.25	6099.90
November	43.53	3482.00
December	36.59	2927.22
Annually		94276.93

Table 7. Ratio between achieved and projected results.

Month	Estimated production kWh	Electricity produced kWh	Difference in percentages %
January	3818.88	4165.50	109.08
February	4792.32	6697.93	139.76
March	7263.36	8130.87	111.94
April	10483.20	8504.89	81.13
May	12504.96	11474.59	91.76
June	12879.36	10629.75	82.53
July	13104.00	11511.35	87.85
August	11980.80	11829.69	98.74
September	9210.24	8823.24	95.80
October	6364.80	6099.90	95.84
November	3744.00	3482.00	93.00
December	3294.72	2927.22	88.85
Annually	99440.64	94276.93	94.81

After analyzing the results from above tables, it is seen that despite the large deviations in some months from +39.76 % to -18.87% on an annual basis, the electricity produced is only 5.19% less than previously planned.

The preliminary forecast does not take into account losses in the wires, and the SolarLog 500 system only measures losses in the inverter and the DC network from the photovoltaic modules. In order to get an accurate idea of the real amount of losses in the entire system, a comparison must be made between the readings of the outgoing electricity meter and the data from the SolarLog 500.

3. Conclusions

The comparative analysis of the results shows that:

▪ The performance of the photovoltaic installation is high when all PV modules are illuminated evenly, with the maximum amount of solar radiation.

▪ The serial connection of PV modules in a string increases the voltage to the required level for connection to the power grid. On the other hand, optimization of the installed power capacity is possible by changing the orientation of the modules and the connection between the modules.

▪ The fluctuation of the generated power by the photovoltaic modules is a major problem affecting the yield of electrical energy.

▪ The frequent switching of the photovoltaic system due to shading of the PV modules is associated with the operation of the inverter in a nonlinear section of the operating characteristic, giving rise to transient processes. This worsens the electrical parameters of the output voltage and current. Higher harmonics appear in the spectrum of the output indicators and additional reactive components, leading to power loss.

▪ The operability of the synthesized models is proven by comparing the theoretical and experimental results.

On an annual basis, the difference between the actual and forecasted amounts of electricity is only 5.19%. Future studies should focus on accounting for losses in wires, switching, and protection equipment.

References

[1] Keseev, V. (2022). Problems and Opportunities for Cost-Effective Photovoltaic Systems for Private Use. The Journal of CIEES, 2(1), 21–24. DOI: 10.48149/jciees.2022.2.1.4.

[2] V. Zinoviev, D. Koeva and Z. Ivanova, (2024). Charging Infrastructure and E-mobility Integration: Economic and Energy Benefits for Sustainable Grid Management, 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, 2024, pp. 1-4, doi: 10.1109/CIEES62939.2024.10811424.

[3] Koeva, D., Kutkarska, R., & Zinoviev, V. (2023). High Penetration of Renewable Energy Sources and Power Market Formation for Countries in Energy Transition: Assessment via Price Analysis and Energy Forecasting. Energies, 16(23), 7788. DOI: 10.3390/en16237788.

[4] Fazylova, A., Kussainov, A., Baidullina, A., & Smailova, A. (2023). Solar Panel Tracker System Using GPS Technology. The Journal of CIEES, 2(2), 19–24. https://doi.org/10.48149/jciees.2022.2.2.3.

[5] J. A. Azzolini, M. J. Reno and J. Yusuf, (2023). A Model-Free Approach for Estimating Service Transformer Capacity Using Residential Smart Meter Data," 2023 IEEE 50th Photovoltaic Specialists Conference (PVSC), San Juan, PR, USA, 2023, pp. 1-1, doi: 10.1109/PVSC48320.2023.10360083.

[6] V. Lara-Fanego, C. A. Gueymard and L. Micheli, (2023). Soiling Model for PV Applications: Improved Parameterizations, 2023 IEEE 50th Photovoltaic Specialists Conference (PVSC), San Juan, PR, USA, 2023, pp. 1-3, doi: 10.1109/PVSC48320.2023.10359694.

[7] Maniscalco, M. P., Longo, S., Miccichè, G., Cellura, M., & Ferraro, M. (2024). A Critical Review of the Environmental Performance of Bifacial Photovoltaic Panels. Energies, 17(1), 226. https://doi.org/10.3390/en17010226.

[8] Mamodiya, U., & Tiwari, N. (2023). Design and Implementation of Hardware-Implemented Dual-Axis Solar Tracking System for Enhanced Energy Efficiency. Engineering Proceedings, 59(1), 122. https://doi.org/10.3390/engproc2023059122.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.5

Analysis of Modern Approaches to Security in IoT Networks

Marieta Haka
Technical University of Varna/ Faculty of Computer Sciences and Automation, Varna, Bulgaria

marieta.yordanova@tu-varna.bg

Abstract: IoT networks pose many security challenges due to the transfer and storage of a large amount of data and the need for a long battery life of the end devices. Cyberattacks on IoT devices are growing daily and detecting them and limiting their consequences is key to consumer trust in IoT-based solutions, and hence their wider application in various business solutions. This article presents an analysis of the advantages and disadvantages of approaches to increasing security in IoT networks based on blockchain technologies, artificial intelligence and cryptographic security methods.

Keywords: IoT, Security, Blockchain, Artificial Intelligence, Cryptographic Solutions.

Received 26 September 2024
Accepted 30 November 2024
Published 20 December 2024

1. Introduction

Internet of Things (IoT) is a technology that allows connected objects on a network such as software applications and intelligent systems to interact, collect, and process massive amounts of data, providing a variety of services to end users. IoT devices range from small sensors and actuators to smart tools, enabling companies to automate processes and reduce labor costs in healthcare, smart home, and smart industry with multiple applications [1].

Over the past 5 years, IoT has had a significant impact on the advancement of communication by enabling the integration of disparate objects within a unified network. Thanks to this technology, companies can automate processes and reduce labor costs. IoT is one of the most important technologies for business and everyday life and has the potential to gain momentum in usage [2]. The number of IoT devices is expected to exceed 29 billion by 2030, indicating the rapid growth of IoT [3]. In recent years, IoT data transmission has been increasing due to the integration of IoT applications across a wide range of domains [4].

IoT applications are being integrated across a wide range of industries, leading to the rapid expansion of the market. Wireless Sensor Networks (WSNs) play a critical role in IoT deployment [5]. In addition, WSN is an essential technology especially for real-time application development. They enable automation of various processes based on measured environmental parameters. WSN is used in healthcare and other industries to transform various service sectors that use IoT data 33transmission [2].

Despite the benefits of IoT, cyber-attacks are becoming more frequent as the flow of IoT data increases, posing a threat to the privacy of IoT data. The limited processing power and insufficient memory resources of IoT devices make it difficult to implement comprehensive security mechanisms. Because of these limitations, devices are vulnerable to attacks that allow unauthorized access to private information [6]. As a result, devices are susceptible to attacks such as BotNet, Man-in-the-middle, Distributed Denial of Service (DDoS) [7,8]. Due to these vulnerabilities, it is crucial to ensure the security of IoT communication sessions. Identifying resource-constrained devices and their associated resources is a challenging task in today's busy environment [9].

The process for recruiting research papers is performed systematized according to the algorithm shown in Figure 1, following the main steps of the updated PRISMA method [10]. During the review of papers, a search is made for the keywords "IoT", "security" and "proposed" in the databases of Google Scholar, Science Direct and ACM.

The search is filtered in the range from 2020 to 2024. As a result, a total of 101 research papers are identified. The purpose of this filtering is to find contemporary paper related to the topic. After analyzing the papers for relevance through their abstracts, 86 scientific of them are identified. Then, an analysis is made of whether the problem related to IoT security is discussed and whether a solution to this problem is proposed. The papers that do not comply these criteria are 26 and are thus not considered. The residual 60 papers are considered the most proper for analyzing modern approaches to secure IoT networks.

2. IoT Security Technologies

Various technologies such as Blockchain, Artificial Intelligence, and Cryptographic methods are being used to ensure the security of IoT which have been improving the security of IoT over the last 5 years. These technologies are an integrated approach to protect devices and their data from various types of cyber-attacks. Combining them into a holistic approach is essential to create resilient and secure IoT systems in the future.

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

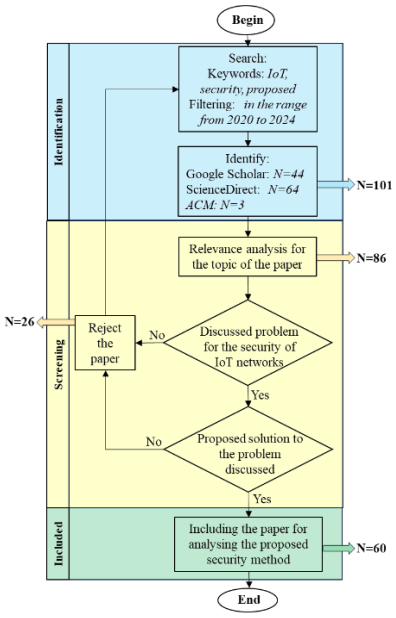


Fig. 1. Prisma process of literature review.

2.1. Blockchain

Blockchain technology is efficient due to its decentralized nature and the high degree of security it provides for data storage and transactions. By using cryptographic solutions and consensus mechanisms, Blockchain provides immutability and protection of information, making it suitable for IoT security. Security solutions have been developed using this method.

The proposal in [11, 12] includes a specific protocol for secure authentication of personal data when exchanging information between users and medical sensor devices. In the protocol, Blockchain is used to store the device information, authentication key and chaotic Chebyshev card to secure the authentication process and key. The objective of the proposed protocol is to solve the security problem of users of electronic medical services in IoMT. In [13] by proposing a Blockchain based framework for IoT data management using the Delegated Proof of Stake (DPoS) consensus algorithm the author proposes an approach to solve the security problem in IoT networks. Interplanetary File System (IPFS) distributed storage system and Docker are implemented to evaluate the network performance in terms of throughput, latency and resource utilization. In [14], Combo-Chain is proposed, a system implemented on Ethereum's access control platform and is based on attributes (ABAC), smart contracts and sharding seeks to solve the problem of access control to various resources in IoT environments. The study in [15] focuses on the security problem of communication between IoT devices that communicate over multi-hop cellular networks. A Blockchain-based approach with multitier architecture is proposed to solve this problem. The IoT network is partitioned into clusters using self-clustering method designed with EASISS-NEWO technique to increase network lifetime and security and reduce processing burden, network load and latency. In the study [16], an improved DPOS-PBFT controllable consensus mechanism is proposed to simultaneously guarantee the security of inter-node anticollision attacks and the efficiency of transaction consensus. The goal of this proposal is to solve problems such as network delays and transmission errors. In [17], the problem of implementing service-oriented architecture in IoT which is complex to maintain scalability and transaction exchange in a federated cloud system is addressed. Blockchain based microservice security system is proposed. This enables the exchange of transactions between permissioned Blockchain managers at different cloud service providers with some limitations. In addition, a microservice and Blockchain based security framework is implemented to ensure security and protect access control. Security features are implemented based on a smart contract between authorized Blockchain managers to achieve interoperability

In [18], a Blockchain based IoT data storage solution is proposed that performs batch transaction recording to optimize the data read and write speed. The solution aims to establish a balance between performance and data integrity in IoT transactions for agriculture. The data is first encrypted using RC5 algorithm and then stored using off-chain Merkle tree. The objective of the proposed solution is to solve the problem of low efficiency in collecting and processing IoT data in agriculture and security issues in storing this data. In [19], a Blockchain based framework is proposed for secure delivery of end-of-the-end software updates for IoT devices using attribute-based encryption. The objective of the proposed solution is to secure software updates to address the vulnerability of IoT devices to hacker attacks.

The study in [20] presents a lightweight hierarchical Blockchain based on multi-chain access control in IoT systems. The study in [21] considers DDoS and Sybil attacks as part of the security problems and a lightweight Proof of Work (PoW) for Blockchain in IoT is proposed to solve this problem. Heterogeneity Considered Trust Mechanism and Trust based Time-Constrained PoW (TBTC-PoW) is presented. Reasonable time windows of consensus nodes are allocated according to computational resources, trust values and mining difficulty, which reduces energy consumption and improves PoW security. In [22], Proof of Concept (PoC) is proposed to integrate Blockchain and smart contracts into the information flows used in various Common Data Environments. The objective of the proposed solution is to reduce human errors and increase the reliability and transparency of decision-making processes at construction sites pertaining to the structural system. Smart contracts with different levels of complexity are used, and the enhanced version compares the exchanged information with the data collected by IoT sensors on the construction site.

These studies highlight the importance of integrating Blockchain technology into IoT systems to address security challenges and provide secure and reliable IoT solutions. Blockchain technology offers as a solution to secure data communication and to provide a reliable and decentralized network system. Blockchain technology offers significant advantages for IoT security through decentralized structure and high level of data protection through consensus mechanisms such as PoW, DPoS and PBFT. The solutions discussed show that Blockchain can

improve access management, protect data from hacking attacks and ensure secure communication between IoT devices.

Despite these advantages, the application of Blockchain solutions to IoT security causes a scalability problem because Blockchain networks create difficulties in managing the large amount of data generated by IoT devices, which can lead to difficulties in managing large volumes of data and delays in processing [23]. The complexity of integration and lack of standardization increase the cost and challenges of deploying IoT ecosystems that use Blockchain methods [24].

2.2. Artificial intelligence

Artificial intelligence methods also have an important role to play in improving IoT security. AI-based cyber-attack detection and prevention systems can identify anomalies and potential threats, enabling a fast and effective response to potential incidents.

In [25], an automatic intrusion detection system is proposed using a well-known machine learning model, Random Forest, on a dataset (UNSW-NB15). The goal of this proposal is to improve the detection rate and reduce false problem alerts by improving the detection accuracy of network attacks. In [26], a CyberAIBot intrusion detection system for IoT cybersecurity targeting operational and information technology network traffic is presented. The proposed solution in [27] includes a cost-based classifier (CRFC) to develop an efficient Intrusion Detection System (IDS). The CRFC based classification is improved by incorporating a cost matrix computed based on feature importance which helps to improve the feature separation process even if there is feature imbalance.

In [28], an efficient IoT network anomaly mitigation system is developed by designing and deploying a DDoS attack detection system that uses a statistical method combining three algorithms: exponentially weighted moving average (EWMA), K-nearest neighbors (KNN), and cumulative sum (CUSUM) algorithm. In [29], an IoT-driven cross-device method is proposed to learn an IDS model on the traffic of different IoT devices included in the widely used N-BaIoT dataset. The purpose of this method is BotNet discovery from IoT through Deep Autoencoders. In [30], a feature selection solution is proposed using a classifier based on genetic algorithm. The aim of the method is intrusion detection in the IoT environment which is facing threats from BotNet attacks. The research [31] presents an approach to reduce DDoS attacks by being closer to the source of the attack, which provides faster response and greater efficiency. This approach combines host-based and network-based intrusion detection systems (HIDS and NIDS). The model offers a blended approach to anomaly detection at both the local and network level. The use of federated learning allows devices to process their data locally and contribute to the overall detection system, which improves the accuracy of detected anomalies and reduces the load on centralized systems.

In the research [32], a flexible edge (Edge) security approach is created that automatically creates and adapts security policies for edge IoT devices. The approach combines a dynamic security policy generator with a conflict detection and resolution system, a bias-aware risk assessment system, a regulatory compliance analysis system, and an AI-driven adaptivity integration system. In [33], a Blockchain based security system is proposed that uses PUF model to protect IoT devices by sharing alarm signals in the network. The use of machine learning and Blockchain technology results in low false positive rates and high detection accuracy in the system. The goal of this model is to efficiently and securely share data across the network, which reduces the likelihood of cyber-attacks and improves the overall security of IoT infrastructures. In [34], critical security challenges on the Internet of Things (IoT) domain are addressed by applying a solution that combines Convolutional Neural Networks (CNN) for feature extraction and the XGBoost model for intrusion detection. By applying the introduced hyperparameter optimization algorithm, more efficient models capable of handling intrusion detection effectively are constructed.

In [35], a complete real-time cyber-attack detection architecture is developed to simulate complex attack scenarios and provide appropriate countermeasures. The architecture uses current data and artificial intelligence modules to analyze and visualize threats, which improves the understanding of attacks and response capabilities. The goal of this system is to analyze data and prevent cyberattacks in a virtual environment, which is key to verifying and validating various defense methods.

Artificial Intelligence solutions enable proactive detection of new and unknown threats by analyzing network traffic anomalies. They can continuously learn and adapt to new types of attacks, such as DDoS or BotNet, and identify complex patterns of behavior in real time.

Despite these advantages, using artificial intelligence to protect IoT has several drawbacks. Using AI systems can be costly and difficult to deploy, especially for small businesses, and increases the potential for cyberattacks by creating new risks. Also, AI can create false positives, making it more difficult to detect new threats. This creates vulnerability to new cyber-attacks [36]. Such solutions often require a large amount of data and computational resources for training and analysis, which can be challenging for IoT devices with limited resources [37].

2.3. Cryptographic methods

Cryptographic methods are essential for securing IoT networks. Technology encompasses various methods such as symmetric and asymmetric encryption and hashing that protect communication and information from unauthorized access and manipulation, ensuring data confidentiality and integrity. The use of cryptographic techniques enhances the protection of communication channels, data generated by IoT devices, and the management of these devices [38]. Protecting data privacy in IoT settings is critical, as exposure of sensitive data can lead to challenges for both organizations and individuals. There is research addressing this problem by applying cryptographic techniques [39]. The proposal presented in [40] involves using a combination of end-to-end encrypted messages to solve the problem. To protect the useful data generated by MQTT, the Fernet cryptographic method is applied. This method provides authentication using SHA256 for hashing and AES128 for encryption

algorithms. The study in [41] presents an innovative algorithm that uses artificial intelligence to improve the encryption process of autonomous IoT systems. The main goal of the algorithm is to minimize the computational complexity associated with data encryption at both endpoints and intermediate nodes of IoT systems. To achieve this, an MD5 hashing algorithm is used on the encrypted data collected in IoT. The proposal in [42], involves the development and implementation of a cryptographic system for IoT. The system uses the AES algorithm in Electronic Code Book, Cipher Block Chaining and Counter modes of operation as well as additional security schemes such as AES Galois/Counter Mode and AES Galois Message Authentication Code to encrypt and decrypt text, images and electronic data applications. The research in [43] introduces adaptive eXtensible Access Control Markup Language (XACML) access policies specifically designed for heterogeneous distributed IoT environments. The main goal of these policies is to extend the capabilities of traditional XACML by integrating access code generation and verification schemes. To ensure the security of the access code, it is encrypted using MD5 and SHA-1 hashing. In [44], an algorithm is presented that uses artificial intelligence to improve the encryption process of autonomous IoT systems. The main goal of the algorithm is to minimize the computational complexity associated with data encryption at both endpoints and intermediate nodes of IoT systems. To achieve this, the algorithm uses MD5 hashing to encrypt the data collected at the IoT end nodes.

In [45], Lamport Merkle Digital Signature Verification is implemented to protect sensitive patient data from unauthorized access. Furthermore, authentication of IoT devices is achieved by creating hash value trees using Lamport Merkle Digital Signature. The goal of this strategy is to increase the security and privacy of IoT devices used in healthcare. In [46], the challenges associated with the identification and authentication of IoT devices are addressed by proposing the Secure Communication and Authentication for IoT applications using the Blockchain method. Using Blockchain and a hybrid cryptosystem that includes AES, the Elliptic Curve Digital Signature Algorithm (ECDSA) and the SHA hash function, this method provides a complete security solution. AES is used to ensure the confidentiality of communication between two devices, while ECDSA establishes secure communication between the device and the cluster coordinator. The goal of this approach is to strengthen IoT security measures by providing protection against potential attacks and optimizing computation and storage costs.

In [47], an architecture for AES that is resilient to errors and attacks is proposed for IoT applications, offering a cost-effective solution for error detection in security applications. By integrating the processes of AES encryption and decryption, it provides a comprehensive approach to real-time data protection. The architecture allows for efficient processing and ensures that the system can detect and handle errors. The study in [48] presents a scheme for preserving the privacy of data generated by IoT devices. The scheme proposes the use of homomorphic encryption to protect the data sent from user devices to the coordinator. By employing this encryption technique, the scheme aims to prevent unauthorized access and ensure that unreliable cloud servers cannot obtain information about the specific tasks performed on the patient's encrypted data.

The main objective is to enhance the confidentiality and security of sensitive medical information, thereby instilling confidence in patients and healthcare providers regarding the protection of their data. A scheme for authenticated key agreement is proposed in [49]. By utilizing Elliptic Curve Cryptography (ECC), the proposed solution ensures a high level of protection against unauthorized access. This approach guarantees the maintenance of trust and reliability of IoT systems in the face of evolving cyber threats. The aim of the research in [50] is to ensure that users can search for specific information in Blockchain without compromising the security and integrity of the data. By integrating deep learning algorithms and homomorphic encryption, the system offers a reliable solution for protecting sensitive information while enabling effective searching. In [51], through a combination of different cryptographic algorithms, the proposed Hybrid and Adaptive Cryptographic framework aims to increase the security and reliability of communication channels in IoT networks. The use of AES, RSA, and ECC algorithms in a hybrid manner provides a reliable and versatile approach to encryption, meeting the diverse communication requirements of IoT devices. The study in [52] focuses on increasing the security of communication between IoT and Blockchain by introducing an algorithm to generate a secure secret code. By including a secure secret code in the original message generated by IoT devices, the algorithm aims to ensure confidentiality and integrity of the transmitted data.

Using ECC to generate a hash of the secret code and message adds an extra layer of protection against unauthorized access. In addition, AES is used to protect all information using a single secret key. These keys are pre-generated and distributed to the targeted devices, allowing them to decrypt the encrypted data. In [53], the NTM-LEACH-RSA algorithm is used to solve security problems in WSN. The main objective of this approach is to optimize energy use while extending the uptime of the network. Using a cryptographic algorithm, RSA communication and data integrity within WSN are effectively protected. In [54] it is presented the development of Reconfigurable ASCON Hash Functions for IoT Applications (RECO-ASCON) - a reconfigurable cryptographic processor that offers a solution for working with multiple hash modes. By incorporating the ASCON Hash and Hasha algorithms, this solution provides secure message transmission in the IoT field. The versatility of RECO-ASCON allows it to adapt to different hashing requirements, providing a reliable cryptographic solution for IoT.

The main objective of [55] is to establish a reliable model for the protection of consumer data and the maintenance of the privacy of patients' personal data in the field of IoMT. To achieve this, a model for searching encrypted data and a hybrid cryptographic algorithm is employed, which combines the principles of the Caesar cipher, Elliptic Curve Diffie-Hellman (ECDH), and the

Digital Signature Algorithm (DSA). This combination enables the protection of messages during their transmission and facilitates secure key exchange between clients and healthcare centers. In [18], increasing the security and reliability of software updates is the main goal of the proposed Blockchain-based distributed software update framework. Using smart contracts and the ECDSA digital signature algorithm, the framework ensures the authenticity of the identity of the software creator. Additionally, the integrity of the software update is protected by verification using the SHA-3 cryptographic hash. This comprehensive approach aims to provide end-to-end protection and verification throughout the entire software delivery process.

In [56], to improve patient care and enable remote medical consultations, the MedIoTverse framework is presented. This framework covers vital parameters such as heart rate, blood pressure, and body temperature for effective patient monitoring. The focus of the proposed solution is to provide protection in the transmission of patient data to the health server. For this purpose, the AES-256 cryptographic algorithm is used, which provides a stable and reliable encryption method. The research in [57] aims to address vulnerabilities related to client IoT node authentication using the Tempered ECDSA algorithm. Using a timestamp that is not shared and has a short lifespan adds an extra layer of security to the authentication process. Cryptographic solutions are critical to the security of IoT networks, ensuring the confidentiality, integrity, and authenticity of data, preventing unauthorized access and manipulation. Various methods such as AES, RSA, SHA-256, MD5, and ECDSA are used to encrypt, hash, and sign data, providing security when devices exchange information. Cryptographic algorithms such as AES and RSA provide secure communication and are reliable in critical systems where privacy is key. Also, solutions such as ECC and optimized versions of AES are suitable for resource-constrained devices in IoT, offering high security and minimal resource usage [58, 59].

Table 1 presents the most used IoT security methods. From the analysis of IoT protection, over the past 5 years, the most used methods are Blockchain and cryptographic approaches. Blockchain technology is used for its decentralized structure and high level of data protection through consensus mechanisms such as PoW, DPoS, and PBFT. However, generating a large volume of data from IoT devices can lead to processing delays, and this creates an inability to protect data. Cryptographic methods are used because of the ability to create high-security IoT solutions with minimal use of resources, which makes them preferred over Blockchain. Of the cryptographic methods considered, AES is the most used, as it is standardized by the National Institute of Standards and Technology in the United States [60] and is recognized as a secure and reliable cryptographic algorithm that is essential for the security of IoT networks [61].

Table 1. Existing IoT Security Solutions

	Technology	Method		References				
				2024	2023	2022	2021	2020
Security	Blockchain	Consensus Mechanisms	PoW	[11];	[20];			
			PoC				[21];	
			DPoS	[12];	[15];			
		Distributed Ledger	EOSIO	[12];				
			Hyperledger Fabric		[16]; [17];	[50];		
			Ethereum	[13];	[14]; [16];			
		Smart Contracts		[11]; [12]; [13];	[14]; [15]; [16]; [17]; [18];	[19]; [32]; [50];	[46]; [21];	
	(Artificial Intelligence)	IDS (Intrusion Detection System)	Support Vector Machines (SVM)	[24];		[32];		
			Random Forests (RF)	[26];				
			K-Nearest Neighbours (kNN)		[14]; [27];			
			Auto-encoders	[25];	[28];		[41];	
			Recurrent Neural Network (RNN)	[34];		[50];		
			Genetic Algorithm (GA)		[29];		[44];	
		IPS (Intrusion Prevention System)	Federated Learning		[31];			
			Convolutional Neural Networks (CNN)		[32];			
	Cryptographic solutions	Data Encryption	AES, RSA, ECC, DH	[9]; [55]; [58];	[17]; [48]; [51]; [52];	[31]; [49]; [50];	[45]; [46]; [47];	[41];
		Hash Functions	SHA256, MD5, SHA3	[10];	[15]; [17]; [51]; [53]; [54];		[40]; [42]; [43];	[39];
		Digital Signatures	RSA, ECDSA, DSA	[56];	[38]; [54];	[31];	[44]; [45];	

1. Conclusion

This study examines the advantages and disadvantages of core security technologies in Internet of Object (IoT) systems, including blockchain, artificial intelligence, and cryptography. Blockchain improves access control and protects data from hacker attacks in the IoT but poses challenges with scalability and integration.

The lack of compliance with standards aggravates the costs and difficulties of using blockchain-based IoT systems. The capabilities of artificial intelligence include threat detection by analyzing atypical situations in network traffic, but its implementation comes with high costs and new risks, such as false alarms and the need for extensive data training. These factors could pose a serious problem for devices that have limited resources. Cryptographic methods are a mandatory component for securing IoT networks, ensuring the confidentiality, integrity, and authenticity of data. AES and RSA are efficient algorithms that provide secure communication and are used successfully in critical systems. Encryption methods are known for their minimal resource requirements, making them suitable for IoT devices with limited computing power. According to the study, the AES algorithm is the most used cryptographic method in IoT networks due to its efficiency and standardization. After the security techniques in IoT systems studied, the use of cryptographic methods for IoT security is mainly observed.

Their advantages such as offering high security with minimal resources make them suitable for environments with limited computing capabilities. Of the cryptographic methods, the use of the AES algorithm in IoT networks prevails. With key lengths of 128, 192, and 256 bits, this encryption algorithm is widely used due to its efficiency in making decryption a complex process.

References

[1] Sayed, M. (2024). The internet of things (iot), applications and challenges: a comprehensive review., *Journal of Innovative Intelligent Computing and Emerging Technologies (JIICET)*, vol. 1, no. 01, pp. 20-27

[2] Nassra, I. & Juan, V. (2023). Data compression techniques in IoT-enabled wireless body sensor networks: A systematic literature review and research trends for QoS improvement, *Internet of Things* vol. 23 pp.100806.

[3] Eltayieb, N. Rashad E. Yongjian L. Fagen L. & Shijie Z. (2024). A heterogeneous signcryption scheme with Cryptographic Reverse Firewalls for IoT and its application" *Journal of Information Security and Applications*, vol. 83 pp.103763.

[4] Garah, A. Nader, M. & Kirgizov, S. (2024). Enhancing IoT data confidentiality and energy efficiency through decision tree-based self-management, *Internet of Things* vol. 26 pp. 101219.

[5] Liao, S. (2024). Blockchain Sensor Network Based CPS Analysis in Healthcare System for Real Time Applications Using 6G IoT Model and Deep Learning Techniques, *Wireless Personal Communications*, pp. 1-16, doi: 10.1007/s11277-024-11185-1

[6] Rozlomii, I. Andrii, Y. & Serhii, N. (2024). Data security of IoT devices with limited resources: challenges and potential solutions, *In doors*, pp. 85-96.

[7] Lokendra, V. & Das, D. (2021). SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain, *Journal of Parallel and Distributed Computing*, vol. 154, pp. 94-105.

[8] Ali, A. Pasha, M.F. Ali, J. Fang, O.H. Masud, M. Jurcut, A.D. Alzain, M.A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography, *Sensors*, vol. 22, pp. 528, https://doi.org/10.3390/s22020528

[9] Nadhan, A. S. & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications, *Biomedical Signal Processing and Control*, vol. 88, pp.105511.

[10] Ed-Dafali, S., Adardour, Z., Derj, A., Bami, A., & Hussainey, K. (2025). A PRISMA-Based Systematic Review on Economic, Social, and Governance Practices: Insights and Research Agenda, *Business Strategy and the Environment*, vol. 34, no.), pp.1896-1916.

[11] Lin, Q. Li, X. Cai, K. Prakash, M., & Paulraj, D. (2024). Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking, *Information Sciences*, vol. 654, pp.119783.

[12] Miao, J. Wang, Z. Wu, Z. Ning, X. & Tiwari, P. (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things, *Expert Systems with Applications*, vol. 237, pp.121329.

[13] Haque, E. U. Shah, A. Iqbal, J. Ullah, S. S. Alroobaea, R. & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus, *Scientific Reports*, vol.14, no.1, pp. 7841.

[14] Bakhtiary, V. Mirabi, M. Salajegheh, A. & Erfani, S. H. (2024). Combo-Chain: Towards a hierarchical attribute-based access control system for IoT with smart contract and sharding technique, *Internet of Things*, vol. 25, pp. 101080.

[15] Kiran, A. Mathivanan, P. Mahdal, M. Sairam, K. Chauhan, D. & Talasila, V. (2023). Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques, *Mathematics*, vol.11, vol. 9, pp. 2073.

[16] Huang, R. Yang, X. & Ajay, P. (2023). Consensus mechanism for software-defined blockchain in internet of things, *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 52-60.

[17] Alshudukhi, K. S. Khemakhem, M. A. Eassa, F. E. & Jambi, K. M. (2023). An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment, *Electronics*, vol. 12, no. 3, pp. 776.

[18] Zhao, Y. Li, Q. Yi, W. & Xiong, H. (2023). Agricultural IoT data storage optimization and information security method based on blockchain, *Agriculture*, vol.13, no. 2, pp. 274.

[19] Solomon, G. Zhang, P. Brooks, R. & Liu, Y. (2023). A secure and cost-efficient blockchain facilitated IoT software update framework, *IEEE Access*, vol. 11, pp. 44879-44894.

[20] Abdi, A. I. Eassa, F. E. Jambi, K. Almarhabi, K. Khemakhem, M. Basuhail, A. & Yamin, M. (2022). Hierarchical blockchain-based multi-chaincode access control for securing IoT systems, *Electronics*, vol. 11, no. 5, 711.

[21] Qi, L. Tian, J. Chai, M. & Cai, H. (2023). LightPoW: A trust based time-constrained PoW for blockchain in internet of things, *Computer Networks*, vol. 220, pp.109480.

[22] Ciotta, V. Mariniello, G. Asprone, D. Botta, A. & Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept, *Automation in Construction*, vol. 132, pp. 103925.

[23] Morar, C. D. & Popescu, D. E. (2024). A Survey of Blockchain Applicability, Challenges, and Key Threats, *Computers*, vol. 13, no. 9, pp. 223.

[24] Stanco, G. Navarro, A. Frattini, F. Ventre, G. & Botta, A. (2024). A comprehensive survey on the security of low power wide area networks for the Internet of Things, *ICT Express*.

[25] Maghrabi, L. A. (2024). Automated network intrusion detection for internet of things security enhancements. *IEEE Access.*

[26] Serrano, W. (2024). CyberAIBot: Artificial Intelligence in an Intrusion Detection System for CyberSecurity in the IoT, *Future Generation Computer Systems*, pp. 107543.
[27] Pramilarani, K. & Kumari, P. V. (2024). Cost based random forest classifier for intrusion detection system in internet of things, *Applied Soft Computing*, vol. 151, pp. 111125.
[28] Alzahrani, R. J. & Alzahrani, A. (2023). A novel multi algorithm approach to identify network anomalies in the IoT using Fog computing and a model to distinguish between IoT and Non-IoT devices, *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, pp.19.
[29] Catillo, M. Pecchia, A. & Villano, U. (2023). A deep learning method for lightweight and cross-device IoT botnet detection, *Applied Sciences*, vol. 13, no. 2, pp. 837.
[30] Liu, X. Du, Y. (2023). Towards Effective Feature Selection for IoT Botnet Attack Detection Using a Genetic Algorithm. *Electronics*, vol. 12, pp. 1260, https://doi.org/10.3390/electronics12051260
[31] de Caldas Filho, F. L., Soares, S. C. M., Oroski, E., de Oliveira Albuquerque, R., Da Mata, R. Z. A., De Mendonça, F. L. L., & de Sousa Júnior, R. T. (2023). Botnet detection and mitigation model for IoT networks using federated learning, *Sensors*, vol. 23, no. 14, pp. 6305.
[32] Halgamuge, M. N. & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments, *Computers & Security*, vol. 148, pp.104128.
[33] Babu, E. S. SrinivasaRao, B. K. N. Nayak, S. R. Verma, A. Alqahtani, F. Tolba, A., & Mukherjee, A. (2022). Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks, *Computers and Electrical Engineering*, vol. 103, pp. 108287.
[34] Salb, M. Jovanovic, L. Bacanin, N. Antonijevic, M. Zivkovic, M. Budimirovic, N. & Abualigah, L. (2023). Enhancing internet of things network security using hybrid cnn and xgboost model tuned via modified reptile search algorithm, *Applied Sciences*, vol. 13, no. 23, pp.12687.
[35] Ciric, V. Milosevic, M. Sokolovic, D. & Milentijevic, I. (2024). Modular deep learning-based network intrusion detection architecture for real-world cyber-attack simulation, *Simulation Modelling Practice and Theory*, vol. 133, pp. 102916.
[36] Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities, *Sensors*, vol. 23, no. 17, pp. 7470.
[37] Ramos-Cruz, B. Andreu-Perez, J. & Martínez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research, *Neurocomputing*, pp. 127427.
[38] Perazzo, P. Righetti, F. La Manna, M. & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices, *Computer Communications*, vol. 170, pp. 151-163.
[39] Muneeswari, G. Varun, S. S. Hegde, R. Priya, S. S. Shermila, P. J. & Prasanth, A. (2023). Self-diagnosis platform via IOT-based privacy preserving medical data, *Measurement: Sensors*, vol. 25, pp. 100636.
[40] Ismail, E. G. Chahboun, A. & Raissouni, N. (2020). Fernet Symmetric Encryption Method to Gather MQTT E2E Secure Communications for IoT Devices.
[41] Li, B. Feng, Y. Xiong, Z. Yang, W. & Liu, G. (2021). Research on AI security enhanced encryption algorithm of autonomous IoT systems, *Information sciences*, vol. 575, pp. 379-398.
[42] Panagiotou, P. Sklavos, N. Darra, E. & Zaharakis, I. D. (2020). Cryptographic system for data applications, in the context of internet of things, *Microprocessors and Microsystems*, vol. 72, pp. 102921.
[43] Riad, K. & Cheng, J. (2021). Adaptive XACML access policies for heterogeneous distributed IoT environments, *Information Sciences*, vol. 548, pp. 135-152.
[44] Li, B. Feng, Y. Xiong, Z. Yang, W. & Liu, G. (2021). Research on AI security enhanced encryption algorithm of autonomous IoT systems, *Information sciences*, vol. 575, pp. 379-398.
[45] Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare, *Computer Communications*, vol. 170, pp. 200-208, https://doi.org/10.1016/j.comcom.2021.02.002.
[46] Sheikhpour, S. Ko, S. B. & Mahani, A. (2021). A low cost fault-attack resilient AES for IoT applications. Microelectronics *Reliability*, vol. 123, pp. 114202.
[47] Salim, M. M. Kim, I. Doniyor, U. Lee, C. & Park, J. H. (2021). Homomorphic encryption based privacy-preservation for iomt, *Applied Sciences*, vol. 11, no. 18, pp. 8757.
[48] Musthafa, A. S. Preya, A. J. Alneyadi, F. M., Alattas, N. S. El Hassan, G. & Zia, H. (2023, November). Safeguarding IoT Device Deployment in Healthcare: Analysis and Strategies for Enhanced Security and Privacy, In 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES) (pp. 1-7). IEEE, https://doi.org/10.1109/CIEES58940.2023.10378838.
[49] Ali, A. Pasha, M. F. Ali, J. Fang, O. H. Masud, M. Jurcut, A. D. & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography, *Sensors*, vol. 22, no. 2, pp. 528, https://doi.org/10.3390/s22020528.
[50] Patil, K. S. Mandal, I. & Rangaswamy, C. (2022). Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption, *Pervasive and Mobile Computing*, vol. 82, pp. 101552, https://doi.org/10.1016/j.pmcj.2022.101552.
[51] Parmar, M. & Shah, P. (2023). Internet of things-blockchain integration: a robust data security approach for end-to-end communication. *Indnesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 1050-1057.
[52] Anitha, S. Saravanan, S. & Chandrasekar, A. (2023). Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. Measurement: *Sensors*, vol. 29, pp.100889.
[53] El-Hadedy, M. Guo, X. Yoshii, K. Cai, Y., Herndon, R., Banta, B. & Hwu, W. M. (2023). RECO-ASCON: Reconfigurable ASCON hash functions for IoT applications, *Integration*, vol. 93, pp. 102061.
[54] Abikoye, O. C., Oladipupo, E. T., Imoize, A. L., Awotunde, J. B., Lee, C. C., & Li, C. T. (2023). Securing critical user information over the internet of medical things platforms using a hybrid cryptography scheme, *Future Internet*, vol. 15, no. 3, pp. 99.
[55] Mohammed, Z. K. Mohammed, M. A. Abdulkareem, K. H. Zebari, D. A. Lakhan, A. Marhoon, H. A. ... & Martinek, R. (2024). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption, *Applied Soft Computing*, vol. 158, pp. 111588, https://doi.org/10.1016/j.asoc.2024.111588.
[56] Puthiyidam, J. J., Joseph, S., & Bhushan, B. (2024). Temporal ECDSA: A timestamp and signature mask enabled ECDSA algorithm for iot client node authentication. *Computer Communications*, vol. 216, pp. 307-323, https://doi.org/10.1016/j.comcom.2024.01.016.
[57] Adeniyi, A. E. Jimoh, R. G. & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security, *Computers and Electrical Engineering*, vol. 118, pp. 109330.
[58] Hu, Z. Li, J. & Wilson, C. (2024). Resilient intermediary-based key exchange protocol for IoT. ACM Transactions on *Internet of Things*, vol. 5, no. 1, pp. 1-31.
[59] Silicon Labs. AN1233: Zigbee Security, Rev. 0.4, Copyright © 2023 by Silicon Laboratories. Available online:

https://docs.silabs.com/zigbee/7.4.2/zigbee-security-overview/ (accessed on 27.02.2025)
[60] Eyad, M.H.; Samer, A.; Amer, A.; Omar, A.S. Implementing and developing multi-stage cryptography technique for low-cost long-range communication system. Bull. Electr. Eng. Inform. 2024, 13.1, 264–276. https://doi.org/10.11591/eei.v13i1.6989.
[61] Hamad, E. M. Alabed, S. Alsaraira, A. & Saraereh, O. A. (2024). Implementing and developing multi-stage cryptography technique for low-cost long-range communication system, *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 1, pp. 264-276.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.6

Homomorphic Encryption for Secure Federated Learning: A PRISMA-Based Systematic Review

Dinko Dinkov
Nikola Vaptsarov Naval Academy, Varna, Bulgaria
d.dinkov@naval-acad.bg

Abstract: Federated learning (FL) enables collaborative training without sharing raw data but remains vulnerable to privacy leakage, poisoned gradients, and incorrect aggregation. Homomorphic encryption (HE) supports secure aggregation over encrypted updates, yet existing solutions are heterogeneous and lack systematic comparison. This paper presents a PRISMA-based systematic review of 104 studies on HE-enabled security mechanisms in FL, analyzed within the confidentiality–integrity–availability (CIA) framework. The results show a growing focus on poisoned-gradient robustness and verifiable aggregation, while only few integrated approaches address all CIA dimensions. These findings outline current limitations and guide future development of secure and trustworthy federated learning systems.

Keywords: homomorphic encryption, network security, federated learning, systematic review.

Received 18 November 2025
Accepted 3 December 2025
Published 15 January 2025

1. Introduction

Federated learning has emerged as a prominent paradigm for collaborative model training without centralizing sensitive data, enabling distributed participants to jointly build machine learning models while maintaining local data ownership [1, 2]. Despite this decentralized design, numerous studies demonstrate that standard FL protocols remain vulnerable to privacy leakage, model poisoning, and aggregation manipulation [3, 4, 5, 6]. Consequently, cryptographic protection mechanisms are increasingly integrated into FL systems to provide stronger confidentiality, integrity, and availability guarantees [7].

Among existing privacy-preserving technologies, HE has attracted particular attention due to its ability to enable direct computation over encrypted model updates [7, 8]. By allowing aggregation to be performed in the ciphertext domain, HE prevents the central server from accessing individual client parameters while preserving model accuracy. As a result, HE-based secure aggregation has become one of the most actively investigated directions in privacy-preserving federated learning [9, 10, 11].

In recent years, the research landscape has expanded rapidly, producing a large number of heterogeneous solutions that employ different homomorphic schemes, key management strategies, aggregation protocols, and robustness mechanisms [8, 12, 13]. However, these approaches are typically evaluated under inconsistent threat models, performance metrics, and experimental settings, which complicates direct comparison and limits the ability to identify practically applicable designs. Existing surveys [13, 14] predominantly provide narrative or conceptual overviews, focusing on architectural or theoretical aspects rather than a systematic and reproducible synthesis of the evidence.

To address this limitation, this study conducts a systematic review of HE–based security mechanisms in federated learning using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [15] methodology. The objective is to objectively identify, filter, and analyse relevant scientific publications and to provide a structured comparison of contemporary approaches according to their security guarantees, computational overhead, and practical applicability within the CIA framework.

The main contributions of this work are as follows:

- systematic identification and screening of recent HE-based FL research using transparent inclusion and exclusion criteria;
- structured taxonomy of approaches for enhancing confidentiality, integrity, and availability;
- comparative analysis of cryptographic schemes, aggregation mechanisms, and robustness techniques;
- identification of open challenges and directions for future research.

The remainder of the paper is organized as follows. Section 2 describes the PRISMA-based methodology and study selection process. Sections 3–6 present the comparative analysis of approaches addressing confidentiality, integrity, availability, and integrated protection. Finally, the paper summarizes key findings and outlines future research directions.

2. Systematic review methodology

The analysis of contemporary approaches to enhancing security in federated learning was performed using the PRISMA methodology [15]. The goal of this process is to systematically identify, filter, and select relevant scientific publications that examine the use of homomorphic

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

algorithms to protect the confidentiality, robustness, and correctness of aggregation in FL environments.

The Scopus database was used as the main search source due to its wide coverage of peer-reviewed scientific journals and conferences in the fields of computer science, cryptography, and artificial intelligence. The search covers the period 2022–2025 in order to include the most recent scientific developments on the topic. The search process was carried out using the advanced features of Scopus, applying a language filter for publications in English.

Keywords and phrases related to federated learning and homomorphic encryption were used to identify relevant studies, including "homomorphic encryption," "federated learning," "privacy preserving," "secure aggregation," "poison resistance," and "verification." The key terms were combined using Boolean operators, with the final search expression taking the following form: ("homomorphic encryption") AND ("federated learning") AND ("privacy preserving" OR "secure aggregation" OR "poison resistance" OR "verification").

The initial search identified 634 scientific publications, which were exported for further processing. After removing 13 duplicate (preprint) records, 621 unique articles remained. In the next stage, the titles and abstracts were reviewed, resulting in 385 publications being excluded due to a lack of direct relevance to the research objectives. Of the remaining 236 articles, 109 were excluded due to a lack of access to the full text.

A subsequent applicability check led to the exclusion of another 23 publications in which homomorphic encryption was only mentioned peripherally, without being the main research focus. As a result of this multi-stage process, in accordance with the PRISMA methodology, 104 scientific publications were selected that fully met the inclusion criteria and were used for an in-depth comparative analysis of contemporary approaches to protection in FL.

The process of identifying, filtering, and final selection of publications is summarized in a PRISMA diagram, shown in Figure 1, which visualizes the number of included and excluded studies at each stage of the analysis.

3. Confidentiality mechanisms in federated learning

Within the CIA triad, HE is used in FL as the primary mechanism for ensuring the confidentiality of transmitted client gradients and parameters. Encrypting local updates prevents the direct disclosure of sensitive information during aggregation, as the central server operates entirely on ciphertexts. Along with these advantages, the practical application of HE in FL introduces specific vulnerabilities related mainly to cryptographic key management.

One of the main threats in this context is the “collusion attack”, in which one or more clients collaborate with the aggregating server in order to reveal the individual local updates of the other participants [16]. This vulnerability is mainly characteristic of shared key pair schemes, in which all clients have the same private key for decrypting the aggregated result [17]. In such a configuration, compromising even a single client can lead to a complete loss of confidentiality, as it becomes possible to decrypt the individual encrypted gradients.

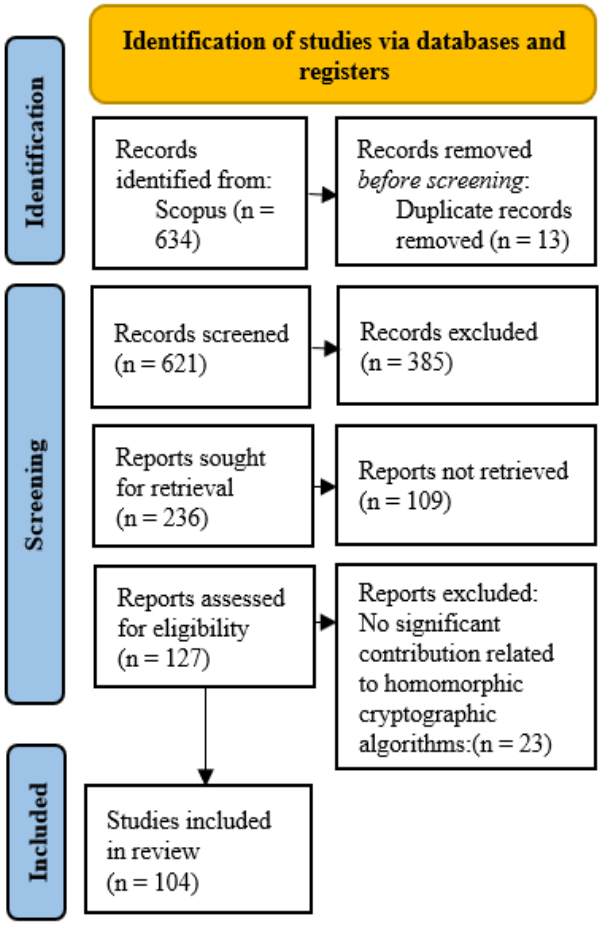


Fig 1. PRISMA-based study selection process.

3.1. Approaches to protection against collusion attacks

In order to limit collusion attacks in FL, various cryptographic and protocol mechanisms have been proposed in the scientific literature. A major group of solutions includes threshold cryptographic schemes and multi-key approaches, which eliminate the single point of trust by requiring the joint participation of a predetermined number of clients in decrypting the aggregated model [18]. In parallel, methods are being developed to neutralize collusive attacks within shared-key schemes, which introduce additional protective mechanisms without compromising the compatibility of HE. Table 1 shows the articles studied, sorted by key scheme.

Some solutions for protection against collusion attacks employ masking and obfuscation of local updates. In the scheme proposed in [17], each client adds a random mask to their homomorphically encrypted gradients before sending them to the aggregation server. To prevent the masks from being revealed in the event of collusion, the mask values are distributed among the participants through verifiable secret sharing, so that neither the server nor a limited coalition of clients has enough information to recover them. Upon aggregation, the masks are summed and correctly neutralized, allowing for the correct aggregate result to be obtained without

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.6

Table 1. Key schemes.

Key scheme	Collusion resistant	2022	2023	2024	2025
Shared key	No	[19, 20, 21, 22, 23]	[6, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33]	[34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57]	[58, 59, 60, 11, 61, 62, 63, 64, 65, 66, 67, 68, 69]
Shared key	Yes	[18, 70]	[71]	[9, 16, 17, 72, 73]	
Threshold cryptography	Yes	[74, 75]	[76]	[77, 78, 79, 80, 81, 82, 83, 84]	[85, 86, 87, 88, 89, 90, 91, 92, 93]
Multi-key	Yes	[94, 95, 96, 97]	[98, 99, 100, 101]	[5, 10, 102, 103, 104, 105, 106]	[107, 108, 109, 110, 111, 112, 113, 114]

revealing the individual gradients. Similarly, the schemes presented in [18] and [70] use blinding factors pre-generated by a trusted party, which are constructed so that their sum is zero. Thanks to this property, the factors are automatically canceled during homomorphic aggregation, ensuring the correctness of the result and protection against collusion between the server and the participants.

Other approaches, such as the schemes proposed in [16] and [71], combine HE with differential privacy by applying Gaussian or Laplace noise to the local gradients so that even with collusion, the original individual data cannot be recovered.

The schemes proposed in [9] and [16] introduce local protection parameters in the form of individual coefficients that are unique to each client and distributed through a trusted third party. These parameters are directly involved in the calculation of local updates and are not known to the aggregating server or other participants. As a result, even in the event of collusion between the server and multiple clients, the lack of information about the individual coefficients limits the ability to reconstruct local gradients and extract sensitive information.

Finally, solutions such as [73] combine HE with additive secret sharing, whereby local models are divided into multiple encrypted shares distributed among different computing nodes under the control of a trusted institution. This approach ensures that no single node or aggregator has enough information to recover the local parameters, thereby providing resistance to collusion attacks and eliminating single points of compromise.

A disadvantage of schemes relying on trusted third parties is the introduction of an additional point of trust—compromising these entities can lead to a complete security breach. In approaches based on differential privacy, noise in the data reduces the accuracy of the model, and in obfuscation techniques, there is an additional communication and computational overhead, in addition to the fact that these techniques must be controlled by a third party. The secret sharing-based mechanism, although highly secure, requires a high degree of coordination and synchronization among participants, making it less applicable in large-scale scenarios.

updates that may indicate collusion or fake identities. Together, these approaches enhance resilience against

4. Integrity protection and poisoned-gradient robustness

Integrity as an element of the CIA triad in FL refers to ensuring the correctness and reliability of the learning process and the resulting global model. Unlike threats to confidentiality, where the goal is to extract sensitive information, attacks on integrity are aimed at manipulating training by submitting incorrect, manipulated, or maliciously constructed updates. Such attacks can lead to a deterioration in convergence, a significant reduction in accuracy, or the introduction of targeted undesirable behavior into the model (e.g., backdoor functionality).

The main source of risk to integrity are the so-called Byzantine clients, which do not follow the training protocol and send modified gradients in order to influence the final result. Due to the decentralized nature of federated learning and the lack of direct access to local data, detecting and neutralizing such attacks is a significant challenge. In response to this, numerous mechanisms for robust aggregation have been proposed in the scientific literature, which aim to limit the impact of malicious updates and preserve the correctness of the global model.

4.1. Robust aggregation with plaintext gradients

When the aggregator has access to gradients in plaintext form, robust aggregation techniques are employed to mitigate the influence of malicious or anomalous clients while tolerating a limited number of Byzantine participants. These methods aim to preserve the stability and convergence of the global model despite adversarial updates. Representative approaches include distance-based schemes such as Krum and Multi-Krum [115], which select or average gradients that are closest to the majority, thereby reducing the impact of outliers, although they remain vulnerable to coordinated Sybil attacks. Statistical techniques, including Trimmed Mean and Geometric Median [116], improve robustness by removing extreme values or estimating a central tendency, at the cost of higher computational complexity. Additional protections rely on norm bounding (clipping) [59] to constrain excessively large updates, as well as Euclidean, Manhattan, or cosine similarity metrics [50], [85] to detect and down-weight suspicious gradients that deviate from the main cluster. Finally, Anti-Sybil mechanisms [117] restrict groups of overly similar

independent malicious behavior but remain less effective against well-coordinated adversaries.

These approaches significantly increase the resilience of federated learning with unencrypted gradients, but their transfer to the context of encrypted data is challenging due to the need for operations such as sorting, comparison, and median, which are computationally heavy or impossible with homomorphic encryption.

4.2. Robust mechanisms over encrypted gradients

This section analyzes 21 scientific publications that present mechanisms for improving the integrity of federated learning against poisoned gradients in the context of homomorphically encrypted local updates. The studies reviewed in Table 2 seek to integrate the cryptographic confidentiality provided by homomorphic encryption with reliable strategies for protecting the global model from malicious clients capable of sending manipulated or structurally incorrect gradients. The central challenge outlined in the literature is the inability to apply traditional algorithms directly to encrypted data due to the computational limitations of homomorphic schemes. Therefore, the approaches discussed develop adapted cryptographic and statistical mechanisms that allow the detection, suppression, or compensation of harmful updates while preserving the confidentiality and integrity of the training process. The first and most extensive group includes approaches based on encrypted distance and similarity metrics, which evaluate the deviation of local updates from a reference or expected model. In a number of schemes such as [85, 89, 112], encrypted Manhattan or Euclidean distance is used, while [5, 51, 78, 86] rely on cosine similarity or correlation measures calculated directly on homomorphically encrypted texts.

The second group of approaches includes clustering and statistical methods for anomaly detection. Reference [35] uses K-means on encrypted cosine similarities, [59] integrates the DBSCAN protocol, which groups gradients based on density and direction. In [90], SNN-based clustering is applied, where the algorithm uses the density of similarity between shared nearest neighbors to identify and filter potentially malicious ones. These mechanisms use group patterns in the data to distinguish between benign and malicious updates, even when the latter are disguised by small deviations.

A third approach involves models that use cryptographic verification through zero-knowledge proofs (ZKP) and virtual environments with provable integrity. The references [19] and 41] apply ZKP to verify that local updates are calculated correctly and do not contain arbitrary values. The most rigorous version of this approach [31] uses a zero-knowledge virtual machine that executes trusted code and generates ZKP in real time for the correctness of the computations, allowing the aggregator to accept only updates with valid proofs.

Another important class of approaches aims to adapt aggregation mechanisms that are resistant to malicious client updates to a homomorphic encryption environment. Reference [55] enables algorithms such as Krum, Multi-Krum, and Median to be executed entirely on encrypted gradients through an interactive masked sorting mechanism, while [50] implements distributed Multi-Krum logic on the Paillier cryptosystem. In this way, classical robust aggregation mechanisms are adapted to work in an encrypted data environment without compromising their efficiency.

Table 2. Integrity.

Category	Method	2022	2023	2024	2025
Distance	Manhattan distance				[85, 112]
	Euclidean distance			[82]	[89, 109]
Similarity	Cosine similarity			[5, 35, 51, 78, 82]	[59, 86, 111]
	Correlation coefficient	[94]		[103]	[69, 90]
Clustering	K-means			[35]	[109, 111]
	SNN				[90]
	DBSCAN				[59],
Statistics	Average distance				[89, 109]
	Inner product				[69]
Zero-knowledge	ZKP	[19]		[41]	
	ZKVM		[31]		
Robust aggregation	Krum			[55]	
	Multi-Krum			[50]	
	Median			[55]	
Dynamic trust	Dynamic thresholds				[85, 89, 109]
	Adaptive weights	[94]		[82]	[59, 69, 112]
	Reputation			[50, 103]	[85, 86, 90, 111]
Blockchain				[50]	[59, 109, 111]
Decentralisation				[35]	
Multi-server schemes		[19, 94]		[5, 78, 103]	[59, 85, 86, 89, 112]

The next direction involves dynamic trust schemes, adaptive weighting, and participant management. Reference [86] adapts customer weights when the model deteriorates, [82] uses a composite Q score, [112] uses a

median benchmark for adaptive weighting, [90] uses customer reputation, and [69] uses dynamic adjustment of participation probability after two-stage anomaly detection. These methods not only filter out manipulated updates, but also adapt the long-term influence of participants according to their behavior.

An important subgroup consists of architectures that use blockchain or decentralization to ensure integrity and transparency. Reference [50] implements blockchain for distributed Multi-Krum verification, while the method in [111] uses blockchain to validate encrypted updates, while [35] eliminates the central server and implements fully decentralized peer-to-peer aggregation.

Two-server and multi-server cryptographic architectures, which prevent collusion by separating roles, also make a significant contribution. The references [85, 86, 59, 103, 78] use independent servers for homomorphic comparisons, normalization, decryption, or verification. Reference [5] introduces edge and auxiliary servers with split secrets, ensuring security even with asynchronous updates.

Despite significant progress, mechanisms for resilience to encrypted poisoned gradients exhibit a number of limitations. Distance and similarity metrics rely on sensitive thresholds and can be circumvented by well-masked updates or highly heterogeneous data. Clustering methods sometimes misclassify benign clients, especially with small samples. Schemes with trusted reference models or medians assume the existence of a stable reference point, which itself can be compromised. Adaptive weights and reputation systems are susceptible to slow, gradually escalating attacks. More secure ZKP solutions guarantee correctness but introduce significant complexity and more difficult integration into real-world FL environments. Decentralized and blockchain approaches increase transparency but require additional synchronization and are vulnerable to coordinated attacks.

5. Availability and reliable aggregation

Within the CIA triad, the aspect of availability in FL is closely linked to the correct and sustainable formation of the global model. A significant threat in this context is an incorrectly aggregating central server, where the aggregator does not correctly perform the intended operations on the received encrypted updates – as a result of compromise, technical malfunction, or deliberate malicious behavior [6]. Unlike the assumption of an "honest but curious" server, here the aggregator can deliberately violate the protocol by modifying, omitting, or injecting updates, leading to systematic distortion or destabilization of the learning process. When using homomorphic encryption, this threat is further complicated because the manipulations are performed on the encrypted texts and remain difficult for clients to detect, with even minimal changes causing significant deviations in the global model, especially with heterogeneous data distribution [61].

5.1. Verifiable aggregation techniques

Modern secure aggregation schemes in FL, based on HE (Table 3), demonstrate high resistance to incorrect aggregation through a combination of cryptographic mechanisms and architectural solutions. The main principle that unites most approaches is the cryptographic "binding" between local client updates and the global aggregate. This binding ensures that any change, distortion, or partial aggregation by the central server automatically violates the verifiable equations – signature, hash, or commitment-based.

Schemes that use an external trusted verifier or a specialized central authority achieve strong control over the server. An example of this is [6], where the trusted authority performs challenge-based checks on blocks of encrypted parameters and on the aggregated model, allowing the detection of partial aggregation, result substitution, or sending different models to different clients. A similar approach is found in [17], where Pedersen commitments, verifiable secret sharing, and homomorphic signatures ensure cryptographic consistency between the submitted and aggregated gradients. In [82] and [61], verification is performed using one-way functions or homomorphic hashes, ensuring that any deviation from the actual sum is detected by the clients.

Other approaches rely on decentralized client verification, which does not rely on a trusted authority in the online phase. References [18] and [70] provide a mechanism whereby clients verify the homomorphic correspondence between the aggregated signature and the individual signatures. This prevents the server from modifying, omitting, or adding updates without the verification failing. Reference [92] extends this principle by embedding hidden information in the gradients and using a linear homomorphic hash for verification – even a minimal change in the aggregated values leads to a mismatch. Similar robustness is offered by [66], which uses Lagrange interpolation and commitment verification, allowing even differentiation between incorrect and malicious server behavior.

A significant portion of the work achieves resistance to incorrect aggregation through architectural solutions that reduce reliance on a single central node. The two-server model in [64] divides the aggregation roles so that no single server can independently skew the result without violating the verification equation. Reference [113] uses a fog–cloud architecture in which homomorphic hashes and CRT compression enable verification of the aggregate regardless of manipulation by the cloud server. Edge-oriented solutions such as [32] provide digital signing of the aggregation result, while TEE-based systems such as [91] eliminate the possibility of modifying the aggregation outside the protected hardware environment.

Modern approaches to verifiable aggregation in FL with HE offer various mechanisms for detecting malicious actions by the aggregator, but each has specific limitations. Solutions based on trusted verifiers provide high security but introduce an additional point of trust that, if compromised, invalidates the entire scheme.

Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.6

Table 3. Verification mechanisms.

Category	Method	2022	2023	2024	2025
Signatures	BLS signature		[6]		[61]
	Signcryption	[18, 70]			
	DTCH		[32]		
	DS				[92]
One-way functions	HF		[6, 32]	[82]	[64, 61]
	HHF				[65, 91, 92, 113]
Commitment structures	Pedersen commitment			[17]	
	Commitment				[66]
Algebraic verification	Labels				[64]
	Lagrange interpolation				[66]

Client-oriented checks eliminate the need for an external authority, but often burden participants with computational costs, especially in models with a large number of parameters, with only a few solutions offering verification with constant complexity. Architectural approaches such as dual-server, fog–cloud, or TEE reduce the risk of manipulation, but require additional infrastructure and do not completely eliminate the possibility of collusion.

6. Integrated security architectures for federated learning

This section discusses integrated schemes for federated learning that simultaneously ensure confidentiality, integrity and availability of the learning process by combining homomorphic encryption with mechanisms to protect against manipulated local updates and incorrect aggregation by the central server. Unlike the approaches discussed earlier, which address threats to confidentiality, integrity, or integrity separately, this section analyzes protocols that provide comprehensive protection in accordance with the CIA triad.

The PAR-FS scheme [62] combines symmetric homomorphic encryption, statistical anomaly detection, and client-side verification of aggregated gradients. Poisoned updates are mitigated using the 2-norm distance between local gradients and the mean vector, where large deviations receive lower weights, reducing the impact of malicious clients. The system employs two servers and digital signatures, enabling clients to recompute and verify the weighted aggregation against the decrypted global model. Thus, PAR-FS both filters anomalous updates and ensures aggregation correctness.

The contract-based hierarchical scheme [72] employs a three-layer architecture (training, aggregation, and consensus), where smart contracts on a blockchain replace the trusted third party. Malicious behavior is mitigated at the consensus layer by scoring aggregation domains according to model accuracy, reducing the influence of unreliable participants. Aggregation correctness and verifiability are ensured through certificate-less aggregatable signatures (CLAS) and Paillier homomorphic encryption, with secret sharing providing robustness to dropouts. Overall, the scheme combines model quality evaluation with cryptographic mechanisms to secure and validate the aggregation process.

PPVFL [49] extends this approach by combining blockchain with homomorphic encryption. Protection against poisoned gradients relies on an honest majority and consensus mechanisms that limit the impact of malicious nodes. Verifiability is ensured through ECDSA signatures that authenticate encrypted updates and a smart contract enabling nodes to compare local and global models to detect manipulation. Aggregation is performed over encrypted parameters, while the blockchain maintains a transparent and immutable record of updates.

The decentralized reputation scheme [84] removes the central server and organizes federated learning in a peer-to-peer network with a dynamically elected leader. Byzantine resilience is achieved through a reputation system that penalizes clients whose gradients deviate from the aggregate, limiting their influence and leadership eligibility. Secure aggregation is performed using SABLE, a coordinate-truncated mean over encrypted data that reduces the effect of outliers. Verifiability is provided through zero-knowledge proofs (SNIPs, zk-SNARKs) and verifiable secret sharing, enabling the leader to prove correct aggregation and clients to validate and reconstruct the global model.

EVFL [56] targets industrial IoT settings and combines fully homomorphic encryption, BLS signatures, and adaptive gradient sparsification (AdaGS). Poisoned updates are mitigated by verifying the integrity of signed encrypted parameters before aggregation, with a trusted authority excluding manipulated contributions through signature and challenge-based checks. The same authority validates the correctness of the homomorphic aggregation and ensures consistent results across agents. AdaGS further reduces communication and computation by transmitting only significant gradient components.

Although they provide a high level of security, the approaches analyzed also have a number of significant drawbacks. PAR-FS [62] relies on Euclidean distance to the mean gradient, which assumes relatively "normal" behavior of the majority of clients and can be circumvented by adaptive, well-coordinated model poisoning attacks; Furthermore, client verification of the full weighted sum can become expensive for large models. Hierarchical and blockchain-based schemes [49, 72] are associated with a significant increase in communication costs due to the need for a consensus layer, smart contract support, and the additional latency inherent in blockchain

infrastructures. The decentralized reputation scheme [84] relies on the correct functioning of the reputation mechanism and may be sensitive to coalitions, Sybil attacks, or dynamic changes in behavior, while the use of ZKP, VSS, and SABLE increases cryptographic complexity. EVFL [56], on the other hand, obtains strong guarantees of confidentiality and verifiability, but the cost of full HE and BLS-based challenge verification remains high, requiring compensation through aggressive gradient smoothing, which can potentially affect accuracy.

7. Discussion

The systematic analysis reveals several clear trends in the evolution of homomorphic encryption–based security mechanisms for FL. First, while early studies primarily focused on confidentiality through secure aggregation and key management, recent research demonstrates a noticeable shift toward integrity and availability guarantees. In particular, the number of proposed solutions addressing poisoned gradient detection and robustness has increased significantly over the last two years of the analysed period as show in Figure 2. A similar growth is observed in approaches incorporating verifiable aggregation, including cryptographic commitments, homomorphic hashes, signatures, and zero-knowledge proofs that enable clients to validate the correctness of the server's behavior. This indicates a transition from purely privacy-preserving designs toward comprehensive trust-aware federated learning systems.

The quantitative distribution summarized in Table 2 and Table 3, and further illustrated through Figure 2, highlights this trend by showing a steady rise in integrity-oriented and verification-based mechanisms compared to earlier years. These results suggest that the research community increasingly recognizes that confidentiality alone is insufficient and that protection against malicious clients and aggregators is equally critical for real-world deployments, particularly in safety- and security-sensitive domains such as healthcare, finance, and industrial IoT.

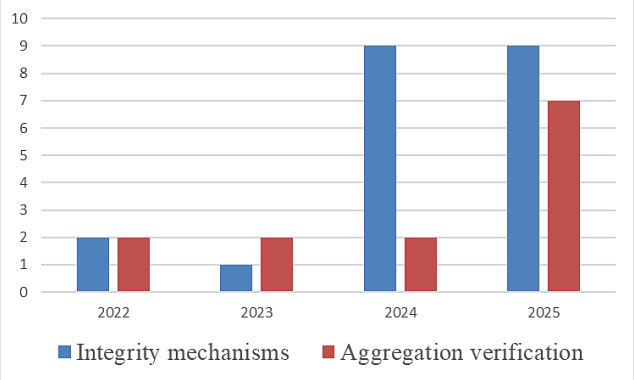


Fig 2. Number of proposed integrity and aggregation verification mechanisms in academic articles (2022–2025).

Despite this progress, the review also shows that fully integrated solutions remain limited. Only five identified models simultaneously address all three dimensions of the CIA triad – confidentiality, integrity, and availability – by combining encrypted aggregation, robustness against poisoned updates, and verifiable or decentralized aggregation protocols. This relatively small number highlights the complexity of achieving comprehensive protection while maintaining acceptable computational and communication overhead. At the same time, it indicates a promising direction for future research. As FL systems move from experimental settings to practical applications, interest in such holistic, end-to-end secure architectures is expected to grow, motivating further work on scalable, efficient, and jointly optimized cryptographic and robustness mechanisms.

8. Conclusion

This paper presented a PRISMA-based systematic review of homomorphic encryption–enabled security mechanisms for federated learning, analysing 104 recent studies within the confidentiality–integrity–availability (CIA) framework. The results show that while early work primarily emphasized confidentiality through secure aggregation, current research increasingly targets integrity and verifiable aggregation to mitigate poisoned gradients and malicious server behaviour. Despite significant progress, only a limited number of approaches provide comprehensive protection across all CIA dimensions, highlighting the complexity of achieving end-to-end security with acceptable overhead. These findings consolidate the current state of the art and indicate that future research should focus on scalable, integrated, and practically deployable cryptographic solutions for trustworthy federated learning.

References

[1] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T. & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency, *arXiv preprint*, arXiv:1610.05492, https://arxiv.org/abs/1610.05492.

[2] McMahan, B., Moore, E., Ramage, D., Hampson, S. & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data, *Artificial Intelligence and Statistics (AISTATS)*, PMLR, pp. 1273-1282.

[3] Zhu, L., Liu, Z. & Han, S. (2019). Deep leakage from gradients, *Proceedings of the 33rd International Conference on Neural Information Processing Systems (NeurIPS)*, Curran Associates Inc., pp. 14774-14784.

[4] Shokri, R., Stronati, M., Song, C. & Shmatikov, V. (2017). Membership inference attacks against machine learning models, *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 3-18, https://doi.org/10.1109/SP.2017.41.

[5] Zhou, A., Jiang, N. & Tang, T. (2024). Asynchronous Robust Aggregation Method with Privacy Protection for IoV Federated Learning, *World Electric Vehicle Journal*, vol. 15, no. 1, p. 18, https://doi.org/10.3390/wevj15010018.

[6] Gao, H., He, N. & Gao, T. (2023). SVeriFL: Successive verifiable federated learning with privacy-preserving, *Information Sciences*, vol. 622, pp. 98-114, https://doi.org/10.1016/j.ins.2022.11.124.

[7] Shalabi, E., Khedr, W., Rushdy, E. & Salah, A. (2025). A comparative study of privacy-preserving techniques in federated learning: A performance and security analysis, *Information*, vol. 16, no. 3, p. 244, https://doi.org/10.3390/info16030244.

[8] Xin, W., Jiaqian, L., Xueshuang, D., Haoji, Z. & Lianshan, S. (2025). A survey of differential privacy techniques for federated learning, *IEEE Access*, vol. 13, pp. 6539-6555, https://doi.org/10.1109/ACCESS.2024.3523909.

[9] Sun, H., Chen, X. & Yuan, K. (2024). FL-EASGD: Federated Learning Privacy Security Method Based on

Homomorphic Encryption, *Computers, Materials and Continua*, vol. 79, no. 2, pp. 2361–2373, https://doi.org/10.32604/cmc.2024.049159.
[10] Liu, W., Zhou, T., Chen, L., Yang, H., Han, J. & Yang, X. (2024). Round efficient privacy-preserving federated learning based on MKFHE, *Computer Standards & Interfaces*, vol. 87, Art. no. 103773, https://doi.org/10.1016/j.csi.2023.103773.
[11] Zhu, B. & Niu, L. (2025). A privacy-preserving federated learning scheme with homomorphic encryption and edge computing, *Alexandria Engineering Journal*, vol. 118, pp. 11–20, https://doi.org/10.1016/j.aej.2024.12.070.
[12] Aziz, R., Banerjee, S., Bouzefrane, S. & Le Vinh, T. (2023). Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm, *Future Internet*, vol. 15, no. 9, p. 310, https://doi.org/10.3390/fi15090310.
[13] Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A. & Verykios, V. S. (2024). Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review, *Information*, vol. 15, no. 11, p. 697, https://doi.org/10.3390/info15110697.
[14] Manzoor, H. U., Shabbir, A., Chen, A., Flynn, D. & Zoha, A. (2024). A survey of security strategies in federated learning: Defending models, data, and privacy, *Future Internet*, vol. 16, no. 10, p. 374, https://doi.org/10.3390/fi16100374.
[15] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Moher, D. (2021). *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews*. *PLOS Medicine*, *18*(3), e1003583. https://doi.org/10.1371/journal.pmed.1003583
[16] Wei, Q. & Rao, G. (2024). EPFL-DAC: Enhancing Privacy in Federated Learning with Dynamic Aggregation and Clipping, *Computers & Security*, vol. 143, Art. no. 103911, https://doi.org/10.1016/j.cose.2024.103911.
[17] Ming, Y., Wang, S., Wang, C., Liu, H., Deng, Y., Zhao, Y. & Feng, J. (2024). VCSA: Verifiable and collusion-resistant secure aggregation for federated learning using symmetric homomorphic encryption, *Journal of Systems Architecture*, vol. 156, Art. No. 103279, https://doi.org/10.1016/j.sysarc.2024.103279.
[18] Du, W., Li, M., Yang, X., Wu, L. & Zhou, T. (2022). VCFL: A verifiable and collusion attack resistant privacy preserving framework for cross-silo federated learning, *Pervasive and Mobile Computing*, vol. 86, Art. no. 101697, https://doi.org/10.1016/j.pmcj.2022.101697.
[19] Ma, X., Zhou, Y., Wang, L. & Miao, M. (2022). Privacy-preserving Byzantine-robust federated learning, *Computer Standards & Interfaces*, vol. 80, Art. no. 103561, https://doi.org/10.1016/j.csi.2021.103561.
[20] Wibawa, F., Catak, F. O., Sarp, S. & Kuzlu, M. (2022). BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models, *Cryptography*, vol. 6, no. 3, pp. 34, https://doi.org/10.3390/cryptography6030034.
[21] Kurniawan, H. & Mambo, M. (2022). Homomorphic Encryption-Based Federated Privacy Preservation for Deep Active Learning, *Entropy*, vol. 24, no. 11, pp. 1545, https://doi.org/10.3390/e24111545.
[22] Xia, L., Zheng, P., Li, J., Tang, W. & Zhang, X. (2022). Privacy-preserving gradient boosting tree: Vertical federated learning for collaborative bearing fault diagnosis, *IET Collaborative Intelligent Manufacturing*, vol. 4, no. 3, pp. 208–219, https://doi.org/10.1049/cim2.12057.
[23] He, D., Du, R., Zhu, S., Zhang, M., Liang, K. & Chan, S. (2022). Secure Logistic Regression for Vertical Federated Learning, *IEEE Internet Computing*, vol. 26, no. 2, pp. 61–68, https://doi.org/10.1109/MIC.2021.3138853.
[24] Wu, X., Fan, Y., Zhang, J. & Gao, Z. (2023). Federated Latent Dirichlet Allocation for User Preference Mining, *Journal of Web Engineering*, vol. 22, no. 4, pp. 639–677, https://doi.org/10.13052/jwe1540-9589.2244.
[25] Fontenla-Romero, O., Guijarro-Berdiñas, B., Hernández-Pereira, E. & Pérez-Sánchez, B. (2023). FedHEONN: Federated and homomorphically encrypted learning method for one-layer neural networks, *Future Generation Computer Systems*, vol. 149, pp. 200–211, https://doi.org/10.1016/j.future.2023.07.018.
[26] Deng, S., Zhang, J., Li, T., Jiang, X. & Wang, F. (2023). LSBlocFL: A secure federated learning model combining blockchain and lightweight cryptographic solutions, *Computers and Electrical Engineering*, vol. 111, Part B, Art. no. 108986, https://doi.org/10.1016/j.compeleceng.2023.108986.
[27] Ghavamipour, A. R., Turkmen, F., Wang, R. & Liang, K. (2023). Federated Synthetic Data Generation with Stronger Security Guarantees, in *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT)*, ACM, pp. 31–42, https://doi.org/10.1145/3589608.3593835.
[28] Xu, Y., Hu, X., Wei, J., Yang, H. & Li, K. (2023). VF-CART: A communication-efficient vertical federated framework for the CART algorithm, *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 1, pp. 237–249, https://doi.org/10.1016/j.jksuci.2022.11.013.
[29] Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., Zebari, D. A., Nedoma, J., Martinek, R., Kadry, S. & Garcia-Zapirain, B. (2023). Homomorphic federated learning schemes enabled pedestrian and vehicle detection system, *Internet of Things*, vol. 23, Art. no. 100903, https://doi.org/10.1016/j.iot.2023.100903.
[30] Angulo, E., Márquez, J. & Villanueva-Polanco, R. (2023). Training of Classification Models via Federated Learning and Homomorphic Encryption, *Sensors*, vol. 23, no. 4, pp. 1966, https://doi.org/10.3390/s23041966.
[31] Zhang, B., Lu, G., Qiu, P., Gui, X. & Shi, Y. (2023). Advancing Federated Learning through Verifiable Computations and Homomorphic Encryption, *Entropy*, vol. 25, no. 11, pp. 1550, https://doi.org/10.3390/e25111550.
[32] Zhang, J., Liu, Y., Wu, D., Lou, S., Chen, B. & Yu, S. (2023). VPFL: A verifiable privacy-preserving federated learning scheme for edge computing systems, *Digital Communications and Networks*, vol. 9, no. 4, pp. 981–989, https://doi.org/10.1016/j.dcan.2022.05.010.
[33] Huang, Y., Feng, X., Wang, W., He, H., Wang, Y. & Yao, M. (2023). EFMVFL: An Efficient and Flexible Multi-party Vertical Federated Learning without a Third Party, *ACM Transactions on Knowledge Discovery from Data*, vol. 18, no. 3, pp. 1–20, https://doi.org/10.1145/3627993.
[34] Wang, Z., Yu, X., Wang, H. & Xue, P. (2024). A federated learning scheme for hierarchical protection and multiple aggregation, *Computers and Electrical Engineering*, vol. 117, Art. no. 109240, https://doi.org/10.1016/j.compeleceng.2024.109240.
[35] Hijazi, N. M., Aloqaily, M. & Guizani, M. (2024). Collaborative IoT learning with secure peer-to-peer federated approach, *Computer Communications*, vol. 228, Art. no. 107948, https://doi.org/10.1016/j.comcom.2024.107948.
[36] Chen, B. & Ye, J. (2024). A safe parameter aggregation method under encrypted state for federated learning, *Procedia Computer Science*, vol. 247, pp. 1257–1266, https://doi.org/10.1016/j.procs.2024.10.151.
[37] Truhn, D. et. al. (2024). Encrypted federated learning for secure decentralized collaboration in cancer image analysis, *Medical Image Analysis*, vol. 92, Art. no. 103059, https://doi.org/10.1016/j.media.2023.103059.
[38] Stripelis, D., Gupta, U., Saleem, H., Dhinagar, N., Ghai, T., Anastasiou, C., Sánchez, R., Ver Steeg, G., Ravi, S., Naveed, M., Thompson, P. M. & Ambite, J. L. (2024). A federated learning architecture for secure and private neuroimaging

analysis, *Patterns*, vol. 5, no. 8, Art. no. 101031, https://doi.org/10.1016/j.patter.2024.101031.
[39] Song, C., Wang, Z., Peng, W. & Yang, N. (2024). Secure and Efficient Federated Learning Schemes for Healthcare Systems, *Electronics*, vol. 13, no. 13, pp. 2620, https://doi.org/10.3390/electronics13132620.
[40] Li, L., Sun, X., Shi, N., Ci, X. & Liang, C. (2024). A Stealthy Communication Model for Protecting Aggregated Results Integrity in Federated Learning, *Electronics*, vol. 13, no. 19, pp. 3870, https://doi.org/10.3390/electronics13193870.
[41] Rao, G. R. K., Ghanimi, H. M. A., Ramachandran, V., Al-Qahtani, D., Dadheech, P. & Sengan, S. (2024). Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training, *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 27, no. 2A, pp. 361–370, https://doi.org/10.47974/JDMSC-1891.
[42] Anuvarshini, B., Varshaa, D., Sujithra, M. & Devi, D. S. (2024). Preserving privacy in healthcare analytics: Federated learning for breast cancer prediction in a collaborative learning framework, *Grenze International Journal of Engineering and Technology*, vol. 10, no. 2, Part 4, pp. 5538–5544
[43] Ullah, I., Deng, X., Pei, X., Mushtaq, H. & Uzair, M. (2024). IoV-SFL: A blockchain-based federated learning framework for secure and efficient data sharing in the internet of vehicles, *Peer-to-Peer Networking and Applications*, vol. 18, Art. no. 34, pp. 1–20, https://doi.org/10.1007/s12083-024-01821-9.
[44] Pan, Y., Chao, Z., He, W., Jing, Y., Li, H. & Wang, L. (2024). FedSHE: Privacy preserving and efficient federated learning with adaptive segmented CKKS homomorphic encryption, *Cybersecurity*, vol. 7, Art. no. 40, https://doi.org/10.1186/s42400-024-00232-w.
[45] Shen, C., Zhang, W., Zhou, T., Zhang, Y. & Zhang, L. (2024). An efficient and secure privacy-preserving federated learning framework based on multiplicative double privacy masking, *Computers, Materials & Continua*, vol. 80, no. 3, pp. 4729–4748, https://doi.org/10.32604/cmc.2024.054434.
[46] Xiong, R., Ren, W., Zhao, S., He, J., Ren, Y., Choo, K.-K. R. & Min, G. (2024). CoPiFL: A collusion-resistant and privacy-preserving federated learning crowdsourcing scheme using blockchain and homomorphic encryption, *Future Generation Computer Systems*, vol. 156, pp. 95–104, https://doi.org/10.1016/j.future.2024.03.016.
[47] Tan, Z.-S., See-To, E. W. K., Lee, K.-Y., Dai, H.-N. & Wong, M.-L. (2024). Privacy-preserving federated learning for proactive maintenance of IoT-empowered multi-location smart city facilities, *Journal of Network and Computer Applications*, vol. 231, Art. no. 103996, https://doi.org/10.1016/j.jnca.2024.103996.
[48] Rieyan, S. A., News, M. R. K., Rahman, A. B. M. M., Khan, S. A., Zaarif, S. T. J., Alam, M. G. R., Hassan, M. M., Ianni, M. & Fortino, G. (2024). An advanced data fabric architecture leveraging homomorphic encryption and federated learning, *Information Fusion*, vol. 102, Art. no. 102004, https://doi.org/10.1016/j.inffus.2023.102004.
[49] Mahato, G., Mishra, B. K., Haldar, R., Roy, S. D. & Wang, G. (2024). A blockchain-based privacy-preserving federated learning for healthcare data sharing, *Computers in Biology and Medicine*, vol. 173, Art. no. 108268, https://doi.org/10.1016/j.compbiomed.2024.108268.
[50] Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X. & Guizani, M. (2024). A blockchain-based privacy-preserving federated learning scheme for Internet of Vehicles, *Digital Communications and Networks*, vol. 10, no. 1, pp. 126–134, https://doi.org/10.1016/j.dcan.2022.05.020.
[51] Xu, R., Gao, S., Li, C., Joshi, J. & Li, J. (2024). Dual defense: Enhancing privacy and mitigating poisoning attacks in federated learning, *Advances in Neural Information Processing Systems*, vol. 37, pp. 70476-70498, doi: 10.52202/079017-2253.
[52] Pais, V., Rao, S., Muniyal, B. & Yun, S. (2024). FedICU: a federated learning model for reducing the medication prescription errors in intensive care units, *Cogent Engineering*, vol. 11, no. 1, Art. no. 2301150, https://doi.org/10.1080/23311916.2023.2301150.
[53] Al-Janabi, A., Al Janabi, S. & Al Khateeb, B. (2024). Healthcare privacy-preserving federated transfer learning using CKKS-based homomorphic encryption and PYHFELTool, *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 3, Art. no. 30, https://doi.org/10.52866/ijcsm.2024.05.03.029.
[54] Wang, M., Wang, Q. Y., Zhang, Y. H., Zhang, Z. X., Feng, Y. N. & Cao, Y. F. (2024). Preserving differential privacy in neural networks for foreign object detection with heterogeneity-based noising among distributed devices, *The Journal of Supercomputing*, vol. 80, pp. 21447–21474, https://doi.org/10.1007/s11227-024-06243-1.
[55] Jiang, S., Yang, H., Xie, Q., Ma, C., Wang, S. & Xing, G. (2024). Lancelot: Towards efficient and privacy-preserving Byzantine-robust federated learning within fully homomorphic encryption, *arXiv preprint*, arXiv:2408.06197.
[56] Wu, J., Wu, C., Chen, C., Jin, J. & Zhou, C. (2024). EVFL: Towards Efficient Verifiable Federated Learning via Parameter Reuse and Adaptive Sparsification, *Mathematics*, vol. 12, no. 16, pp. 2479, https://doi.org/10.3390/math12162479.
[57] Wang, B. & Yang, F. (2024). Lightweight and privacy-preserving hierarchical federated learning mechanism for artificial intelligence-generated image content, *Journal of Real-Time Image Processing*, vol. 21, no. 4, pp. 1957–1973, https://doi.org/10.1007/s11554-024-01524-7.
[58] Zhang, Y., Lu, Y., Liu, F., Li, C., Gong, Z., Hu, Z. & Xu, Q. (2025). Privacy-preserving and communication-efficient stochastic alternating direction method of multipliers for federated learning, *Information Sciences*, vol. 691, Art. no. 121641, https://doi.org/10.1016/j.ins.2024.121641.
[59] Xiao, J., Nie, H., Yi, Z., Tang, X. & Lu, S. (2025). Federated learning with bilateral defense via blockchain, *Neural Networks*, vol. 185, Art. no. 107199, https://doi.org/10.1016/j.neunet.2025.107199.
[60] He, Y., Wei, L., Chen, F., Zhang, H., Yu, J. & Wang, H. (2025). FedAI: Federated recommendation system with anonymized interactions, *Expert Systems with Applications*, vol. 271, Art. no. 126564, https://doi.org/10.1016/j.eswa.2025.126564.
[61] Wang, R., Xiong, L., Geng, J., Xie, C. & Li, R. (2025). An effective and verifiable secure aggregation scheme with privacy-preserving for federated learning, *Journal of Systems Architecture*, vol. 161, Art. no. 103364, https://doi.org/10.1016/j.sysarc.2025.103364.
[62] Zhang, C., Zhang, X., Yang, X., Liu, B., Zhang, Y. & Zhou, R. (2025). Poisoning attacks resilient privacy-preserving federated learning scheme based on lightweight homomorphic encryption, *Information Fusion*, vol. 121, Art. No. 103131, https://doi.org/10.1016/j.inffus.2025.103131.
[63] Castro, F., Impedovo, D. & Pirlo, G. (2025). An efficient and privacy-preserving federated learning approach based on homomorphic encryption, *IEEE Open Journal of the Computer Society*, vol. 6, pp. 336–347, https://doi.org/10.1109/OJCS.2025.3536562.
[64] Kang, Y., Tan, W., Fan, L., Chen, Y., Lai, X. & Weng, J. (2025). GHEFL: Grouping Based on Homomorphic Encryption Validates Federated Learning, *Future Internet*, vol. 17, no. 3, pp. 128, https://doi.org/10.3390/fi17030128.
[65] Banerjee, A., Mahato, G. K. & Chakraborty, S. K. (2025). Securing FANET using federated learning through homomorphic matrix factorization, *International Journal of*

Information Technology, vol. 17, no. 1, pp. 17–36, https://doi.org/10.1007/s41870-024-02197-y.
[66] Xie, D. & Li, D. (2025). Privacy-Preserving and Verifiable Personalized Federated Learning, *Symmetry*, vol. 17, no. 3, pp. 361, https://doi.org/10.3390/sym17030361.
[67] Asiri, M., Khemakhem, M. A., Alhebshi, R. M., Alsulami, B. S. & Eassa, F. E. (2025). RPFL: A reliable and privacy-preserving framework for federated learning-based IoT malware detection, *Electronics*, vol. 14, no. 6, Art. no. 1089, https://doi.org/10.3390/electronics14061089.
[68] Liang, X., Xu, Y., Lin, Y., Chen, L., Zhang, Z., Wang, H. & Liu, J. (2025). Federated split learning via dynamic aggregation and homomorphic encryption on non-IID data, *The Journal of Supercomputing*, vol. 81, Art. no. 63, https://doi.org/10.1007/s11227-024-06612-w.
[69] Bai, F., Zhao, Y., Shen, T., Zeng, K., Zhang, X. & Zhang, C. (2025). FedOPCS: An optimized poisoning countermeasure for non-IID federated learning with privacy-preserving stability, *Symmetry*, vol. 17, no. 5, p. 782, https://doi.org/10.3390/sym17050782.
[70] Du, W. & Gao, S. (2022). A Homomorphic Signcryption-Based Privacy-Preserving Federated Learning Framework for IoT, *Security and Privacy*, Art. no. 8380239, https://doi.org/10.1155/2022/8380239.
[71] Zhao, J., Huang, C., Wang, W., Xie, R., Dong, R. & Matwin, S. (2023). Local differentially private federated learning with homomorphic encryption, *The Journal of Supercomputing*, vol. 79, pp. 19365-19395, https://doi.org/10.1007/s11227-023-05378-x.
[72] Wei, Q., Rao, G. & Wu, X. (2024). Contract-based hierarchical security aggregation scheme for enhancing privacy in federated learning, *Journal of Information Security and Applications*, vol. 85, Art. no. 103857, https://doi.org/10.1016/j.jisa.2024.103857.
[73] Saidi, A., Amira, A. & Nouali, O. (2024). Securing decentralized federated learning: cryptographic mechanisms for privacy and trust, *Cluster Computing*, vol. 28, no. 2, https://doi.org/10.1007/s10586-024-04957-8.
[74] Sav, S., Bossuat, J.-P., Troncoso-Pastoriza, J. R., Claassen, M. & Hubaux, J.-P. (2022). Privacy-preserving federated neural network learning for disease-associated cell classification, *Patterns*, vol. 3, no. 5, Art. no. 100487, https://doi.org/10.1016/j.patter.2022.100487.
[75] Park, J. & Lim, H. (2022). Privacy-Preserving Federated Learning Using Homomorphic Encryption, *Applied Sciences*, vol. 12, no. 2, pp. 734, https://doi.org/10.3390/app12020734.
[76] Grivet Sébert, A., Checri, M., Stan, O., Sirdey, R. & Gouy-Pailler, C. (2023). Combining homomorphic encryption and differential privacy in federated learning, in *Proceedings of the 20th Annual International Conference on Privacy, Security and Trust (PST)*, IEEE, pp. 1–7, https://doi.org/10.1109/PST58708.2023.10320195.
[77] Tian, H., Wen, Y., Zhang, F., Shao, Y. & Li, B. (2024). Lattice based distributed threshold additive homomorphic encryption with application in federated learning, *Computer Standards & Interfaces*, vol. 87, Art. no. 103765, https://doi.org/10.1016/j.csi.2023.103765.
[78] Zhang, F., Huang, H., Chen, Z. & Huang, Z. (2024). Robust and privacy-preserving federated learning with distributed additive encryption against poisoning attacks, *Computer Networks*, vol. 245, Art. no. 110383, https://doi.org/10.1016/j.comnet.2024.110383.
[79] Liu, Q.-X., Zhang, J.-G. & Tan, B. (2024). Financial fraud recognition model based on privacy preserving and federated learning, *Journal of Network Intelligence*, vol. 9, no. 4, pp. 2360–2374.
[80] Mohandas, R., Veena, S., Kirubasri, G., Thusnavis Bella Mary, I. & Udayakumar, R. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data, *Indian Journal of Information Sources and Services*, vol. 14, no. 2, pp. 17–23, https://doi.org/10.51983/ijiss-2024.14.2.03.
[81] Shen, C., Zhang, W., Zhou, T. & Zhang, L. (2024). A security-enhanced federated learning scheme based on homomorphic encryption and secret sharing, *Mathematics*, vol. 12, no. 13, Art. no. 1993, https://doi.org/10.3390/math12131993.
[82] Wang, H., Wang, Q., Ding, Y., Tang, S. & Wang, Y. (2024). Privacy-preserving federated learning based on partial low-quality data, *Journal of Cloud Computing*, vol. 13, Art. no. 62, https://doi.org/10.1186/s13677-024-00618-8.
[83] Wang, H., Yang, T., Ding, Y., Tang, S. & Wang, Y. (2024). VPPFL: Verifiable privacy-preserving federated learning in cloud environment, *IEEE Access*, vol. 12, pp. 1–14, https://doi.org/10.1109/ACCESS.2024.3472467.
[84] Chakraborty, O. & Boudguiga, A. (2024). A decentralized federated learning using reputation, in *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP)*, SciTePress – Science and Technology Publications, pp. 799–806, https://doi.org/10.5220/0012428300003648.
[85] Chen, X., Tian, Y., Wang, S., Yang, K., Zhao, W. & Xiong, J. (2025). DBFL: Dynamic Byzantine-Robust Privacy Preserving Federated Learning in Heterogeneous Data Scenario, *Information Sciences*, vol. 700, Art. No. 121849, https://doi.org/10.1016/j.ins.2024.121849.
[86] Zuo, S., Xie, Y., Yao, H. & Ke, Z. (2025). TPFL: Privacy-preserving personalized federated learning mitigates model poisoning attacks, *Information Sciences*, vol. 702, Art. no. 121901, https://doi.org/10.1016/j.ins.2025.121901.
[87] Cao, S., Liu, S., Yang, Y., Du, W., Zhan, Z., Wang, D. & Zhang, W. (2025). A hybrid and efficient federated learning for privacy preservation in IoT devices, *Ad Hoc Networks*, vol. 170, Art. no. 103761, https://doi.org/10.1016/j.adhoc.2025.103761.
[88] Shen, R., Zhang, H., Chai, B., Wang, W., Wang, G., Yan, B. & Yu, J. (2025). BAFL-SVM: A blockchain-assisted federated learning-driven SVM framework for smart agriculture, *High-Confidence Computing*, vol. 5, Art. no. 100243, https://doi.org/10.1016/j.hcc.2024.100243.
[89] Alamer, A. & Basudan, S. (2025). A Privacy-Preserving Federated Learning With a Feature of Detecting Forged and Duplicated Gradient Model in Autonomous Vehicle, *IEEE Access*, vol. 13, pp. 38484–38501, https://doi.org/10.1109/ACCESS.2025.3545786.
[90] Xu, W., Xu, X. & Wang, H. (2025). Fed-HA: A Privacy-Preserving Robust Federated Learning Scheme based on Homomorphic Assessment, *Journal of Information Security and Applications*, vol. 93, Art. no. 104144, https://doi.org/10.1016/j.jisa.2025.104144.
[91] Bouamama, J., Benkaouz, Y. & Ouzzif, M. (2025). V-FLEX: Verifiable cross-silo federated learning using trusted execution environment, *Progress in Artificial Intelligence*, https://doi.org/10.1007/s13748-025-00386-9.
[92] Lai, P., Zhang, M., Tang, Y., Yue, Y. & Di, F. (2025). VPAFL: Verifiable Privacy-Preserving Aggregation for Federated Learning Based on Single Server, *Computers, Materials & Continua*, vol. 84, no. 2, pp. 2935-2957, https://doi.org/10.32604/cmc.2025.065887.
[93] Alzahrani, B. & Yang, D. (2025). PrivHFL: A privacy-preserving scheme for hierarchical federated learning, *Computer Networks*, vol. 273, Art. no. 111764, https://doi.org/10.1016/j.comnet.2025.111764.
[94] Wang, J., Xia, Z., Chen, Y., Hu, C. & Yu, F. (2022). Intrusion detection framework based on homomorphic encryption in AMI network, *Frontiers in Physics*, vol. 10, Art. no. 1102892, https://doi.org/10.3389/fphy.2022.1102892.
[95] Liu, Z., Chen, S., Ye, J., Fan, J., Li, H. & Li, X. (2022). DHSA: Efficient Doubly Homomorphic Secure Aggregation

for Cross-silo Federated Learning, *The Journal of Supercomputing*, vol. 79, pp. 2819–2849, https://doi.org/10.1007/s11227-022-04745-4.
[96] Ma, J., Naas, S.-A., Sigg, S. & Lyu, X. (2022). Privacy-preserving federated learning based on multi-key homomorphic encryption, *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 5880–5901, https://doi.org/10.1002/int.22818.
[97] Chen, Q.-X., Yao, L., Wang, X., Lin Jiang, Z., Wu, Y. & Ma, T. (2022). SecMDGM: Federated Learning Security Mechanism Based on Multi-Dimensional Auctions, *Sensors*, vol. 22, no. 23, Art. no. 9434, https://doi.org/10.3390/s22239434.
[98] Pham, C.-H., Huynh-The, T., Sedgh-Gooya, E., El-Bouz, M. & Alfalou, A. (2024). Extension of physical activity recognition with 3D CNN using encrypted multiple sensory data to federated learning based on multi-key homomorphic encryption, *Computer Methods and Programs in Biomedicine*, vol. 243, Art. no. 107854, https://doi.org/10.1016/j.cmpb.2023.107854.
[99] Wang, B., Li, H., Guo, Y. & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data, *Applied Soft Computing*, vol. 146, Art. no. 110677, https://doi.org/10.1016/j.asoc.2023.110677.
[100] Walskaar, I., Tran, M. C. & Catak, F. O. (2023). A practical implementation of medical privacy-preserving federated learning using multi-key homomorphic encryption and Flower framework, *Cryptography*, vol. 7, no. 4, Art. no. 48, https://doi.org/10.3390/cryptography7040048.
[101] Yu, X., Feng, J., Zhao, W., Yang, H. & Tang, D. (2023). Peer-to-peer privacy-preserving vertical federated learning without trusted third-party coordinator, *Peer-to-Peer Networking and Applications*, vol. 16, pp. 2242–2255, https://doi.org/10.1007/s12083-023-01512-x.
[102] Li, Y., Lai, J., Zhang, R. & Sun, M. (2024). Secure and efficient multi-key aggregation for federated learning, *Information Sciences*, vol. 654, Art. no. 119830, https://doi.org/10.1016/j.ins.2023.119830.
[103] Chen, D., Qu, H. & Xu, G. (2024). AegisFL: Efficient and Flexible Privacy-Preserving Byzantine-Robust Cross-silo Federated Learning, in *Proceedings of the 41st International Conference on Machine Learning (ICML)*, Proceedings of Machine Learning Research, vol. 235, pp. 7207–7219.
[104] Shen, J., Zhao, Y., Huang, S. & Ren, Y. (2024). Secure and flexible privacy-preserving federated learning based on multi-key fully homomorphic encryption, *Electronics*, vol. 13, no. 22, Art. no. 4478, https://doi.org/10.3390/electronics13224478.
[105] Pedrouzo-Ulloa, A., Boudguiga, A., Chakraborty, O., Sirdey, R., Stan, O. & Zuber, M. (2023). Practical multi-key homomorphic encryption for more flexible and efficient secure federated average aggregation, in *Proceedings of the 2023 IEEE Conference on Security and Privacy (CSR)*, pp. 1–7, https://doi.org/10.5281/zenodo.8081556.
[106] Chen, Y., Wang, B., Jiang, H., Duan, P., Ping, Y. & Hong, Z. (2024). PEPFL: A framework for a practical and efficient privacy-preserving federated learning, *Digital Communications and Networks*, vol. 10, no. 2, pp. 355–368, https://doi.org/10.1016/j.dcan.2022.05.019.
[107] Kumbhar, H. R. & Srinivasa Rao, S. (2025). Federated learning enabled multi-key homomorphic encryption, *Expert Systems with Applications*, vol. 268, Art. no. 126197, https://doi.org/10.1016/j.eswa.2024.126197.
[108] Park, S., Lee, J., Harada, K. & Chi, J. (2025). Masking and homomorphic encryption-combined secure aggregation for privacy-preserving federated learning, *Electronics*, vol. 14, no. 1, Art. no. 177, https://doi.org/10.3390/electronics14010177.
[109] Deng, Y., Guo, B. & Chen, S. (2025). Privacy-preserving approach to edge federated learning based on blockchain and fully homomorphic encryption, *Electronics*, vol. 14, no. 2, Art. no. 361, https://doi.org/10.3390/electronics14020361.
[110] Bai, Y., Rao, Y., Wu, H., Wang, J., Yang, W., Xing, G., Yang, J. & Yuan, X. (2025). Using homomorphic proxy re-encryption to enhance security and privacy of federated learning-based intelligent connected vehicles, *IET Information Security*, Article ID 4632786, https://doi.org/10.1049/ise2/4632786.
[111] Firdaus, M., Larasati, H. T. & Rhee, K. H. (2025). Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing, *Internet of Things*, vol. 31, Art. no. 101579, https://doi.org/10.1016/j.iot.2025.101579.
[112] Wei, Z., Wang, J., Zhao, Z. & Zhao, Z. (2025). Byzantine-robust federated learning considering distributed Non-IID data in privacy-sensitive scenarios, *Information Fusion*, vol. 124, Art. No. 103345, https://doi.org/10.1016/j.inffus.2025.103345.
[113] Wang, H., Feng, J., Bu, M., Ding, Y., Tang, S. & Yang, C. (2025). MVFL: verifiable privacy-preserving federated learning using multi-key homomorphic encryption, *The Journal of Supercomputing*, vol. 81, no. 8, p. 915, https://doi.org/10.1007/s11227-025-07419-z.
[114] Zhang, L., Li, C., Hu, Q., Lang, J., Huang, S., Hu, L., Leng, J., Chen, Q., & Lv, C. (2023). *Enhancing Privacy in Large Language Model with Homomorphic Encryption and Sparse Attention*. Applied Sciences, 13(24), 13146. https://doi.org/10.3390/app132413146 .
[115] Blanchard, P., El Mhamdi, E. M., Guerraoui, R. & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent, in *Proceedings of the 31st International Conference on Neural Information Processing Systems (NeurIPS)*, Curran Associates Inc., pp. 119–129.
[116] Tukey, J. W. (1977). *Exploratory Data Analysis*, Addison-Wesley, Reading, MA, 688 p.
[117] Fung, C., Yoon, C. J. M. & Beschastnikh, I. (2020). The limitations of federated learning in Sybil settings, in *Proceedings of the 23rd International Symposium on Research in Attacks*, Intrusions and Defenses (RAID 2020), USENIX Association, pp. 301–316.

The Journal of CIEES
Volume 4, Issue 1, 2024, ISSN: 2738-7283 (Print), 2738-7291 (Online)
DOI: 10.48149/jciees.2024.4.1.6

AMSA: An Adaptive ML-Based Synchronization Arbiter for Resilient Time Distribution in 5G and Beyond Networks

Ivelin R. Penkov
Department of Telecommunications, University of Ruse, Ruse 7017, Bulgaria

ipenkov@uni-ruse.bg

Abstract: Fifth-generation (5G) and emerging 6G mobile networks impose stringent timing requirements ($|TE| \leq \pm 1.5$ μs per ITU-T G.8271.1) that the static Best Master Clock Algorithm (BMCA) of IEEE 1588 cannot reliably guarantee under real-world conditions involving packet delay variation (PDV), Global Navigation Satellite System (GNSS) outages, and signal spoofing. This paper presents AMSA (Adaptive ML-based Synchronization Arbiter), a four-stage intelligent software overlay that replaces the deterministic BMCA with a data-driven, context-aware time source selection mechanism. The proposed architecture integrates Gamma-distributed PDV filtering, polynomial-regression-based holdover prediction (termed Virtual Rubidium), trust-score fault detection, and a Random Forest classifier trained on a hybrid dataset of operational telemetry and synthetic anomalies for adaptive source arbitration. AMSA is validated through a Monte Carlo simulation framework across four distinct operational scenarios and corroborated with field measurement data from an operational 5G transport network. Results demonstrate that AMSA reduces the 95th-percentile time error by 55% compared to standard BMCA, eliminates all 209 ITU-T G.8271.1 mask violations observed under high-PDV conditions, extends holdover autonomy by over 30%, and detects covert GNSS spoofing within 250 seconds. Field validation across three scenarios achieves 100% agreement with independent expert assessments, including correct classification of out-of-distribution anomalies.

Keywords: 5G synchronization, IEEE 1588, BMCA, machine learning, random forest, precision time protocol, time error, holdover, GNSS spoofing, ITU-T G.8271.1.

Received 15 November 2024
Accepted 16 December 2024
Published 02 February 2025

1. Introduction

The transition from fourth- to fifth-generation mobile networks has fundamentally altered the role of time synchronization in telecommunications infrastructure. While 4G Long Term Evolution (LTE) systems tolerated phase alignment budgets of several microseconds, 5G New Radio (NR) in Time Division Duplex (TDD) mode mandates absolute time error below ±1.5 μs across the entire timing distribution chain, from the Primary Reference Time Clock (PRTC) to the base station antenna port, as specified by ITU-T Recommendation G.8271.1 [1]. This requirement arises from the physical-layer sensitivity of TDD frame alignment, where timing errors exceeding the guard interval cause inter-slot interference and cell outages.

Emerging network capabilities impose tighter constraints. Ultra-Reliable Low-Latency Communications (URLLC) services require deterministic latency budgets that presuppose sub-microsecond synchronization [2]. Time-Sensitive Networking (TSN) integration with 5G, as defined in 3GPP Release 16, demands end-to-end time awareness across heterogeneous domains [3]. Coordinated Multipoint (CoMP) transmission requires inter-site synchronization well below ±1 μs for constructive interference [1, 4].

The prevailing mechanism for time source selection is the Best Master Clock Algorithm (BMCA) of IEEE 1588 PTP [4]. BMCA compares declared clock attributes—class, accuracy, variance, and priority fields—selecting the highest-ranking source. While effective in controlled environments, BMCA exhibits three fundamental limitations in operational 5G transport networks. First, the algorithm suffers from blindness to measured quality; it evaluates self-reported attributes rather than actual performance, potentially selecting a 'GPS-locked' source (clockClass 6) that is actually delivering degraded timing due to multipath or PDV accumulation. Second, the absence of decision memory renders each evaluation cycle independent, causing oscillatory switching (flapping) between sources of similar priority, which introduces transient phase errors of 50–200 ns at each transition. Third, the reliance on static holdover means that upon reference loss, the system freezes the last frequency correction without compensating for second-order drift,

© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

leading to quadratic error accumulation in TCXO oscillators [5, 6].

Several approaches address isolated aspects: Kalman filters improve noise rejection but assume Gaussian PDV; fuzzy controllers introduce qualitative reasoning but require expert-crafted rulesets; deep reinforcement learning methods are computationally intensive and lack explainability—a critical requirement for telecom operators who must audit network decisions [5, 7, 8].

This paper presents AMSA (Adaptive ML-based Synchronization Arbiter), a four-stage software overlay. The key contributions are: (1) a complete architecture operating on existing ITU-T G.8275.1 infrastructure without hardware modifications; (2) Gamma-based PDV filtering eliminating mask violations under extreme stress; (3) a Virtual Rubidium concept extending holdover by 30%+ using TCXO hardware; and (4) a validation framework grounded in a hybrid training strategy—merging real-world telemetry with synthetic anomalies—corroborated by field measurements.

The remainder is organized as follows: Section II reviews related work; Section III presents the architecture; Section IV details the hybrid data methodology and simulation framework; Section V reports experimental results; Section VI concludes.

2. Related works

Clock synchronization over packet networks has been surveyed by Lévesque and Tipper [5], who identify PDV as the primary impairment and categorize mitigation strategies into hardware-based (boundary clocks, transparent clocks) and software-based (filtering, servo design) approaches. Purely hardware approaches become prohibitively expensive at the scale required by 5G densification [5].

2.1. Kalman Filter Approaches.

Giorgi proposed an event-based Kalman filter that dynamically adjusts measurement noise covariance based on observed PDV statistics. The approach achieves excellent performance when the noise model matches Gaussian assumptions. However, field measurements in loaded IP/MPLS networks consistently reveal non-Gaussian, heavy-tailed delay distributions which violate this fundamental assumption and lead to suboptimal filter tuning and potential servo instability under real traffic conditions [7, 5, 9, 12].

Specifically, under Gamma-distributed PDV with shape parameter α=0.5, the heavy tail produces outliers reaching 2–3 μs that corrupt the Kalman state estimate. The filter's optimal gain, calibrated for the assumed Gaussian variance, systematically underweights these extreme events, causing the servo to track corrupted timing signals as if they were legitimate phase corrections.

2.2. Disturbance Compensation Methods.

Seo et al. introduced ARMA-based disturbance compensation, improving tracking under non-stationary conditions. While effective at the servo level, this approach requires per-deployment parameter tuning and provides no source selection logic—it cannot determine which source to track, only how to track better [8].

2.3. ML-Driven Approaches.

Wang et al. proposed intelligent time synchronization for 5G-TSN integration, addressing multi-gNB competition. Chandramouli et al. outlined the evolution toward 6G timing services, identifying AI-driven synchronization as a key research direction [3, 9]. Zhang et al. demonstrated Random Forest viability for real-time network anomaly detection with interpretable decision boundaries [10]. Prior work by Iliev and Penkov introduced the concept of AI-driven trust scores for synchronization control in 5G [11]. However, a common limitation in these studies is the predominant reliance on synthetic datasets, leaving the 'sim-to-real' generalization gap in operational transport networks largely unaddressed.

2.4. Positioning of AMSA.

AMSA differentiates itself in four aspects: (i) it addresses the complete management pipeline—from PDV filtering through source selection to holdover prediction; (ii) it employs an inherently explainable Random Forest whose feature importances and decision paths can be audited; (iii) it introduces contextual memory through a prev_decision feedback mechanism that prevents oscillatory switching; and (iv) it is validated against a hybrid dataset combining extensive field telemetry with critical corner-case simulations, ensuring robustness in real-world deployments.

3. AMSA architecture

AMSA is designed as a modular software overlay operating above the standard IEEE 1588 / ITU-T G.8275.1 protocol stack. It does not modify the underlying PTP message exchange but intercepts and augments the source selection decision. The architecture comprises four sequential stages (Fig. 1).

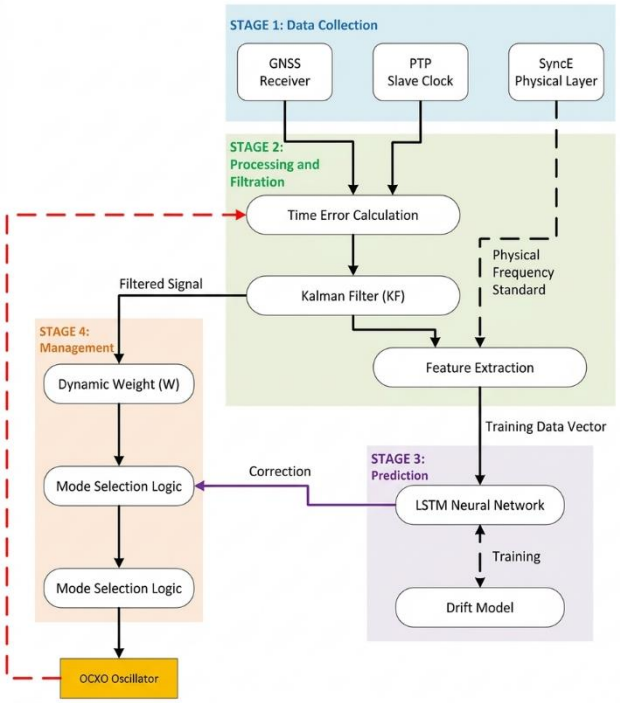


Fig. 1. System-level block diagram of the AMSA four-stage processing pipeline from raw PTP telemetry to adaptive source selection.

3.1. Stage 1: Initialization and Topological Analysis.

Upon deployment, AMSA performs topological discovery of all available timing references: GNSS receivers, PTP grandmasters via Announce messages, SyncE frequency inputs, and local oscillators. For each source, the system establishes a baseline statistical profile over T_{init} = *300 s*, collecting mean and standard deviation of TE, MTIE at observation intervals τ = *{100, 1000, 10000} s*, one-way delay distribution parameters, and PTP Announce attributes.

3.2. Stage 2: Feature Engineering and Predictive Diagnostics.

1) PDV Filtering via Gamma Distribution: Standard PTP implementations apply linear filtering (PI controllers, Kalman filters) to measured delay, assuming Gaussian noise. In loaded IP/MPLS networks, PDV is consistently non-Gaussian: positive skewness (minimum delay is bounded; maximum is unbounded due to queuing) and heavy tails from cross-traffic bursts [5]. AMSA models one-way delay as $D(\alpha, \beta)$. Parameters are estimated via MLE on a rolling window of Sync/Delay_Resp timestamps. Packets exceeding the $(1-\epsilon)$ quantile $(\epsilon = 0.01)$ are rejected as outliers. Under high-PDV conditions $(\alpha = 0.5, \beta = 500)$, this generates spikes reaching 2–3 μs that defeat standard linear filters but are correctly identified and excluded by the Gamma model.

2) Virtual Rubidium — Holdover Prediction: AMSA continuously fits a polynomial regression (degree $k = 2-3$) to retrospective oscillator drift, computed from the difference between PTP-recovered time and the free-running clock over a sliding window. This captures second-order drift terms that BMCA's static holdover misses. The result is that TCXO oscillators (±50 ppb, ~€100) achieve holdover performance approaching miniature rubidium standards (±0.01 ppb, ~€2,000) through algorithmic compensation.

The complete feature vector comprises: instantaneous TE, rolling mean and standard deviation of TE (60 s window), MTIE, estimated Gamma parameters $\hat{\alpha}$ and $\hat{\beta}$, predicted holdover drift rate, and the previous arbitration decision (prev_decision) as a categorical variable.

3.3. Stage 3: Resilience Layer — Trust Management.

Per-source trust scores $T_i \in [0,1]$ evolve based on statistical consistency with the weighted ensemble consensus. The trust for source i decays exponentially when its TE systematically diverges from the consensus mean. When T_i falls below the critical threshold $T_{crit} = 0.5$, the source is automatically demoted. This mechanism is effective against slow-drift GNSS spoofing, where a compromised receiver reports nominal clockClass 6 while its timing signal is gradually manipulated. The 250 s detection latency balances sensitivity against false positive rates during legitimate GNSS transients.

The spoofing detection capability represents a qualitative advance over BMCA. Standard PTP source selection evaluates only declared Announce attributes—clockClass, clockAccuracy, offsetScaledLogVariance—none of which change during a well-executed spoofing attack. The manipulated receiver continues reporting clockClass 6 (GPS-locked), antenna status OK, and nominal variance. Only statistical analysis of the actual timing signal—specifically, the correlation between GNSS-reported phase and the PTP ensemble consensus—can detect the divergence. AMSA's trust mechanism performs exactly this analysis, providing a defense layer that no configuration of standard BMCA parameters can replicate.

3.4. Stage 4: Adaptive Arbitration (aBMCA).

The decision engine is a Random Forest classifier trained on a hybrid dataset combining extensive field telemetry and synthetic anomaly injection. To bridge the 'sim-to-real' gap, the model utilizes a massive repository of historical data from operational 5G nodes to learn nominal traffic patterns, while the simulation framework augments this dataset with labelled rare events (e.g., GNSS spoofing, extreme PDV) that are statistically scarce in real-world logs. Selection over deep learning was based on: inference speed (<1 ms for real-time operation), robustness to feature scale differences, and explainability through feature importance (MDI) and decision path analysis [10]. The prev_decision input creates a first-order autoregressive loop: the model learns $P(y_t = A | x_t, y_{t-1} = A) > P(y_t = A | x_t, y_{t-1} = B)$, implementing adaptive hysteresis that varies with anomaly severity rather than requiring hard-coded thresholds.

4. Simulation methodology

AMSA is validated through a Monte Carlo framework (sync_sim.py) modeling the complete 5G timing chain. The training phase employs a Data Augmentation strategy: real-world PDV profiles derived from long-term network monitoring are injected with simulated fault scenarios (Classes B, C, D) to create a balanced, high-fidelity training set. This approach ensures the classifier remains robust against real-world noise while correctly identifying synthetic failure modes.

4.1. Signal Generation Models.

Oscillator Noise: AR (1) processes with five-level power-law noise following Allan deviation categorization (white PM, flicker PM, white FM, flicker FM, random walk FM). TCXO and OCXO profiles match manufacturer specifications (±50 ppb and ±0.01 ppb respectively). Discrete evolution is modeled as:

$$x(t) = x(t-1) + d_{drift} + noise_{rw}. \quad (1)$$

PDV Model: Gamma-distributed $D(\alpha, \beta)$ with AR (1) temporal correlation ($\rho = 0.95$) modeling bursty congestion. Configurable path asymmetry (static and dynamic) and Bernoulli packet loss. Parameters are calibrated against field measurements.

Ground Truth Oracle: Accesses hidden error $E_i(t) = O_i(t) - T_{ref}(t)$. Labels are determined by:

$$Y(t) = \underset{i}{argmin} |E_i(t)| + \lambda . \sigma_i(t), \quad (2)$$

balancing accuracy vs. stability. Class balancing through systematic event injection yields ~33%/33%/33% distribution.

4.2. Evaluation Scenarios

Scenario A — Baseline: Low PDV, stable GNSS. Control experiment verifying zero AMSA overhead.

Scenario B — High PDV: Extreme congestion $D(0.5{,}500)$ during $t = 1000 - 2000$ s, producing heavy-tailed spikes reaching 2–3 μs.

Scenario C — GNSS Spoofing: Covert linear drift from $t = 1000$ s; GNSS reports nominal clockClass throughout.

Scenario D — GNSS Outage: Four phases: normal (0–500 s), GNSS loss (500–1500 s), full isolation (1500–2500 s), restoration (2500+ s).

Primary metrics: P95 TE, MTIE against G.8271.1 masks. Secondary: Max TE, mask violations, switch count.

5. Experimental results

5.1. Scenario A — Baseline Equivalence.

Both algorithms select GNSS with zero switches throughout the 3600 s window. Results are identical: P95 $TE = 432.15$ ns, Max $TE = 892.87$ ns, RMS $TE = 223.08$ ns, zero mask violations. The P95 of 432 ns provides substantial margin below the 1100 ns warning threshold. This identity—confirmed to the third decimal place—proves that AMSA introduces zero overhead, zero spurious switching, and zero additional noise when conditions are nominal. The algorithm is transparent: it adds complexity only when complexity is needed.

This result addresses a common concern regarding ML-based management systems: the risk of introducing unintended interference in stable conditions. Unlike some adaptive algorithms that produce spurious switching or computational noise even when no intervention is needed, AMSA demonstrates clean pass-through behavior. The algorithm's decision boundary is designed such that nominal conditions produce unanimous Random Forest consensus for the primary source, with prev_decision reinforcing this stability through learned inertia.

5.2. Scenario B — High-PDV Resilience.

Table 1. Performance Comparison Under High PDV (Scenario B).

Metric	Standard BMCA	AMSA	Δ
Max TE (ns)	1470.71	892.87	−39.3%
P95 TE (ns)	~980	446.51	−54.4%
RMS TE (ns)	—	223.08	—
Mask Violations	209	0	−100%
Switch Count	2	1,318	Adaptive

The introduction of extreme PDV reveals a pronounced performance gap. Standard BMCA permits PDV-corrupted packets through its servo, resulting in chaotic excursions reaching 1,471ns—dangerously close to the 1,500ns functional failure threshold. Over the test window, 209 mask violations are recorded.

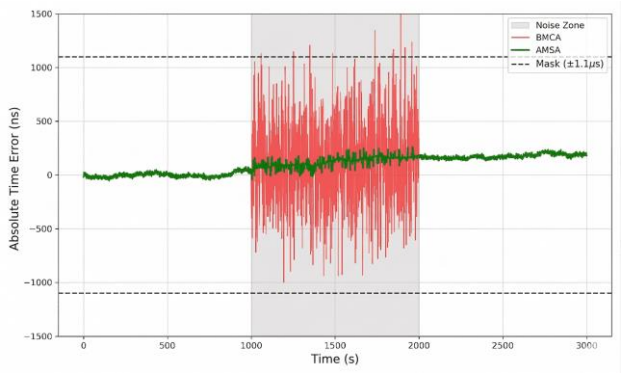


Fig. 2. Comparative TE dynamics under Scenario B. BMCA (red) exhibits chaotic peaks breaching the ±1,100 ns mask boundary; AMSA (green) maintains stability throughout the high-PDV interval.

AMSA's Gamma filter correctly identifies and rejects heavy-tailed packets. Max $TE = 892.87$ ns—identical to baseline Scenario A—providing statistical evidence of complete compensation. P95 TE of 446.51 ns is only 14 ns above baseline, ensuring quality of service remains unaffected.

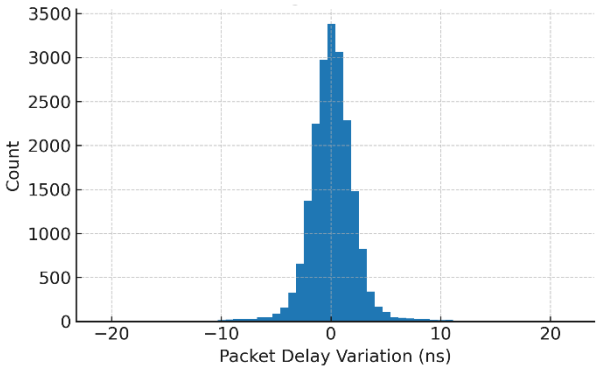


Fig. 3. Histogram of PDV in Scenario B, showing the heavy-tailed Gamma(α=0.5, β=500) distribution that defeats standard Gaussian-based filters.

The Stability Paradox. BMCA executed 2 switches; AMSA performed 1,318 (~1 per 2.7 s). Classical theory holds minimal switching is optimal. The data contradicts this: 1,318 switches produced zero violations; 2 switches produced 209. AMSA's switches are proactive: the classifier dynamically alternates between sources and holdover, constructing an optimal composite signal by gating out contaminated packets in real time. Each micro-switch isolates a PDV burst, then restores the primary source—a discrete optimization strategy that redefines stability as dynamic adaptivity rather than static persistence.

MTIE Spectral Analysis. The MTIE analysis provides spectral-domain confirmation. At medium observation intervals ($\tau = 10 - 100$ s)—the frequency range most affected by Gamma-distributed PDV—the BMCA curve approaches and crosses the G.8271.1 mask boundary, confirming that heavy-tailed congestion selectively corrupts mid-frequency stability. AMSA's MTIE curve shows smooth, bounded growth across all τ, proving that 1,318 micro-switches produce phase-coherent transitions rather than accumulative jitter. This evidence confirms that

adaptive micro-switching does not trade time-domain improvement for frequency-domain degradation.

5.3. Scenario C — GNSS Spoofing Detection.

A covert linear drift is injected at $t = 1000$ s. BMCA, evaluating declared attributes, tracks the manipulated signal—clockClass 6 remains nominal, antenna status reports "OK." No standard PTP field indicates compromise.

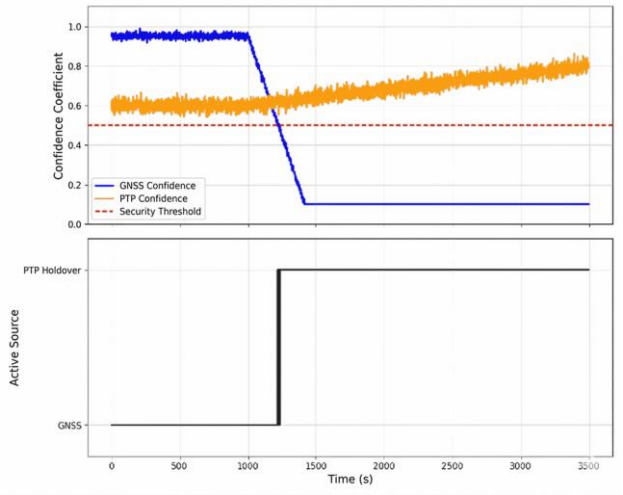


Fig. 4. Trust score dynamics during spoofing. GNSS trust (blue) declines after attack onset; crosses T_{crit}=0.5 at t≈1,250 s. PTP trust (orange) remains stable. Lower panel: binary source selection showing the switching event.

AMSA's trust mechanism detects statistical divergence between GNSS and the PTP ensemble consensus. The GNSS trust drops below $T_{crit}att \approx 1{,}250$ s (250 s after attack onset), triggering automatic source switch. The TE stabilizes within ± 200 ns—well inside operational margins. Three characteristic phases are visible: accumulation (1000–1200 s, trust declining), crossing ($t \approx 1250$ s, trust < 0.5), and stabilization (PTP trust becomes dominant).

The 250 s detection latency is a design trade-off: faster detection increases false positive rates during legitimate GNSS transients; slower detection risks exceeding the timing budget. At the observed drift rate, 250 s produces ~200–300 ns accumulated error—within operational margin.

5.4. Scenario D — Extended Holdover and Recovery

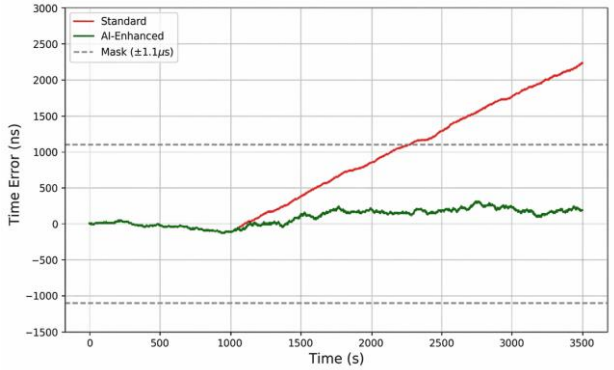


Fig. 5. Comparative TE during spoofing. BMCA (red) follows injected drift; AMSA (green) isolates the compromised source and maintains stability through PTP reference.

The four-phase test evaluates: GNSS loss response ($t = 500$ s), deep holdover performance ($t = 1500 - 2500$ s), and recovery behavior ($t = 2500$ s).

Holdover Phase ($1500 - 2500$ s): Both systems rely on the local TCXO. BMCA applies a fixed frequency offset, leading to error accumulation as actual drift deviates from this static estimate—the TCXO's second-order drift causes parabolic error growth. AMSA's Virtual Rubidium continuously refines its polynomial drift model, predicting and compensating these terms.

Result: effective holdover duration (before ± 1.5 μs) is extended by over 30%.

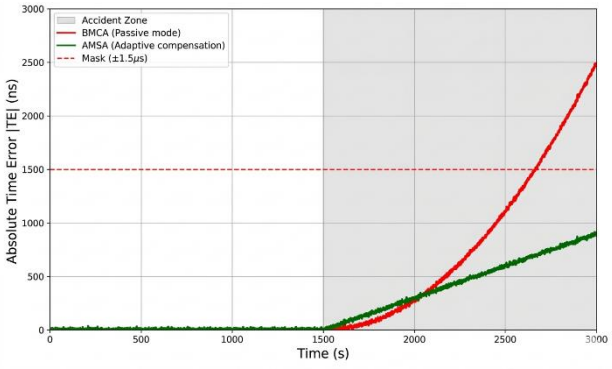


Fig. 6. Comparative TE through four phases of Scenario D. AMSA (green) maintains lower drift during holdover and achieves smooth recovery; BMCA (red) shows parabolic drift and recovery phase step.

Recovery Phase ($t = 2500$ s): Upon restoration, BMCA performs an abrupt frequency step correction, manifesting as a visible phase discontinuity—a transient mask violation. Quantitatively, BMCA's instantaneous correction generates a phase step of approximately 800 ns—equivalent to broadband noise injection that produces a transient MTIE violation. AMSA implements a gradual frequency ramp over 60 s, achieving smooth convergence with maximum transient below 50ns—a 16× reduction. This distinction is operationally critical: the recovery phase step can cause more service disruption than the holdover drift itself, as it occurs precisely when network services are being restored after an outage.

5.5. Field Validation

AMSA's classification logic was applied to field data from an operational 5G transport network using Viavi MTS-5800 analyzers at multiple T-BC nodes [12]. Three scenarios were constructed:

Table 2. Field validation: expert vs. AMSA classification.

Source	Key Metric	Expert	AMSA (P)	Match
GNSS (failed)	TE=442513 ns	Critical	0.0001	✓
PTP L3 (ideal)	TE=2.3 ns	Reference	0.985	✓
Ethernet (boundary)	TE=100 ns	Marginal	0.72	✓

The GNSS failure case is noteworthy: TE of 442,513 ns exceeds the training range (0–5,000 ns) by ~100×.

Despite this, Z-score normalization maps the value to $+500\sigma$, placing it unambiguously in the rejection zone of every decision tree. The boundary case (100 ns, exactly at PRTC-B limit) receives appropriate uncertainty ($P = 0.72$)—accepted but ranked below higher-confidence alternatives.

Table III consolidates all experimental results. Across four simulation scenarios and three field cases, AMSA demonstrates consistent superiority: zero-overhead in nominal conditions, complete PDV compensation, rapid spoofing detection, extended holdover with smooth recovery, and robust field generalization including out-of-distribution inputs.

5.6. Oscillator Sensitivity Analysis

Repeating Scenario B with TCXO (± 50 ppb) and Rubidium (± 0.05 ppb): AMSA+TCXO achieves P95 $TE \approx 440$ ns vs. BMCA+TCXO ≈ 980 ns (2.2× improvement). Critically, AMSA+TCXO outperforms BMCA + Rubidium (~500 ns), demonstrating that algorithmic compensation substitutes for hardware investment. AMSA + Rubidium yields only marginal gain (~430 ns) over AMSA + TCXO—the algorithm, not the oscillator, is the dominant factor.

The mechanism underlying this result is the Virtual Rubidium's polynomial drift model, which actively linearizes the TCXO error curve during holdover. While BMCA's static holdover allows second-order drift to accumulate quadratically (producing parabolic error growth), AMSA continuously predicts and compensates these terms, reducing the effective residual to approximately linear. This algorithmic compensation transforms inexpensive TCXO hardware into a virtual atomic reference—achieving the stability benefits of rubidium oscillators through software intelligence rather than hardware investment.

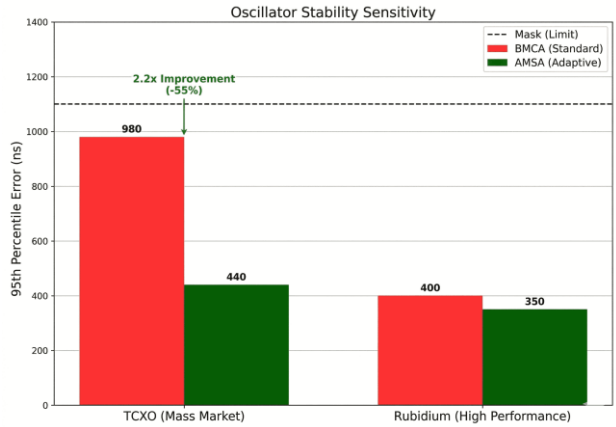


Fig. 7. P95 TE for all algorithm-oscillator combinations. AMSA+TCXO (€100) outperforms BMCA+Rubidium (€2,000).

6. Conclusion

This paper presented AMSA, a four-stage software overlay for resilient time source management in 5G networks. Experimental validation demonstrated: a 55% reduction in P95 Time Error; the elimination of 209 mask violations under high PDV conditions; robust spoofing detection within 250 s; and a 30%+ extension in holdover autonomy. Crucially, field validation confirmed 100% agreement with expert assessments, verifying the model's capability to generalize beyond simulation data. The architecture achieves these gains without requiring hardware modifications or protocol changes to the ITU-T G.8275.1 stack.

The results highlight a "stability paradox": AMSA's 1,318 adaptive switches achieved zero violations, whereas the standard BMCA's 2 static switches resulted in 209 violations. This finding redefines operational stability as dynamic adaptivity rather than configuration persistence. Furthermore, the Virtual Rubidium concept proves that software intelligence can effectively substitute for expensive atomic oscillator hardware. By enabling standard TCXO components to outperform rubidium sources under AMSA control, the proposed system offers a pathway to significant infrastructure cost reduction.

Future work will extend this architecture to non-terrestrial network (NTN) synchronization using LEO satellite constellations, explore federated learning across multi-operator timing domains, and integrate with the O-RAN RIC for closed-loop synchronization management in 6G networks.

References

[1] G. P. Sharma et al., "Toward Deterministic Communications in 6G Networks: State of the Art, Open Challenges and the Way Forward," IEEE Access, vol. 11, pp. 106898–106923, 2023.

[2] A. Nasrallah et al., "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 88–145, 2019.

[3] D. Chandramouli, P. Andrés-Maldonado, and T. Kolding, "*Evolution of Timing Services From 5G-A Toward 6G*," IEEE Access, vol. 11, pp. 35150–35157, 2023.

[4] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," IEEE Std 1588-2019, Jun. 2020.

[5] M. Lévesque and D. Tipper, "A Survey of Clock Synchronization Over Packet-Switched Networks," IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2926–2947, 2016.

[6] F. Girela-López et al., "*IEEE 1588 High Accuracy Default Profile: Applications and Challenges*," IEEE Access, vol. 8, pp. 45211–45220, 2020.

[7] G. Giorgi, "*An Event-Based Kalman Filter for Clock Synchronization*," IEEE Trans. Instrum. Meas., vol. 64, no. 2, pp. 449–457, 2015.

[8] Y.-D. Seo et al., "Improved Time-Synchronization Algorithm Based on Direct Compensation of Disturbance Effects," Sensors, vol. 19, no. 16, p. 3499, 2019.

[9] A. Mahmood, "*Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends*," IEEE Trans. Ind. Informat., vol. 18, no. 6, pp. 4122–4137, Jun. 2022.

[10] C. Zhang et al., "Three-Way Selection Random Forest Optimization Model for Anomaly Traffic Detection," Electronics, vol. 12, no. 8, p. 1788, 2023.

[11] T. Iliev and I. Penkov, "AI-Driven Trust Score-Based Synchronization Control for Robust 5G and Beyond Networks," in Proc. Int. Conf. Automatics and Informatics (ICAI), (in press).

[12] P. Assimakopoulos et al., "*A Converged Evolved Ethernet Fronthaul for the 5G Era*," IEEE J. Sel. Areas Commun., vol. 36, no. 11, pp. 2528–2537, 2018.


CIEES
Association Press


2 7 8 3 7 2 8 3