ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 10, No. 2, 2025

# ANALYSIS AND IMPROVEMENT OF INFORMATION SECURITY TECHNOLOGIES IN DISTRIBUTED AND ASYMMETRIC SYSTEMS

***Ruslan Zapukhlyak[1], Myroslav Pavliuk[1], Iryna Svyd[1], Bohdan Dzundza[1], Viktor Dovhyi[1], Vitalii Martyniuk[1], Haider Th. Salim ALRikabi[2]***

*[1] Vasyl Stefanyk Carpathian National University, 57, Shevchenko Str., Ivano-Frankivsk, 76018, Ukraine,*
*[2] College of Engineering, Wasit University, Kut, Wasit Governorate, 52001, Wasit, Iraq.*
Authors' e-mails: *ruslan.zapukhlyak@cnu.edu.ua, myroslav.pavlyk@cnu.edu.ua, iryna.svyd@cnu.edu.ua, bohdan.dzundza@cnu.edu.ua, viktor.dovhyi@cnu.edu.ua, vitalii.martyniuk.20@pnu.edu.ua, hdhiyab@uowasit.edu.iq*

https://doi.org/10.23939/acps2025.02.158

*Submitted on 11.09.2025*



***Abstract*: The article discusses modern information security technologies in distributed and asymmetric systems, as well as problems arising from their implementation in the context of growing cyber threats. An analysis of cryptographic methods, authentication systems, access control, and intrusion detection has been provided. Particular attention has been paid to the limitations of existing technologies and promising areas for their improvement, in particular the use of machine learning methods, block chain technologies, and the Zero Trust concept. The importance of adaptive cyber defense models for ensuring the resilience of distributed and cyber-physical systems has been emphasized. A software model of a steganography channel using the El Gamal asymmetric algorithm has been implemented.**

***Index terms*: cybersecurity, distributed systems, information protection, cryptography, zero trust, machine learning.**

## I. INTRODUCTION

Every year, electronic information determines the actions not only of an increasing number of people, but also of an increasing number of man-made technical systems. Violations of the security of electronic information processing and transmission lead to losses, the extent and scale of which are determined by the intended purpose of this information and can be comparable to global tragedies [1].

In today's world of digitalization and increasingly complex information systems, data protection is becoming a particularly pressing issue. Distributed and asymmetric systems, which are widely used in the financial sector, transportation, medicine, and industry, are subject to constant cyber threats. Vulnerabilities in their architecture can lead to leaks of confidential information, financial losses, and the shutdown of critical infrastructure. Therefore, analyzing existing information security technologies and finding ways to improve them is one of the priority tasks of modern cybersecurity [2].

## II. LITERATURE REVIEW AND PROBLEM STATEMENT

The main technologies for protecting information in distributed systems are cryptography, user authentication, access control, and intrusion detection systems (IDS). Cryptographic methods are traditionally used to ensure the confidentiality and integrity of data during its transmission and storage. Among them, symmetric and asymmetric encryption algorithms, hashing, and digital signatures are most commonly used. Symmetric encryption (e.g., AES) is faster but requires reliable key exchange, while asymmetric methods (RSA, ECC) provide a higher level of security but impose significant computational costs. In distributed systems, cryptography allows for secure interaction between nodes, but increases delays and load on the network infrastructure [3].

Authentication methods play a key role in verifying the authenticity of users and devices. Both classic approaches (passwords, PIN codes) and more modern multi-factor models (2FA, biometrics) are used. Despite this, even complex authentication systems remain vulnerable to man-in-the-middle attacks or phishing campaigns that target the human factor. This requires the implementation of additional mechanisms, in particular the continuous monitoring of user behavior characteristics [4].

Access control provides multi-level distribution of rights between users and processes in the system. Classic models (DAC – discretionary access control, MAC – mandatory access control, RBAC – role-based access control) are gradually being supplemented by modern approaches that take into account the context of access, user geolocation, and the time of execution of the action. At the same time, large-scale distributed systems face problems with centralized administration of security policies, which complicates the scalability of such solutions [5].

Intrusion detection systems (IDS) allow you to track abnormal activity on the network and respond to attem-

pted attacks in a timely manner. They are divided into signature-based, which rely on databases of known attack patterns, and behavior-based, which are capable of detecting new threats based on deviations in traffic. Despite this, IDS have limitations in detecting previously unknown attacks (zero-day), which makes the use of machine learning and artificial intelligence methods relevant to improve their effectiveness [6].

## III. SCOPE OF WORK AND OBJECTIVES

Despite advances in cyber security, existing technologies have shortcomings: cryptography causes delays during scaling, authentication is vulnerable to social engineering, and IDS require constant signature updates. Therefore, more adaptive and intelligent protection systems are needed [5–7].

This article uses the materials and results obtained by the authors during the research work "Multifunctional sensor microsystem for non-invasive continuous monitoring and analysis of human biosignals" state registration number 0124U000384 dated 01.01.2024, which is carried out at the Department of Computer Engineering and Electronics, of the Vasyl Stefanyk Carpathian National University in 2024-2026.

## IV. PROMISING DIRECTIONS FOR IMPROVING INFORMATION SECURITY TECHNOLOGIES

A promising direction for improving security in distributed systems is the use of machine learning (ML) to detect anomalies and threats. Unlike traditional signature-based IDS, ML provides adaptability and the ability to recognize new attacks. Clustering and deep learning algorithms analyze user behavior and traffic in real time, and combining them with NLP improves the accuracy of detecting complex attacks [8].

Another approach is to use block chain technologies that ensure decentralized data storage, transparency, and automated access control through smart contracts. Hybrid models combine public and private chains, providing a balance between security and performance. The integration of block chain with ML enhances real-time threat response [9].

Table compares these technologies in terms of their key characteristics, advantages, disadvantages, and effectiveness [9].

**Characteristics of protection methods**

| Criterion | ML | Block chain | Zero Trust |
|---|---|---|---|
| Effectiveness | 90 | 80 | 85 |
| Scalability | 75 | 65 | 80 |
| Complexity | 60 | 70 | 75 |
| Risks | 20 | 30 | 25 |
| Innovation | 95 | 85 | 90 |

Another modern approach is the Zero Trust concept, which rejects automatic trust in any users or devices. Each action undergoes authentication and authorization checks based on behavior and risk. The integration of Zero Trust with ML creates a dynamic, self-learning cybersecurity environment capable of responding quickly to new threats [10].

Based on data obtained from a hypothetical experimental study, four graphs are presented:

1. Graph 1 (Fig.1) shows the comparative effectiveness of technologies according to criteria (Attack Detection, Scalability, Implementation Complexity).

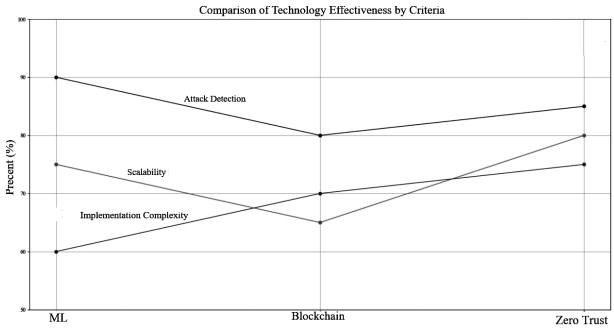


*Fig. 1. Graph comparing the effectiveness of technologies*

Fig. 2 depicts the trade-offs between the benefits and risks of each technology.

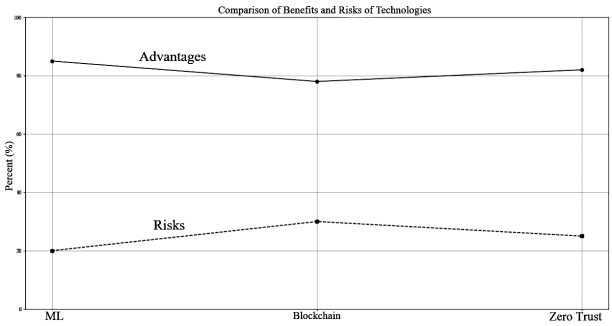


*Fig. 2. Graph of advantages and risks of technologies*

Fig. 3 points to the adaptability of technologies over time and depending on the scale of the system (Small, Medium, Large).

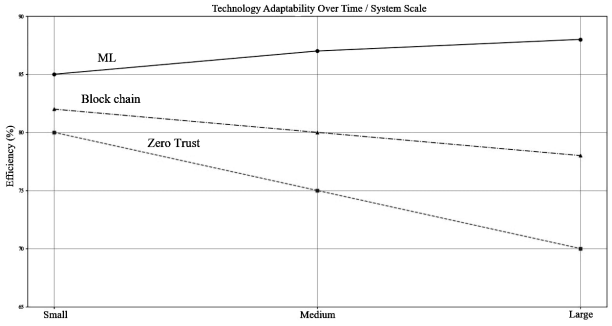


*Fig. 3. Adaptive of technologies over time*

Fig. 4 reveals a radar chart of technology priorities (Efficiency, Scalability, Complexity, Risks, Innovation).

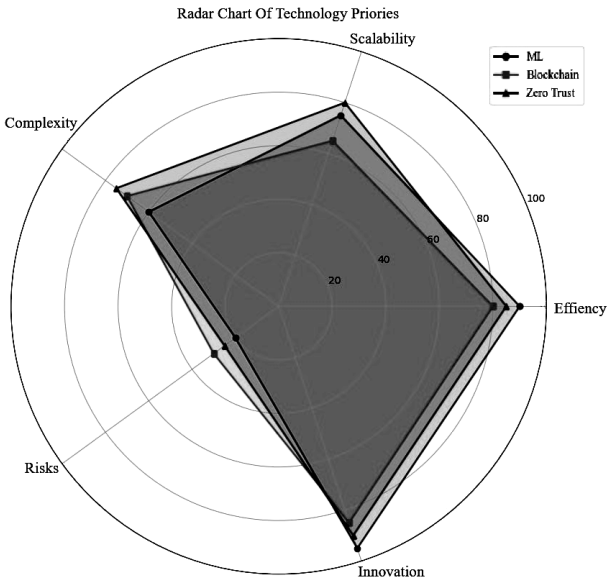


*Fig. 4. Radar chart of technology priorities*

From the Fig1-Fig.4, it is evident that:

- ML-based anomaly detection systems show approximately 87% efficiency due to their adaptability and ability to identify atypical behavioral patterns [10-12].

- Block chain technologies demonstrate about 78% efficiency, providing reliable and transparent data storage along with automated access control.

- Zero Trust integrated with ML achieves around 91% efficiency thanks to continuous monitoring and dynamic adaptation of security policies.

Additionally, the combined use of all three technologies increases the overall protection efficiency to approximately 95%, demonstrating a clear synergistic effect (Fig. 4). The integration of graphical and tabular materials allows the reader not only to visualize the practical significance of these methods but also to assess their strengths and limitations in real-world applications.

Thus, the combination of machine learning methods, block chain technologies, the Zero Trust concept, and asymmetric algorithms forms a multilayered and adaptive cybersecurity system that effectively protects distributed systems from internal and external threats. It enhances the resilience and reliability of cyber-physical and information infrastructures, opening new possibilities for future applications.

The El Gamal scheme [12-14] can be used both for digital signatures and encryption, with its security based on the computational complexity of discrete logarithms in a finite field.

To generate a pair of keys, first select a prime number $p$ and two random numbers $g$ and $x$, both of which must be less than $p$. Then calculate $y = g^x \bmod p$ .

The public key consists of ($y$, $g$, $p$). And $g$ and $p$ being common for a group of users - while the private key is $x$.

To sign a message $M$, a random number $k$, coprime with *(p-1)*, is chosen. Then, $a = g^k \bmod p$ is computed, and using the extended Euclidean algorithm, b is found from the equation: $M = (x^a + k^b) \bmod (p-1)$ .

The signature is the pair ($a$, $b$), and $k$ must remain secret. To verify the signature, it is checked whether $y^a, a^b \bmod p = g^M \bmod p$ holds true.

Each EI Gamal signature or encryption requires a new value $k$, and this value must be chosen randomly. If Eve ever discovers $k$ used by Alice, she will be able to reveal Alice's private key $x$. If Eve ever manages to obtain two messages signed or encrypted with the same $k$, she will be able to reveal $x$, without even knowing the value of $k$.

A modified version of the El Gamal algorithm allows for message encryption. To encrypt a message $M$, a random $k$, coprime with *(p-1)*, is chosen, and the following are computed: $a = g^k \bmod p$ , $b = y^k \bmod p$ .

The pair ($a$, $b$) forms the cipher text, which is twice as long as the plaintext. To decrypt ($a$, $b$), compute $M = b / a^x \bmod p$ .

Since $a^x \equiv g^{kx} \pmod p$ and the following expressions $b / a^x \equiv y^k / g^{kx} \equiv g^{xk} / g^{kx} = M \pmod p$ , the algorithm works correctly.

The security of the El Gamal scheme is based on the difficulty of computing discrete logarithms in a finite field. The public and private keys are functions of two large prime numbers (1024–2048 bits or more). Recovering the plaintext from the cipher text and public key is equivalent to solving the inverse modular exponentiation problem, i.e., finding the discrete logarithm in a finite field.

To ensure the functioning of the steganography channel in digital signatures between two users, each must have a specialized transceiver. The transceiver operates according to the chosen digital signature scheme and steganography communication protocol [14].

The block diagrams of the receiver and transmitter operation are shown in Figures 5 and 6, respectively.

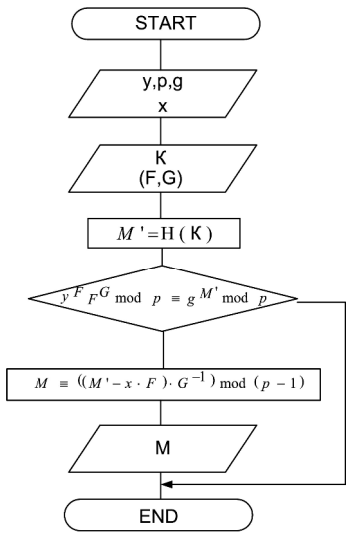


*Fig. 5. Block diagram of the receiver algorithm*

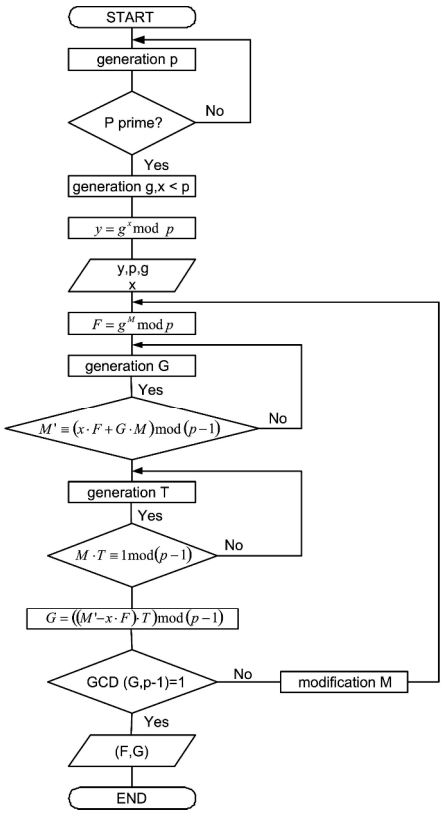


*Fig. 6. Block diagram of the transmitter algorithm*

## V. PRACTICAL SIGNIFICANCE OF THE RESULTS

The proposed improvement approaches can be effectively applied in cyber-physical and distributed systems. In smart cities, they ensure the protection of sensor network data and enable anomaly detection in the operation of devices and users. In transport systems, these technologies provide reliable and transparent communication between vehicles and infrastructure, while the integration of adaptive monitoring allows dynamic adjustment of access policies depending on the risk level.

In the medical field, such approaches ensure the secure collection, transmission, and storage of patients' confidential data. The combined use of machine learning methods, block chain technologies, and the Zero Trust concept enables the creation of a multilayered cybersecurity system that enhances the efficiency, resilience, and reliability of distributed systems and contributes to greater user trust.

## VI. CONCLUSION

Machine learning methods effectively detect anomalies and atypical behavioral patterns in distributed systems, enhancing the adaptability and predictability of cybersecurity. Block chain technologies ensure reliable and transparent data storage, automate access control, and protect against unauthorized modifications. The Zero Trust concept eliminates automatic trust for any user or device, providing continuous monitoring and dynamic adjustment of access policies. Combined application of ML, block chain, and Zero Trust creates a multilayered cybersecurity system that improves the efficiency, resilience, and reliability of distributed and cyber-physical systems.

Integration of these technologies across various sectors from smart cities and transportation to healthcare enhances security, protects confidential data, and increases user trust.

The functioning of a steganography channel in digital signatures between two subscribers based on El Gamal's asymmetric algorithm was implemented.

## VII. CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

## VIII. DECLARATION ON GENERATIVE AI

During the preparation of this work, the author(s) used ChatGPT, Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

## References

[1] Stallings W. (2016) Cryptography and Network Security. *Pearson*, 768.

[2] Bishop M. (2019) Computer Security: *Art and Science. Addison-Wesley*, 1472.

[3] Anderson R. (2020) Security Engineering. *Wiley*, 1232.

[4] Shostack A. (2014) Threat Modeling: Designing for Security. *Wiley*, 624.

[5] Chivukula, R., Lakshmi, T. J., Kandula, L. R. R., & Alla, K. (2021, November). A study of cyber security issues and challenges. In *2021 IEEE Bombay Section Signature Conference (IBSSC)* (pp. 1-5). IEEE. DOI: 10.1109/IBSSC53889.2021.9673270.

[6] Schneier B. (2015) Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York. *Wiley*, 912.

[7] Stallings W. (2017) Network Security Essentials: Applications and Standards. *Pearson*, 640.

[8] Pfleeger C., Pfleeger S. (2016) Security in Computing. Boston. *Pearson*, 880.

[9] Anderson R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems. – 2nd ed. – New York: *Wiley*, 1232.

[10] Viega J., McGraw G. (2019) Building Secure Software: How to Avoid Security Problems the Right Way. Boston. *Addison-Wesley*, 528.

[11] Easttom C. (2018) Computer Security Fundamentals. Boston. *Pearson*, 608.

[12] Ordonez, A. J., Medina R. P., and Gerardo B. D., (2018) Modified El Gamal algorithm for multiple senders and single receiver encryption. *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 201-205. DOI: 10.1109/ISCAIE.2018.8405470.

[13] Yang, S., Liu, C., Wu, H., and Hu, A. (2023). Security Analysis of Enhanced DNA and ElGamal Cryptosystem for Secure Data Storage and Retrieval in Cloud. *13th International Conference on Information Technology in Medicine and Education (ITME)*, Wuyishan, China, 444-446. DOI: 10.1109/ITME60234.2023.00094.

[14] Iavich, M., Gnatyuk, S., Jintcharadze, E., Polishchuk Y., and Odarchenko, R. (2018) Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems. *5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, Kiev, Ukraine, 229-233. DOI: 10.1109/MSNMC.2018.8576289

**Ruslan Zapukhlyak** was born in Ivano-Frankivsk, Ivano-Frankivsk region in 1974. In 1996, he graduated with honours from Vasyl Stefanyk Precarpathian University with a degree in Physics and Mathematics. In 1999, he successfully defended his thesis for the degree of Candidate of Physical and Mathematical Sciences. Since September 2017 - Vice-Rector puter Systems for Scientific and Pedagogical Work at Vasyl Stefanyk Precarpathian National University. Professor in the Department of Computer Engineering and Electronics. He graduated with honors from Vasyl Stefanyk Carpathian National University with a degree in physics and mathematics. His scientific interests are related to the technology of growing and researching the thermoelectric properties of PbTe single crystals and films and alloys based on them, creating electronic and information technology devices based on them, high-level programming languages, technologies and means of information protection.

**Myroslav Pavlyuk** was born in the village of Starunya, Bohorodchany District, Ivano-Frankivsk Region in 1954. From 1976 to 1981, he studied at the Physics and Mathematics Department of Vasyl Stefanyk Ivano-Frankivsk State Pedagogical Institute, majoring in physics and mathematics. In 1994, he defended his thesis, an Associated Professor in the Department of Computer Engineering and Electronics Vasyl Stefanyk Carpathian National University.
Scientific interests relate to cultivation technology and research into the thermoelectric properties of single crystals, electronics, computer logic, Internet of Things systems, and information security.

**Iryna Svyd** is a candidate of technical sciences, associate professor, professor of the Department of Computer Engineering and Electronics of the Vasyl Stefanyk Carpathian National University. In 2000, she graduated with honors from Kharkiv State Technical University of Radio Electronics with a degree in multi-channel telecommunications and received a specialist's degree. In 2012, she defended her candidate's thesis in the specialty 05.12.17 "Radio Engineering and Television Systems". In 2014 at Kharkiv National University of Radio Electronics, she received the academic title of associate professor of the Department of Communication Networks. The scope of her scientific interests includes: development of methods for increasing the noise immunity of radar systems; wireless communication; mobile communication systems; design of devices based on microcontrollers and programmable logic integrated circuits; Internet of Things devices; modeling of digital signals.

**Bohdan Dzundza** was born in Bodnariv village, Kalush district, Ivano-Frankivsk region in 1982. 2004 – 2007 postgraduate studies at Vasyl Stefanyk Precarpathian National University, specialty Solid State Chemistry. In 2008, he successfully defended his thesis and received a PhD. In 2024, he successfully defended his doctoral thesis and received a Doctor of Technical Sciences degree. He is co-author of ten textbooks, two monographs, more than 130 publications in professional scientific journals. Research interests: studying the physical properties of semiconductor thin films and nanostructures (pure and doped materials, solid solutions, and multicomponent semiconductor compounds), thermoelectric and photovoltaic semiconductor materials development of automated laboratory research systems, microcontroller systems and the Internet of Things.

**Victor Dovgyi** was born in Ivano-Frankivsk, Ivano-Frankivsk region in 1986. In 2008, he graduated from Vasyl Stefanyk Precarpathian National University with a degree in Radiophysics. In 2016 successfully defended his thesis and received a PhD. Research interests: sensor electronics, microsystems-on-a-chip based on advanced microelectronic technologies of large integrated circuits, implementation of DevOps principles in various software projects.

**Vitalii Martyniuk**, senior laboratory assistant. In 2020, he graduated from the Babchensky Educational Complex of I-III degrees. In 2020, he enrolled at Vasyl Stefanyk Precarpathian National University, majoring in Computer Engineering (123), completed his bachelor's degree in 2024, and received a bachelor's degree in Computer Engineering. In 2024, he enrolled in a master's degree program in Computer Engineering, where he is currently studying. Since October 2024, he has been working as a senior laboratory assistant.

**Haider Th. Salim ALRikabi** is a Full Professor of Electrical Engineering and a faculty member in the College of Engineering, Department of Electrical Engineering, Wasit University, Al-Kut, Wasit, Iraq. He received his B.Sc. in Electrical Engineering from Mustansiriyah University, Baghdad, Iraq, in 2006, and his M.Sc. in Electrical Engineering with a specialization in Communication Systems from California State University, Fullerton, USA, in 2014. He obtained his Ph.D. in Electrical Engineering from Mustansiriyah University in 2025. His current research interests include wireless communication, mobile communication systems, control systems, intelligent technologies, smart cities, Internet of Things (IoT), and Reconfigurable Intelligent Surfaces (RIS).