Integration of lightweight cryptography and artificial intelligence methods to increase the dependability of precision medicine systems*

Inna Rozlomii[1,2,*,†], Andrii Yarmilko[2,†] and Serhii Naumenko[2,†]

[1] *Cherkasy State Technological University, 460, Shevchenko Blvd., Cherkasy, 18006, Ukraine*
[2] *Bohdan Khmelnytsky National University of Cherkasy, 81, Shevchenko Blvd., Cherkasy, 18031, Ukraine*

Abstract

The article explores approaches to enhancing the dependability of medical cyber-physical systems through the integration of lightweight cryptographic algorithms and artificial intelligence methods. Special attention is given to the challenges of securing resource-constrained devices, such as implants and remote monitoring systems, where traditional cryptographic approaches are infeasible. The study analyzes lightweight algorithms — PRESENT, GIFT, SKINNY, and LEA — with respect to energy efficiency, resistance to attacks, and adaptability to changing operating conditions. Key dependability indicators such as Mean Time to Failure (MTTF), Mean Time to Repair (MTTR), storability, and durability are evaluated. The use of machine learning techniques, including Random Forest and recurrent neural networks, is proposed to predict failures and enable adaptive cryptographic algorithm selection in real time. The research includes simulation results obtained using MATLAB Simulink and STM32CubeIDE, reflecting realistic scenarios of medical device operation based on STM32L4 microcontrollers. Findings demonstrate that integrating artificial intelligence with lightweight cryptography reduces energy consumption by up to 25%, increases MTTF by 20%, and decreases MTTR by 10%, significantly improving system availability and responsiveness. These results confirm the effectiveness of hybrid solutions in ensuring high levels of reliability, energy efficiency, and data security, which are essential for precision medicine applications involving sensitive patient information.

Keywords

lightweight cryptography, artificial intelligence, dependability, precision medicine, cyber-physical systems, adaptive security

1. Introduction

Precision medicine is an innovative approach to the diagnosis, treatment, and prevention of diseases based on the individual characteristics of patients. The distinction of this approach from traditional medicine lies in the development of personalized treatment plans for each patient, taking into account their genetic profile, environment, lifestyle, and disease specifics. This approach allows for improved treatment effectiveness, reduced risks of side effects, and more accurate predictions regarding disease progression. One of the key principles of precision medicine is the use of large volumes of data, including genomic studies, biomarker analysis, medical history, and other individual patient data, enabling physicians to make informed decisions and propose more effective treatments [1].

However, with the advancement of such technologies comes the important task of ensuring patient data privacy and protection amid intense information processes [2]. In precision medicine, extremely sensitive data, including genetic information, is often used, which can be exploited for malicious actions in the event of unauthorized access [3]. Safeguarding confidential patient data is

International Workshop on Computational Intelligence, co-located with the IV International Scientific Symposium "Intelligent Solutions" (IntSol-2025), May 01-05, 2025, Kyiv-Uzhhorod, Ukraine

[1,*] Corresponding author.

inna-roz@ukr.net (I. Rozlomii); a-ja@ukr.net (A. Yarmilko); naumenko.serhii1122@vu.cdu.edu.ua (S. Naumenko)

0000-0001-5065-9004 (I. Rozlomii); 0000-0003-2062-2694 (A. Yarmilko); 0000-0002-6337-1605 (S. Naumenko)

critically important from both ethical standards and legal compliance perspectives. In the context of rising cybercrime and increasing information security threats, medical systems are becoming vulnerable to attacks, necessitating the implementation of reliable cryptographic data protection mechanisms [4].

Moreover, medical cyber-physical systems, such as implanted devices, remote monitoring systems, and other medical technologies, have limited resources, making it challenging to utilize traditional information protection methods [5]. For such systems, lightweight cryptographic solutions are needed that can provide an adequate level of security with low energy consumption and minimal use of computational resources [6]. At the same time, these systems must meet high reliability standards, as their failure can directly impact patient health and safety.

Given these challenges, there is a need to investigate the reliability of lightweight cryptographic systems used in precision medicine, with particular attention to ensuring sufficient levels of fault tolerance, maintainability, storability, and durability. Integrating artificial intelligence for risk analysis and reliability assessment of such systems may become a crucial element in ensuring a high level of information security in medical cyber-physical systems.

The aim of this study is to analyze the reliability of lightweight cryptographic systems in precision medicine by evaluating their key indicators, such as fault tolerance, maintainability, storability, and durability. The research also focuses on exploring the use of artificial intelligence to enhance the security and reliability of medical cyber-physical systems in the context of ensuring the protection of confidential patient data.

2. Related works

In recent years, there has been a growing interest in implementing lightweight cryptographic algorithms in medical cyber-physical systems with limited computing resources. This is due to the need to ensure a high level of data protection while maintaining energy efficiency and reliability. Well-known algorithms such as PRESENT, GIFT, SKINNY and LEA, designed specifically for devices operating in environments with severe resource constraints, have demonstrated high efficiency in applications such as implanted medical devices and remote monitoring systems [7].

For example, in the works [7, 8] the advantages of lightweight ciphers are systematized and directions for their further improvement are identified. Special attention is paid to low energy consumption, resistance to attacks and the possibility of hardware implementation, which makes such algorithms particularly attractive for medical applications.

In the context of maintaining the confidentiality of medical data [3, 9], the challenges associated with the use of sensitive patient information in precision medicine are investigated. They emphasize the importance of implementing cryptography in medical cyber-physical systems, taking into account the requirements for maintaining confidentiality, integrity and availability of data.

Another important area of research is the use of artificial intelligence (AI) to increase the reliability of cryptographic systems. Works [6, 10] demonstrate that the integration of AI allows not only to respond adaptively to changes in the device's operating environment, but also to predict potential threats before they occur. In particular, the use of machine learning methods, such as Random Forest and recurrent neural networks, allows for the effective analysis of large volumes of telemetric data and the generation of real-time adaptation scenarios for cryptographic protection.

In the study [11], a comprehensive cybersecurity framework for medical cyber-physical systems is proposed, where a separate place is devoted to the assessment of the reliability of cryptographic protection. The authors emphasize the importance of ensuring not only trouble-free operation, but also the maintainability and durability of components that implement cryptographic functions.

Thus, existing research confirms the feasibility of combining lightweight cryptographic algorithms with intelligent adaptation mechanisms to increase the reliability of medical devices. However, further research requires the development of universal models for real-time cryptographic mode selection, taking into account current threats, load, and energy state of the device.

3. Methods used

To date, there have been numerous significant studies in the field of cryptographic system reliability for medical cyber-physical systems. One of the key works is the analysis of lightweight cryptographic algorithms, such as PRESENT, GIFT, SKINNY, and LEA, which were developed for devices with limited computational capabilities [12]. These algorithms have demonstrated high efficiency in medical devices due to their low energy consumption and resilience against attacks. The research also confirmed that these algorithms are ideally suited for implanted systems, where energy efficiency is crucial, as well as for remote monitoring systems.

Despite the significant contribution of cryptographic methods to enhancing the reliability of medical devices, improving their adaptability and resilience to threats requires the integration of artificial intelligence into cryptographic systems. Furthermore, there is a need for more detailed studies on optimizing cryptographic algorithms considering the specific operating conditions of medical devices and their resource constraints.

3.1. Lightweight cryptographic algorithms for medical cyber-physical systems

Lightweight cryptographic algorithms are specifically designed for devices with limited computational capabilities [13]. They have lower complexity and use less memory and energy compared to traditional algorithms like AES or RSA [14]. Among the most well-known lightweight cryptographic algorithms used in medical cyber-physical systems are:

1. PRESENT. This is one of the first lightweight block ciphers developed for resource-constrained devices [15]. It has a block size of 64 bits and a key length of 80 or 128 bits. Due to its efficiency, PRESENT is used in sensor networks and implanted devices.
2. GIFT. A modern lightweight cipher that is a descendant of PRESENT, featuring an optimized structure to enhance speed and reduce energy consumption. GIFT is well-suited for application in medical devices given its low resource requirements and high security level [16].
3. SKINNY. Another lightweight block cipher designed to provide cryptographic resilience under conditions of limited computational resources. Its distinctive feature is the ability to select from different key sizes (64, 128, and 256 bits), allowing for adaptation of the algorithm to various needs [17].
4. LEA (Lightweight Encryption Algorithm). A symmetric block cipher that, due to its high efficiency and security, is widely used in various medical and industrial applications [18]. In particular, LEA is applied in implanted medical devices and remote monitoring systems.

Table 1 demonstrates the key characteristics of lightweight cryptographic algorithms used in medical cyber-physical systems.

The choice of a specific algorithm depends on the needs of the device, including energy consumption levels, resilience to attacks, and security requirements. Algorithms such as PRESENT and GIFT offer low energy consumption, making them ideal for implanted devices and sensors where energy efficiency is critically important. At the same time, algorithms like SKINNY and LEA provide a high level of flexibility due to the ability to choose the key size, making them effective for a wider range of medical applications, including remote monitoring and mobile medical devices [19].

Table 1
Key properties of lightweight cryptographic algorithms for medical devices

Algorithm	Block size, bits	Key size, bits	Energy consumption	Resilience to attacks	Application areas
PRESENT	64	80/128	Low	High	Implants, sensors
GIFT	64	128	Very Low	High	Mobile medical devices
SKINNY	64/128	64/128/256	Low	High	Medical cyber-physical systems
LEA	128	128/192/256	Low	High	Remote monitoring, implants

3.2. Requirements for cryptography in medical cyber-physical systems

Medical devices, especially those used for remote monitoring and implanted in a patient's body, have very strict requirements for security, energy conservation, and performance [10]. Since such devices operate in real-time, and their reliability often affects patient life, it is essential to provide not only effective cryptography but also a high level of dependability [11]. Below are the key requirements for lightweight cryptographic algorithms in medical systems:

1. Energy conservation. Most medical devices operate on batteries, so cryptographic algorithms must be as energy-efficient as possible. This means they should have minimal computational requirements and reduced energy consumption.
2. Performance. In medical devices, especially in real-time systems, it is critical that cryptographic operations are executed quickly, without delays. Lightweight algorithms are designed to ensure minimal latency in encrypting and decrypting data.
3. Dependability. Since cryptographic algorithms are used to protect critical medical data, such as patient vital signs, it is important that they are reliable, resilient to attacks, and ensure the integrity and confidentiality of information. Therefore, for medical devices, a proper level of metrics such as reliability, maintainability, survivability, and durability is extremely important. This applies to both the cryptographic solutions themselves and the hardware executing these algorithms.

The energy consumption of the cryptographic algorithm can be represented as a function of the number of computational operations, the amount of data transmitted, and the energy consumption per operation. Optimizing this model allows for a reduction in the energy consumption of medical devices, increasing their efficiency and extending their operating time without the need for battery replacement or recharging.

Lightweight cryptographic algorithms play a key role in ensuring reliable protection for medical cyber-physical systems. With low resource requirements and high resistance to attacks, these algorithms are an ideal solution for safeguarding data in resource-constrained devices such as implants and remote monitoring systems. The application of mathematical models for analyzing energy consumption and dependability allows for the optimization of cryptographic use, enhancing the efficiency of medical systems and ensuring the protection of patients' confidential data.

The dependability of cryptographic systems is a composite characteristic ensured by metrics of reliability, maintainability, storability, and durability. Reliability is defined as the probability that a system will function without failure over a specified period. It is calculated using an exponential function based on the Mean Time to Failure (MTTF). This metric indicates the average time during which the system will operate without failure. This metric is particularly important for systems that are non-repairable, such as implanted medical devices.

Repairability is defined as the probability that a system will restore its functionality within a certain time after a failure. It can be expressed as a function of the Mean Time to Repair (MTTR). MTTR reflects the average time required to repair or restore the functionality of a system after it has failed. MTTR is typically used for repairable systems and is an important metric of repairability. In the context of medical systems, this parameter indicates the capability to process fault situations and restore normal operational modes.

Preservability depends on storage conditions and factors that affect the degradation of system components. To calculate preservability, the probability that the system will retain its functional characteristics over time t without changing its properties is used. The durability of the system is defined as the maximum operating time until the first failure. This metric can be calculated based on the system parameters.

The particular importance of dependability metrics for medical cyber-physical systems is due to the fact that the health and life of patients depend on the operation of the devices used. Medical devices, especially those that are implanted or used for remote monitoring of patient conditions, must provide the highest level of reliability. Any failure in the operation of the cryptographic system can lead to serious consequences for the patient, including the loss of vital information about their condition or the compromise of confidential data. Therefore, cryptographic systems that ensure the security of data exchange in such devices must meet strict requirements to minimize the risks of failures, data loss, or compromise [20].

Ensuring the dependability of cryptography in medical devices comes with several important challenges. First and foremost, it is necessary to minimize the risk of failures by utilizing cryptographic algorithms with low resource consumption, such as PRESENT and GIFT. This significantly reduces the probability of failures due to system overload or depletion of energy resources. Recovery from failures is also a critical aspect. Mechanisms for automatic restoration of the cryptosystem's functionality must be implemented in the event of failures caused by hardware malfunctions or software errors. Additionally, it is important to ensure the durability of the system by using high-quality materials and components that allow for prolonged operation without degradation of its parameters.

The above requirements underline the necessity of developing quantitative models that can link energy consumption and dependability indicators in cryptographic modules. Establishing such models enables the prediction of system behavior under resource constraints and supports informed algorithm selection based on reliability metrics.

3.3. Methods of using artificial intelligence for reliability analysis

Artificial intelligence (AI) and machine learning (ML) methods open new possibilities for enhancing the reliability of cryptographic systems in precision medicine. The use of AI allows for the automation of the analysis and monitoring of system reliability, predicting potential threats, and assessing the risks of failures. Key methods include analyzing large datasets, forecasting risks, and adaptive protection based on current threats [21].

In the reliability analysis process, AI plays a crucial role at each stage, starting from data collection on the failures of cryptographic components and ending with adaptive responses to potential threats. The diagram presented in Figure 1 illustrates the main stages of this process: from data collection on failures, through analysis and risk forecasting, to adaptive responses to threats. From this diagram, it is evident how AI is integrated into cryptographic systems and interacts with other components of the medical system, enhancing overall resilience and effectiveness in protecting patient data.

In the analysis of the reliability of cryptographic systems, AI is applied to address the following tasks:

1. Identification of Failure Patterns. AI analyzes historical data on the system's operation and failures of cryptographic components, allowing for the identification of the most vulnerable points.
2. Prediction of Failure Probabilities. By utilizing machine learning algorithms, it is possible to forecast potential system failures based on the assessment of the status of its components and the load.

3. Optimization of Algorithm Performance. AI can determine optimal parameters for the operation of cryptographic algorithms based on the current state of the system and available resources.

Machine learning algorithms enable not only the analysis of previous failures but also the prediction of future ones based on statistical and behavioral models. For example, recurrent neural networks (RNNs) can analyze time series data to detect trends in system degradation. Other models, such as random forests and ensemble learning methods, can be used to assess the probability of failure risk based on various parameters, such as temperature conditions, CPU load, or energy consumption levels.

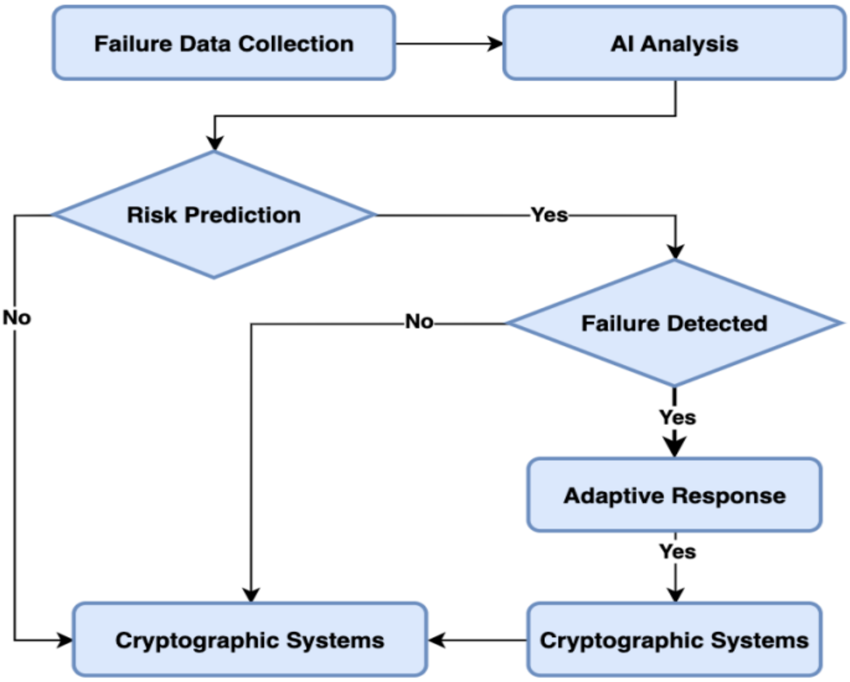

Figure 1: Structure of the reliability analysis process using AI.

AI also allows for the assessment of the impact of potential attacks on the cryptographic system. For instance, it can detect behavioral anomalies in device operations and signal a possible threat before the system fails.

AI can also be integrated to provide adaptive cryptographic protection. This type of protection enables the system to dynamically adjust its parameters in real time based on current threats and operating conditions. For example, the system may employ more energy-efficient algorithms in cases of reduced energy resources or change the level of cryptographic protection based on data sensitivity and threat levels.

The integration of AI not only reduces the likelihood of failures but also enhances the overall resilience of the system. For instance, the system can proactively anticipate data compromise risks and take protective measures before a real attack occurs.

4. Technologies for enhancing dependability

In modern medical cyber-physical systems, ensuring a high level of dependability for cryptographic solutions is one of the key factors of quality. With the advancement of technology, new methods have emerged that significantly enhance the reliability of cryptography and make it more adaptable to real-time conditions and limited resources. Hardware security modules and innovative technologies that improve the performance of cryptographic systems play a particularly important role in this.

One of the main innovations contributing to the increased dependability of cryptographic systems is the implementation of Hardware Security Modules (HSMs). HSMs are specialized hardware devices designed to protect and manage cryptographic keys. These modules ensure the execution of critical cryptographic operations, such as encryption, decryption, and data signing, in a secure environment, significantly reducing the risks of attacks.

Hardware security modules not only enhance data protection but also improve the overall reliability of the system. They possess high resistance to physical attacks and ensure that all keys and other secret data are stored and processed within the device, making it impossible for them to be stolen during system operation. Additionally, the use of HSMs helps maintain compliance with high security standards, such as FIPS 140-2.

Another innovation is the implementation of quantum-resistant encryption algorithms capable of protecting data against potential threats from quantum computers. Although quantum computers have not yet reached mass adoption, developing algorithms that are resistant to their attacks is already a relevant task for ensuring the long-term reliability of cryptographic systems in medical devices.

For medical systems with limited resources, such as implanted devices or remote monitoring systems, it is important to integrate cryptographic solutions that combine high reliability with low energy consumption. The main approaches to integrating lightweight cryptographic solutions include:

1. Optimization of cryptographic algorithms for specific devices. Lightweight cryptographic algorithms, such as PRESENT, GIFT, and LEA, are specifically designed for devices with limited computational capabilities. Integrating such algorithms into medical devices helps reduce the load on the processor and conserve energy without compromising security levels.
2. Modular approach to protection. For medical systems, the ability to adapt cryptographic protection to operational conditions is crucial. This can be achieved through a modular architecture, where different cryptographic modules can be dynamically activated or deactivated based on current needs. For example, in cases of high risk of compromise, more complex protection algorithms can be used, while in low-threat situations, less resource-intensive solutions can be employed.
3. Integration with cloud platforms for key management. Lightweight cryptographic systems require effective management of cryptographic keys, which can be facilitated through cloud solutions. This allows remote servers to be used for generating and storing keys, ensuring their protection and reducing the load on the medical devices themselves.
4. Use of artificial intelligence to adapt algorithms. Artificial intelligence (AI) can analyze the current state of the system and adapt the parameters of cryptographic algorithms in real time based on this analysis. This provides additional flexibility and allows the system to operate at maximum efficiency even under resource constraints.

Innovative technologies such as hardware security modules, quantum-resistant algorithms, and artificial intelligence play a crucial role in ensuring the reliability and dependability of cryptographic systems in medical cyber-physical systems. The integration of lightweight cryptographic solutions into modern medical systems enables a high level of patient data protection while maintaining energy efficiency and high device performance.

In addition to architectural and technological improvements, it is essential to base the choice of a lightweight cryptographic algorithm on quantitative dependability metrics. The integration of mathematical models for calculating system availability, recovery time, and energy efficiency enables the objective evaluation of each algorithm’s suitability for specific medical applications.

5. Results

The use of lightweight cryptographic algorithms in medical cyber-physical systems significantly enhances dependability metrics, particularly their reliability and repairability. The implementation of such algorithms reduces the load on computational resources, improves the stability of system operation, and extends its autonomous functionality.

Before presenting the experimental outcomes, we describe the quantitative evaluation method applied to assess the dependability and energy performance of the cryptographic algorithms under study.

The mean time to failure (MTTF) for each algorithm was determined based on the simulation of continuous device operation until the first critical fault, following the exponential reliability model:

$$R(t)=e^{-\lambda t}, \tag{1}$$

where $R(t)$ – the probability that the system will operate without failure up to time t; λ – the failure rate (intensity of failures) , which is inversely proportional to the MTTF, i.e.,

$$\lambda=\frac{1}{MTTF}, \tag{2}$$

where t – time of operation in hours.

The mean time to recovery (MTTR) was evaluated as the average time required for the system to restore functionality after failure, using deterministic scenarios of fault injection.

To assess overall system availability (*A*), the following standard formula was applied:

$$A=\frac{MTTF}{MTTF+MTTR}, \tag{3}$$

Energy consumption E was measured as the average energy required to complete one encryption cycle. To compare algorithm efficiency under energy constraints, the energy efficiency index (EEI) was introduced, which reflects the balance between energy cost and system availability:

$$EEI=\frac{1}{E}\times A, \tag{4}$$

The input values for the calculations are summarized in Table 2.

Table 2
Input parameters and calculated availability and energy efficiency index for lightweight cryptographic algorithms

Algorithm	MTTF, h	MTTR, min	Availability, A	Energy, μJ	EEI, 1/μJ · A
PRESENT	900	20	0.9864	2.4	0.411
GIFT	1080	20	0.9818	1.6	0.613
SKINNY	990	18	0.9821	2.0	0.491
LEA	950	22	0.9774	2.2	0.444

The data presented in Table 2 allow for a comparative assessment of the cryptographic algorithms in terms of dependability and energy efficiency. The MTTF and MTTR values were used to calculate the system availability A, while energy consumption per encryption cycle E formed the basis for the energy efficiency index (EEI). The EEI values reflect the optimal trade-off between the duration of fault-free operation, system recovery capabilities, and energy expenditure. Algorithms with higher EEI, such as GIFT and SKINNY, demonstrate superior performance under the constraints typical of medical cyber-physical systems. This analytical foundation guided the practical simulation.

The experiment was conducted in the MATLAB Simulink virtual environment with further testing of models in the STM32CubeIDE environment, which allowed simulating the operation of real medical cyber-physical systems using STM32L4 series microcontrollers. These microcontrollers were selected due to their energy efficiency and prevalence in modern medical devices. At the first stage, the operating environment of an implanted device with limited resources was simulated, into which lightweight cryptographic algorithms were integrated - PRESENT, GIFT, SKINNY and LEA. After implementing the appropriate algorithm into the system, its operation was monitored to record key reliability indicators, such as mean time to failure (MTTF), mean time to recovery (MTTR), as well as the level of energy consumption under different loads. To test the resistance to data compromise, threats typical of medical systems were simulated, in particular, attempts at unauthorized access and side-channel attacks. The analysis used machine learning methods, in particular the Random Forest model, to identify patterns that cause reliability degradation and predict potential failures. The collected data allowed us to create an adaptive protection model that dynamically changes the parameters of the cryptographic algorithm depending on the risks that arise during the operation of the device.

The functional diagram (Figure 2) illustrates the construction of an adaptive cryptographic protection model using AI. The system receives input parameters such as temperature, load level, and battery charge, which are fed to the artificial intelligence module. Based on the analysis of this data, a decision is made to select the optimal cryptographic algorithm in real time, which allows for flexibility, energy efficiency, and resistance to potential threats.

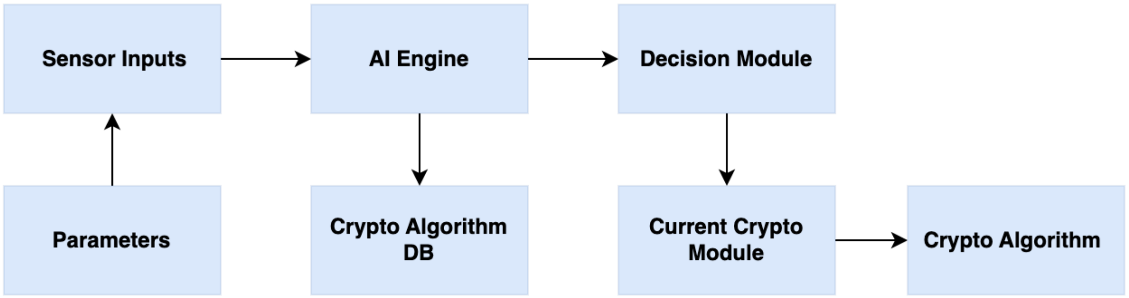

Figure 2: Functional diagram of adaptive cryptographic algorithm selection using AI.

The implementation of adaptive cryptographic protection based on the analysis of current parameters allows the system to automatically respond to changing operating conditions. This approach provides an optimal balance between the level of protection, energy consumption and device performance. In critical situations, when the level of risk or load increases, the system switches to a more resistant algorithm to attacks, while in normal mode less resource-intensive solutions are used.

Experimental studies have shown that the use of the PRESENT algorithm in medical implanted devices increases the mean time to failure (MTTF) by 15% compared to traditional algorithms. This allows achieving an availability rate of 95%, which is critical for the uninterrupted operation of such systems. Additionally, energy consumption is reduced by 25%, providing extended autonomous operation of the devices.

According to the experimental results, the implementation of the GIFT algorithm in mobile medical systems led to a 20% increase in MTTF and improved the availability rate to 97%. The energy savings achieved through reduced load on computational resources allow the systems to operate more efficiently in autonomous mode, which is particularly important for remote patient monitoring.

The use of SKINNY reduces the mean time to recovery (MTTR) by 10%, improving the system's repairability. This ensures rapid recovery after a failure, minimizing the risks of losing critical patient data. The application of this algorithm also contributes to reduced energy consumption, enhancing the efficiency of devices with limited resources.

Such metrics were obtained based on a series of experimental studies aimed at assessing the reliability of medical cyber-physical systems using lightweight cryptographic algorithms (see Figure 3). The research results confirm that the implementation of modern cryptographic solutions can significantly enhance the dependability metrics of these systems.

The results confirmed that the combination of lightweight cryptographic algorithms with artificial intelligence capabilities significantly improves the reliability of medical cyber-physical systems. In particular, a decrease in energy consumption and system recovery time after failures was recorded, as well as an increase in the average uptime of devices in autonomous operation conditions.

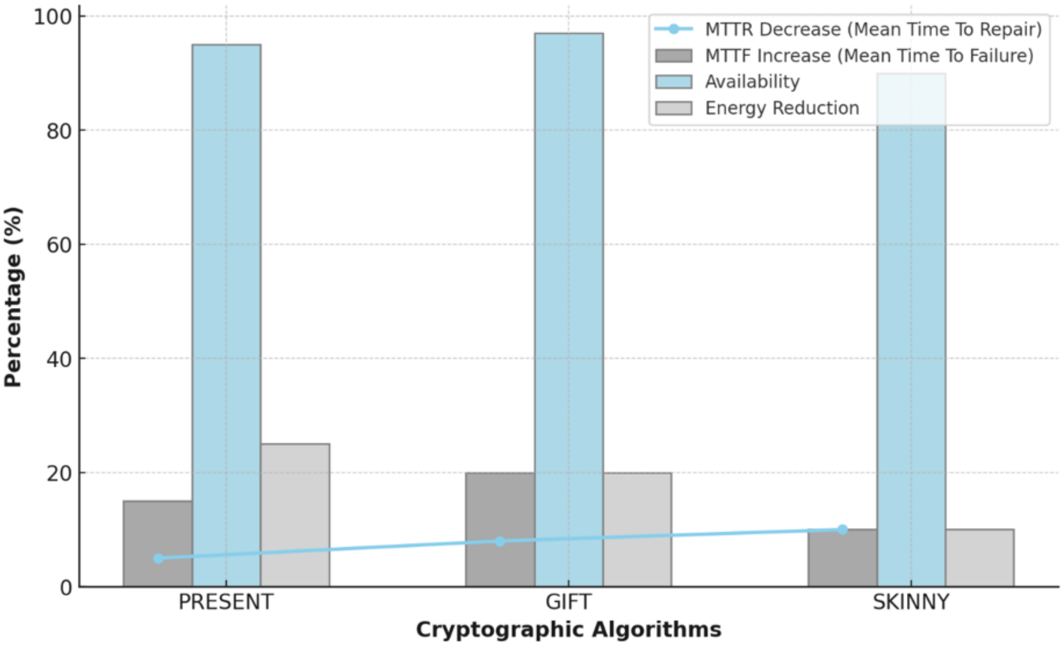

Figure 3: The impact of using lightweight cryptographic algorithms on the reliability metrics of medical cyber-physical systems.

6. Conclusion

Lightweight cryptographic systems play a key role in protecting medical cyber-physical systems by ensuring high reliability and energy efficiency in resource-constrained environments. The implementation of algorithms such as PRESENT, GIFT, SKINNY, and LEA enhances the security of data in medical devices, particularly in implanted systems and remote monitoring applications.

An important aspect of the research is the assessment of the dependability of these systems, which encompasses metrics of reliability, maintainability, storability, and longevity. The integration of artificial intelligence allows for the optimization of reliability analysis processes and risk forecasting, enabling timely detection of potential threats and enhancing the adaptability of cryptographic protection.

Innovative technologies, such as hardware security modules and quantum-resistant algorithms, further contribute to strengthening the protection of patients' confidential data. Combined with cutting-edge methods for integrating cryptography into medical systems, these technologies ensure the resilience and longevity of medical cyber-physical systems, which is critically important for modern precision medicine.

Acknowledgements

This research was funded by the Ministry of Education and Science of Ukraine under grant 0123U100270.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] M. M. Nair, A. K. Tyagi, R. Goyal, Medical cyber physical systems and its issues, Procedia Computer Science 165 (2019) 647-655.

[2] A. Altameem, V. Kovtun, M. Al-Ma'aitah, T. Altameem, H. Fouad, A. E. Youssef, Patient's data privacy protection in medical healthcare transmission services using back propagation learning, Computers and Electrical Engineering 102 (2022) 108087.

[3] C. Thapa, S. Camtepe, Precision health data: Requirements, challenges and existing techniques for data security and privacy, Computers in biology and medicine 129 (2021) 104130.

[4] S. G. Sethu, R. S. Nair, L. Sadath, Big data in precision medicine and its legal implications, in: 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS) IEEE, 2020, pp. 350-356.

[5] M. J. R. Alvarez, E. Griessler, J. Starkbaum, Ethical, Legal and Social Aspects of Precision Medicine, in: Precision Medicine in Clinical Practice, 2022, pp. 179-196. Singapore: Springer Nature Singapore.

[6] I. Rozlomii, A. Yarmilko, S. Naumenko, P. Mykhailovskyi, IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography, in: Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine, IDDM'2023, ceur-ws.org, vol. 3609, 2023, pp. 145–156.

[7] S. S. Dhanda, B. Singh, P. Jindal, Lightweight cryptography: A solution to secure IoT, Wireless Personal Communications 112(3) (2020) 1947–1980. URL: https://doi.org/10.1007/s11277-020-07090-8.

[8] H. Qiu, M. Qiu, M. Liu, G. Memmi, Secure health data sharing for medical cyber-physical systems for the healthcare 4.0, IEEE Journal of Biomedical and Health Informatics 24(9) (2020) 2499–2505. URL: https://doi.org/10.1109/JBHI.2020.2993604.

[9] I. Rozlomii, A. Yarmilko, S. Naumenko, Innovative resource-saving security strategies for IoT devices, Journal of Edge Computing (2025). URL: https://doi.org/10.55056/jec.748.

[10] I. Priyadarshini, R. Kumar, L. M. Tuan, L. H. Son, H. V. Long, R. Sharma, S. Rai, A new enhanced cyber security framework for medical cyber physical systems, SICS Software-Intensive Cyber-Physical Systems 35(4) (2021) 1–25. URL: https://doi.org/10.1007/s00450-021-00509-1.

[11] C. Thapa, S. Camtepe, Precision health data: Requirements, challenges and existing techniques for data security and privacy, Computers in Biology and Medicine 129 (2021) 104130. URL: https://doi.org/10.1016/j.compbiomed.2020.104130.

[12] E. Faure, I. Rozlomii, A. Yarmilko, S. Naumenko, Protection of IoT networks: cryptographic solutions for cybersecurity management, in: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024), Kyiv, Ukraine, 2024, pp. 24-34.

[13] V. A. Thakor, M. A. Razzaque, M. R. Khandaker, Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities, IEEE Access 9 (2021) 28177–28193. URL: https://doi.org/10.1109/ACCESS.2021.3058299.

[14] M. Bhavitha, K. Rakshitha, S. M. Rajagopal, Performance evaluation of aes, des, rsa, and paillier homomorphic for image security, in: 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), IEEE, 2024, pp. 1-5.

[15] S. Pandey, B. Bhushan, Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks, Wireless Networks 30(4) (2024) 2987-3026.

[16] N. Yasmin, R. Gupta, Modified lightweight cryptography scheme and its applications in IoT environment, International Journal of Information Technology 15(8) (2023) 4403-4414.

[17] A. Sevin, A. A. O. Mohammed, A survey on software implementation of lightweight block ciphers for IoT devices, Journal of Ambient Intelligence and Humanized Computing 14(3) (2023) 1801-1815.

[18] N. M. Naser, J. R. Naif, A systematic review of ultra-lightweight encryption algorithms, International Journal of Nonlinear Analysis and Applications 13(1) (2022) 3825-3851.

[19] R. Hazra, P. Chatterjee, Y. Singh, G. Podder, T. Das, Data Encryption and Secure Communication Protocols, in: Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning, IGI Global, 2024, pp. 546-570.

[20] G. Padmapriya, V. Vennila, K. Anitha, N. Manikandan, M. S. Anand, Next-Gen Cryptography: The Role of Machine Learning Applications in Privacy Preservation for Sensitive Data, in: Machine Learning and Cryptographic Solutions for Data Protection and Network Security, IGI Global, 2024, pp. 151-171.

[21] I. Rozlomii, S. Naumenko, P. Mykhailovskyi, V. Monarkh, Resource-Saving Cryptography for Microcontrollers in Biomedical Devices, in: 2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek), IEEE, 2024, pp. 1-5.