Resource-efficient solutions for data security at the network level of the Medical Internet of Things*

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 focuses on resource-efficient solutions for ensuring data security at the network level of Medical Internet of Things (MIoT) systems. Modern systems of this type use a vast number of medical devices with limited computational resources and power capacity. To address the challenges of ensuring the confidentiality, integrity, and availability of medical data in such systems, implementing efficient cryptographic solutions is a necessary step. The article substantiates the importance of using lightweight cryptographic algorithms, such as LEA, which demonstrate high performance and minimal energy consumption—critical for the autonomous operation of medical devices. Specifically, a comparative analysis of lightweight cryptographic algorithms and traditional methods showed that LEA encrypts three times faster while consuming significantly less energy compared to AES-128, confirming its suitability for use in MIoT devices. Furthermore, testing LEA revealed reduced CPU load, allowing MIoT systems to respond faster to changes in patients' health conditions. The article also discusses promising directions for security development in MIoT, including quantum cryptography and the use of simulation environments for modeling cyberattacks. Emphasis is placed on the potential of quantum cryptography to provide an unprecedented level of medical data protection, while simulation platforms enable testing of security measures in controlled conditions with various attack scenarios on MIoT systems. The approaches proposed in the article aim to ensure reliable protection of medical data without overloading the devices, which is crucial for maintaining the efficiency of MIoT systems in resource-constrained environments.

Keywords

MIoT, cryptographic algorithms, LEA, AES-128, data security, network level, data confidentiality, data integrity, energy consumption

1. Introduction

The Medical Internet of Things (MIoT) is one of the key directions of modern technologies, integrating medical devices, sensors, software, and network infrastructure to ensure continuous monitoring and management of patients' health conditions [1]. This technology creates opportunities for improving the quality of healthcare services, reducing treatment costs, and optimizing diagnostic and therapy processes. MIoT significantly extends the capabilities of modern medicine, allowing for remote monitoring of patients, automated health parameter control, and timely response to changes in their condition [2].

The number of MIoT devices is steadily increasing, driven by the growing demand for health monitoring technologies, particularly among people with chronic diseases and elderly patients. In 2023, the MIoT market was valued at $144.23 billion USD and is expected to grow at an annual rate of 20.4%, reaching $668.07 billion by 2030 [3]. This growth is attributed to the increasing use of medical devices, such as stationary devices, implantable medical devices, and wearable devices, which are becoming more popular due to improved access to technology and government healthcare initiatives [4]. Among the most common MIoT devices are wearable gadgets for monitoring heart

IDDM'24: 7th International Conference on Informatics & Data-Driven Medicine, November 14–16, 2024, Birmingham, UK

[*] Corresponding author.

[†] These authors contributed equally.

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)

rate, glucose levels, blood pressure, and other vital indicators, as well as medical implants and devices for remote therapy control. In recent years, the MIoT market has shown rapid growth in the number of devices installed in hospitals, clinics, and even at home (Figure 1). It is expected that by 2025, the number of medical IoT devices will increase several times. These trends indicate the need for significant measures to ensure their security [5], as MIoT networks transmit vast amounts of sensitive and critical information related to medical procedures and decisions.

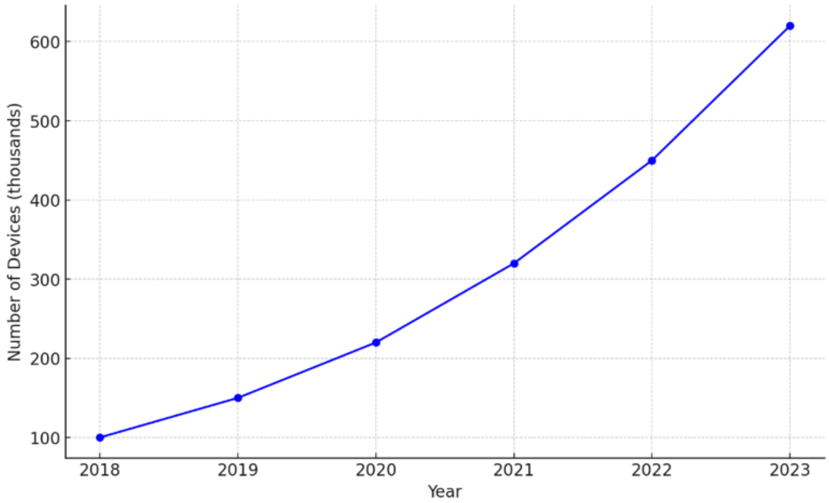


Figure 1: Dynamics of MIoT device implementation.

Structurally, MIoT consists of several layers, specifically the application, network, and physical layers. This three-layer architecture is depicted in Figure 2. The application layer encompasses software solutions and interfaces that interact with users, such as healthcare professionals or patients. Application programs analyze data obtained through medical sensors and use it to assist in decision-making aimed at improving the efficiency of medical care. The network layer is responsible for data transmission between devices, servers, and cloud solutions. It ensures information exchange between different elements of the system but is vulnerable to cyberattacks, which can affect the confidentiality, integrity, and availability of data. The physical layer includes medical devices, sensors, and other hardware components that directly collect data from patients. This layer is the foundation of the entire MIoT system but is also susceptible to physical interference and device failures.

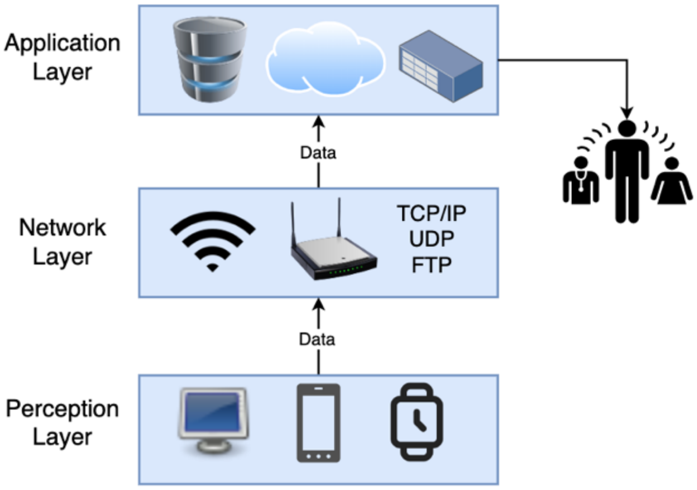


Figure 2: Three-layer MIoT architecture.

The high sensitivity of the data processed in MIoT makes research in this area highly relevant. Since MIoT systems work with confidential medical information that is subject to strict regulatory requirements, ensuring data protection is a critical task [6]. Any data breach or compromise can have serious consequences for both patient health and the legal status of medical institutions. Moreover, data security is a crucial aspect of maintaining patient trust in medical technologies, as any data loss can significantly impact the reputation of healthcare facilities [7].

At the same time, the limited computational power and energy resources of most medical devices make resource efficiency one of the main requirements for ensuring security in MIoT [8]. Traditional encryption methods, which typically require substantial computational and energy resources, are not optimal for such systems. Therefore, implementing lightweight cryptographic solutions that do not overburden devices becomes an urgent necessity [9]. This approach allows for effective data protection while preserving the autonomy and functionality of the devices for extended periods.

Given the structure of MIoT, protection at the network level is particularly important, as it is at this level that data is transmitted between devices and external systems [10]. The network level is one of the most vulnerable components in this structure, and attacks at this level can have critical consequences, including data interception, alteration, or loss. Considering that medical devices often operate in real time, ensuring reliable data security in the network becomes one of the key aspects of safety [11]. The use of resource-efficient protection methods, such as lightweight cryptographic algorithms, helps reduce the risk of attacks without overloading the devices, which is especially relevant for medical applications where every second counts.

The aim of this research is to develop and analyze resource-efficient methods for data protection at the network level of the Medical Internet of Things, which provide an appropriate level of security considering the limited resources of medical devices. Ensuring compliance with these criteria will improve the security of MIoT systems while maintaining their effectiveness and reliability in working with patients.

2. Background research

Currently, the results of numerous studies on data security in MIoT devices have been published. Researchers have considered various approaches to information protection using both traditional and lightweight cryptographic algorithms. Specifically, Qiu et al. analyzed the application of standard encryption methods for data security in medical systems. This study discussed the challenges of adapting these methods to devices with limited computational resources, emphasizing the need to reduce energy consumption and computational costs [12].

Additionally, the study conducted by Prince and Lovesum focuses on the use of protocols that take into account the specifics of medical devices, such as protecting data during transmission from wearable devices to cloud services [13]. The authors developed a lightweight encryption protocol capable of providing the required level of security without significant processor load, which confirms its applicability in real-world scenarios.

The study by Deebak, Al-Turjman, Aloqaily, and Alfandi focuses on improving authentication mechanisms for medical IoT devices by proposing innovative biometric-based schemes that can effectively counter modern threats, such as man-in-the-middle (MITM) attacks [14]. This enhances network-level security and provides an additional layer of data protection.

In another work, Kumar, Gupta, and Tripathi examined the impact of cyber threats on the network level of MIoT, proposing enhanced authentication and access methods [15]. Of particular note is the study conducted to evaluate the effectiveness of lightweight cryptographic algorithms, such as Lightweight Encryption Algorithm (LEA), GIFT, and others, in medical devices, highlighting their suitability for reducing the load on systems with limited resources. These works justify the use of resource-efficient methods capable of providing the required level of security without significant performance loss.

However, considering the continuous expansion of MIoT networks and increasing demands for data confidentiality and integrity, the need to find new resource-efficient solutions for network-level security remains relevant. Current research continues to focus on the development of new cryptographic schemes that consider MIoT device limitations, effectively protect data under constrained computational resources, and ensure low energy consumption, which is critical for medical applications. These aspects define future directions for MIoT security research, aiming not only to enhance security but also to ensure the practicality of solutions in real-world medical IoT device environments.

3. Network level attacks in MIoT

The network layer of MIoT is one of the most vulnerable because devices transmit sensitive medical data over various communication channels, often using weakly protected protocols [16]. The main threats at this layer arise from weak protection of communication protocols, lack of reliable authentication, unencrypted connections, and poor network segmentation. This makes MIoT systems susceptible to various attacks that can compromise the confidentiality, integrity, and availability of medical data [17]. Network-level attacks can have serious consequences for medical systems. They can lead to data access loss, manipulation of patient metrics, theft of sensitive information, and even the disruption of critical medical processes. These attacks are often aimed at intercepting traffic, interfering with data transmission, or disabling network services used by MIoT devices [18]. Table 1 presents the main vulnerabilities of the MIoT network layer.

Table 1
Main vulnerabilities of the MIoT network layer

Type of attack	Description	Protection methods
MITM	Interception of communication between MIoT devices and central systems for spying, altering, or injecting false data.	Implementation of TLS/DTLS, data encryption, robust authentication.
DoS/DDoS	Overloading MIoT devices or networks with traffic, making them unavailable.	Network segmentation, traffic filtering, use of IDPS (Intrusion Detection and Prevention Systems).
Ransomware	Encrypting critical medical data to demand a ransom for unlocking it.	Regular backups, software updates, multi-factor authentication.
Data Breaches	Exploiting vulnerabilities to steal confidential patient information.	Data encryption, access control, traffic monitoring.
Remote Code Execution (RCE)	Remote execution of malicious code on MIoT devices through software vulnerabilities.	Software updates, use of secure protocols, access control.
Replay Attacks	Intercepting and retransmitting legitimate data between devices and servers, deceiving the system.	Use of one-time session keys, replay protection.
Device Takeover	Maliciously gaining control over devices to alter settings or disable them.	Strong authentication, access control, device monitoring.

In addition to analyzing attacks, an important step is to build a model for implementing threats at the network level, which allows for a clear assessment of the risks to the system and its vulnerable points. A unified approach is proposed for constructing a mathematical model that considers the key parameters of network attacks, such as the volume of intercepted traffic, the effectiveness of encryption, and protective mechanisms (1). This model enables an accurate assessment of the probability of a successful attack and aids in developing more robust protection strategies for the MIoT system at the network level.

$$P_s = \frac{\sum_{i=1}^{n}(\frac{T_a}{T_d} \cdot \frac{L_c}{L_t} \cdot \frac{1}{S_e}) \cdot (1 - E_p) \cdot A_n}{n}, \tag{1}$$

where P_s – is the overall probability of a successful attack at the network level, n – is the number of attacks or attack attempts, T_a – is the volume of malicious traffic or data transmitted by the attacker, T_d – is the bandwidth of the protective system (firewalls, IDS/IPS, gateways), L_c – is the number of compromised packets or data, L_t – is the total volume of data transmitted in the network, S_e – is the effectiveness of the encryption used to protect the traffic (measured in bits), E_p – is the effectiveness of the implemented protective mechanisms (including encryption, authentication, network segmentation), and A_n – is the level of network availability or its resilience to attacks.

According to the model, the ratio $\frac{T_a}{T_d}$ characterizes the system's ability to handle malicious traffic or data transmitted by the attacker. If the volume of malicious data entering the network significantly exceeds the bandwidth of the protection system, the probability of a successful attack increases. The ratio $\frac{L_c}{L_t}$ indicates the proportion of compromised traffic among the total volume of transmitted data. The more compromised data in the network, the higher the attacker's chances of gaining control over the information. The parameter S_e accounts for the effectiveness of encryption: the stronger the encryption, the lower the probability that the attacker will successfully decrypt the intercepted data. The effectiveness of the system is also influenced by the parameter E_p, which reflects the level of implemented security measures. If the protective mechanisms are reliable and well-configured, the overall probability of a successful attack decreases. A high probability of success P_s means that the attacker manages to bypass or break the defenses, while a low value indicates the system's ability to effectively handle threats.

Effective protection at the network level includes the implementation of secure data transmission protocols, such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), reliable authentication methods, and network segmentation to minimize risks [19, 20]. The implementation of these measures helps to protect medical data, maintain the confidentiality and integrity of transmitted information, and reduce the likelihood of unauthorized access to devices.

4. Resource-efficient solutions for data security in MIoT

The development of resource-efficient solutions for data security in MIoT is an extremely important task due to the limited computational resources of medical devices. As mentioned, MIoT consists of numerous sensors, wearable gadgets, and stationary medical devices used for monitoring patient health, collecting, and transmitting sensitive medical information. In such conditions, traditional data protection methods may be ineffective due to their inherent high demands on computational power and energy consumption.

Resource-efficient solutions focus on optimizing existing technologies and implementing new approaches that provide the necessary level of security with minimal energy and resource expenditure [21]. Key directions include the implementation of lightweight cryptographic algorithms that reduce the load on the processor and architectural solutions that enhance network protection while maintaining performance [22]. These approaches help create secure, efficient, and energy-saving systems capable of resisting modern cyber threats.

An important component of resource-efficient solutions is the adaptation of security protocols and algorithms for operation under low power and limited computational resources [23]. This includes not only lightweight encryption algorithms but also specialized architectural solutions that reduce risks at the network level while ensuring a high level of reliability and data confidentiality. In particular, a multi-layered approach to security reduces the likelihood of data compromise, enhancing the overall resilience of network systems.

4.1. Resource-efficient cryptographic algorithms for data protection at the network level of MIoT

Resource-efficient cryptographic algorithms are key components for ensuring data security in MIoT, where it is critically important to maintain a balance between security and the limited computational resources of devices. Effective encryption ensures the confidentiality and integrity of data transmitted between MIoT devices and servers, minimizing the risks of compromise. The main challenge lies in selecting cryptographic algorithms that fit the limited resources of devices with low computational power and energy consumption.

One of the key tasks is choosing the appropriate cryptographic algorithm. Lightweight algorithms such as LEA, GIFT, and SPECK provide high data processing speeds with minimal resource load on devices [24]. LEA offers high speed and low energy consumption, making it an ideal choice for low-power MIoT devices. GIFT and SPECK algorithms also have minimal resource requirements and are suitable for devices with limited computational capabilities [25]. In some cases, optimized AES may be used for more powerful devices, providing a high level of security with minor adjustments.

The integration of encryption can be implemented at the software and firmware level of the device. Modern MIoT devices allow firmware updates to add encryption features, and cryptographic libraries such as mbedTLS or WolfSSL support lightweight algorithms [26]. This enables devices to maintain efficiency while protecting data from compromise.

Encrypting data at the transmission stage is also an important component of protection. The use of protocols such as TLS or DTLS ensures reliable encryption of data transmitted between devices and cloud services, safeguarding them from interception. Asymmetric algorithms are used for key exchange, providing secure transmission of keys for subsequent symmetric encryption.

Additionally, protecting data at the device level is crucial for ensuring their security in the event of device compromise. The use of flash or RAM encryption helps safeguard data even in cases of physical access to the device. Some MIoT devices support hardware encryption, which enables faster data processing and reduces the load on the processor.

Key management is a critical aspect of data protection. Securely storing keys in specialized hardware modules (Secure Element) and regularly updating keys prevent the use of vulnerable or compromised keys, maintaining a reliable level of security.

Based on the analysis of resource-efficient cryptographic algorithms and the need for data protection at the network level of MIoT, an important step is to build a secure system architecture. This architecture embodies the integration of modern cryptographic solutions into the software and hardware of MIoT devices and demonstrates how data protection is ensured during transmission over the network. Below is the structure of the secure MIoT system, which illustrates in detail the processes of data encryption, key management, and secure information transmission channels (Figure 3). The presented diagram illustrates the interaction of MIoT devices with cloud services through secure channels, focusing on ensuring the confidentiality and integrity of the transmitted data.

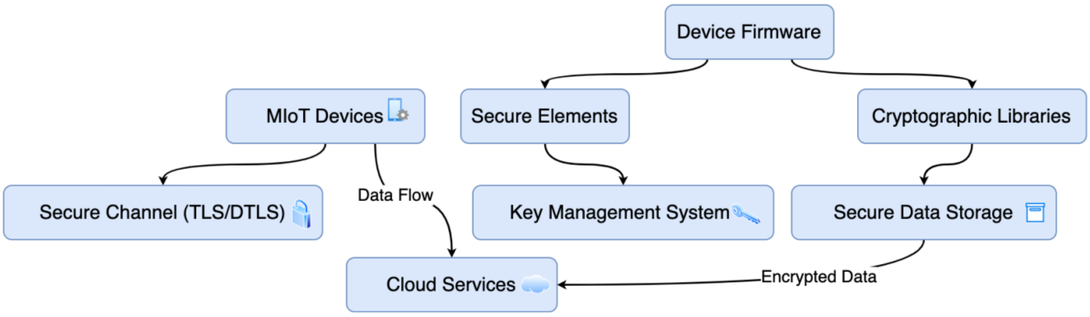


Figure 3: Architecture of the secure MIoT system.

The integration of cryptographic libraries into the device firmware enables encryption at both the storage level and during data transmission. The key management system (Secure Elements) provides secure storage and updating of cryptographic keys, reducing the risk of their compromise and enhancing the overall security of the system.

4.2. Architectural solutions for enhancing security at the network level

Resource-efficient architectural solutions are crucial for ensuring the security of MIoT, as they allow for the effective use of limited computational and energy resources of devices. The network level of MIoT is vulnerable to various types of attacks, making resource-efficient approaches aimed at reducing risks without significantly burdening the system critically important for data protection and the stable operation of devices.

Resource-efficient architectural solutions include:

1. **Network segmentation with traffic minimization.** Dividing devices into different virtual networks (VLANs) optimizes the use of network resources, reduces unnecessary traffic, and ensures data protection in each segment separately. Utilizing segmentation decreases the load on devices and improves the overall system performance.
2. **Implementation of lightweight security gateways.** Security gateways with minimal computational resource requirements monitor traffic and filter data. They can detect suspicious connections and control access to critical services, preventing unauthorized access to MIoT devices.
3. **Integration of lightweight intrusion detection and prevention systems (IDPS).** Lightweight IDPS are recommended for MIoT devices, as they can operate under limited resources. These systems provide real-time attack detection with minimal impact on device performance. They effectively identify anomalous actions, such as man-in-the-middle (MITM) attacks or DDoS attempts, allowing for timely responses to threats.
4. **Optimized network-level encryption.** Implementing TLS or DTLS protocols ensures traffic encryption between devices and servers with minimal energy costs. These protocols can be configured to use lightweight algorithms, such as LEA or GIFT, which provide reliable protection without significantly reducing data processing speed.
5. **Automated security policy management.** Utilizing automated systems for managing access policies and monitoring the network allows for rapid adaptation to changes in the network environment, reducing the need for manual intervention and minimizing the risk of human errors.

The listed resource-efficient architectural solutions provide reliable protection at the network level of MIoT without significantly negatively impacting the computational capabilities of devices. Overall, optimizing network processes, minimizing traffic, and using effective threat detection methods contribute to enhancing the security and stability of MIoT systems.

5. Comparison of proposed methods with traditional approaches

One of the key advantages of the proposed solutions is their low energy consumption, which is critical for battery-operated MIoT devices or those with limited energy resources. The use of lightweight algorithms, such as LEA, significantly extends the battery life of devices as they perform computations faster and with lower energy expenditure.

The proposed resource-efficient cryptographic algorithms, such as LEA, GIFT, and SPECK, differ significantly from traditional algorithms like AES and RSA in terms of efficiency and adaptation to the resource capabilities of MIoT devices. In particular, lightweight algorithms utilize simplified operations, such as XOR, addition, and shifting, which greatly reduce computational costs and energy requirements. Traditional algorithms, while providing a high level of security, often overload MIoT devices due to the complexity of computations and high energy consumption.

During the experiment, several cryptographic algorithms were tested on real models of resource-constrained microcontrollers, such as Texas Instruments CC2538 and NXP Kinetis KL02. The testing included a comparison of metrics such as encryption execution time, power consumption, and impact on the overall performance of the device (Table 2).

Table 2
Operational characteristics of cryptographic algorithms

Algorithm	Encryption time (ms)	Energy consumption (mW)	CPU load (%)
LEA	1.5	18	5
GIFT	1.8	20	6
SPECK	2.0	22	7
AES-128	4.5	38	12
RSA	10.0	65	20

The comparison showed that the resource-efficient algorithms LEA, GIFT, and SPECK have significantly better performance and energy consumption metrics compared to traditional algorithms like AES-128 and RSA. The advantage of 2-3 times faster encryption execution with simultaneously lower CPU load and significantly reduced energy consumption provided by lightweight algorithms is critically significant for MIoT devices.

The security aspects of using lightweight algorithms are also noteworthy: although they are less complex than traditional ones, they can effectively withstand most types of attacks, including those at the network level. The proposed architectural solutions, such as network segmentation and the implementation of lightweight security gateways, further enhance protection by minimizing the risks of data interception and unauthorized access.

6. Analysis of efficiency

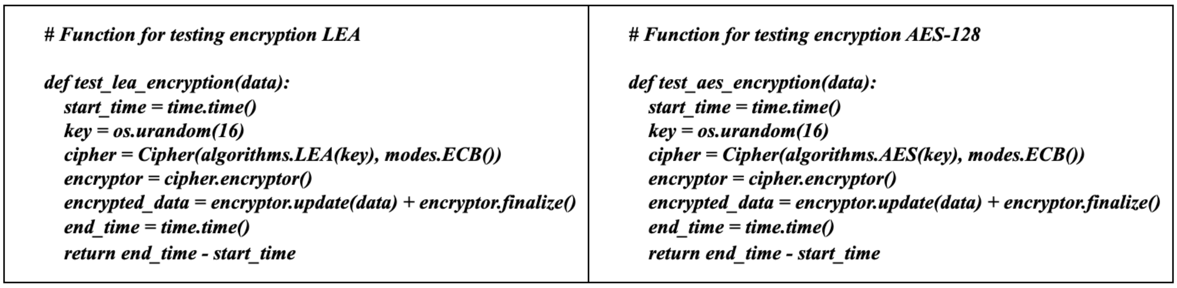
The proposed resource-efficient cryptographic solutions were tested in a software environment using the Python programming language. Undoubtedly, due to the relatively low speed of the resulting applications, Python is not an optimal language for the industrial implementation of cryptographic algorithms. However, it offers significant advantages as a testing and modeling tool in research settings. Its high-level syntax and extensive library ecosystem, such as *cryptography* and *pycryptodome*, allow for rapid prototyping and a focus on evaluating algorithm efficiency without significant time investment in implementation. With a broad selection of libraries for simulation modeling and performance analysis (notably *timeit* for measuring execution time and *psutil* for resource monitoring), Python simplifies experiment execution and data collection regarding efficiency. Its cross-platform nature also ensures versatility for running tests across different environments, which is important for verifying algorithm robustness. Thus, Python serves as a convenient tool for the preliminary evaluation of cryptographic algorithms before low-level implementation in languages optimized for performance, like C or C++.

To ensure accuracy and objectivity in evaluating cryptographic algorithms, a specialized research testbed was created. Its functionality allows for measuring key performance parameters in conditions close to real-world scenarios for MIoT devices. The foundation of these experiments included the following components:

1. **Hardware.** Testing was conducted on a computer equipped with an Intel Core i5 processor and 8 GB of RAM, providing sufficient computational power for simulating MIoT devices. To evaluate the performance of cryptographic algorithms in resource-constrained environments, an ESP32-WROOM-32 microcontroller was used as additional hardware. Power consumption was measured using a power module with power-monitoring capabilities.

2. **Software.** Experiments were conducted in a Linux environment (Ubuntu 20.04) using Python libraries, such as *cryptography* for AES-128 and specialized lightweight libraries for LEA. Performance measurement tools included *timeit* and *psutil*.
3. **Methodology.** Encryption was performed on instances of randomly generated data with a size of 1 KB. The resource demand of the algorithms was evaluated under representative conditions with the following metrics: execution time for encryption and decryption operations, power consumption, and CPU load. To ensure the reliability of results, each algorithm underwent a series of 10 test runs under stable conditions. After each encryption cycle, power consumption measurements were taken. Measurements were recorded using specialized power analysis equipment connected to the ESP32-WROOM-32 microcontroller on which the algorithms were tested. This setup provided actual data on CPU load and energy consumption. The effectiveness of security mechanisms was tested by simulating various attacks, including MITM, DoS, and DDoS, in a controlled environment. For this purpose, specialized scripts were used to model malicious traffic behavior and the system's response to it. Specifically, during DoS attacks, the system's ability to maintain stable operation under load was monitored, while during MITM attacks, the resilience of security algorithms to data interception was assessed. All processes were tracked using an Intrusion Detection System (IDS) to log traffic anomalies. Network resilience was evaluated by calculating the probability of a successful attack, taking into account the system's capability to filter malicious traffic.

The simulation approach allowed precise control over the encryption process, enabling performance assessment and comparison of lightweight algorithms with traditional methods. For testing, the lightweight LEA algorithm and the traditional AES-128 were selected. The tools used for their analysis are presented in Figure 4. Both functions are designed to measure the time required to encrypt random data (based on *os.urandom*) using the LEA and AES-128 algorithms in ECB mode. The encryption process includes key generation, data encryption, and execution time measurement. According to the experiment results, LEA achieved the following: encryption time – 0.0015 seconds, power consumption – 18 mW, CPU load – 5%. For AES-128, the data obtained were: encryption time – 0.0045 seconds, power consumption – 38 mW, CPU load – 12%.



```
# Function for testing encryption LEA

def test_lea_encryption(data):
    start_time = time.time()
    key = os.urandom(16)
    cipher = Cipher(algorithms.LEA(key), modes.ECB())
    encryptor = cipher.encryptor()
    encrypted_data = encryptor.update(data) + encryptor.finalize()
    end_time = time.time()
    return end_time - start_time
```

```
# Function for testing encryption AES-128

def test_aes_encryption(data):
    start_time = time.time()
    key = os.urandom(16)
    cipher = Cipher(algorithms.AES(key), modes.ECB())
    encryptor = cipher.encryptor()
    encrypted_data = encryptor.update(data) + encryptor.finalize()
    end_time = time.time()
    return end_time - start_time
```

Figure 4: Functions for testing encryption with LEA and AES-128.

Thus, the experiment confirmed that lightweight algorithms are significantly more efficient than traditional ones in resource-constrained systems, providing fast encryption with lower energy consumption. The anomalies detected by the IDS confirmed the high effectiveness of lightweight algorithms in identifying and blocking threats. Consequently, they can effectively counteract attacks without overloading the system, specifically by maintaining stable CPU load and minimal energy consumption even during active exposure to malicious factorsthem.

7. Discussion

In addition to the successful testing of the advantages of lightweight cryptographic algorithms, an important aspect is the identification of promising directions for the further development of data protection in MIoT. Among the key trends that could significantly enhance security in medical networks are quantum cryptography and simulation environments for modeling cyberattacks and testing security effectiveness.

Although the implementation of quantum cryptography in MIoT is currently somewhat challenging due to technical limitations and high costs, its potential in the future is undeniable. Quantum algorithms have the ability to provide an exceptionally high level of security due to the properties of quantum mechanics, such as the impossibility of cloning quantum states and detecting interception attempts. The prospects of integrating quantum cryptography into MIoT open new opportunities for securing sensitive medical information. One example is the use of Quantum Key Distribution (QKD) to ensure secure data transmission. However, this requires further research into optimizing quantum solutions for the limited resources of MIoT devices.

Another important direction is the development and use of simulation environments for modeling cyberattacks and testing protective measures. Since real attacks on MIoT systems can have catastrophic consequences for patient health, simulations allow for the prior assessment of network vulnerabilities and the effectiveness of protective measures. Modern simulation platforms provide the ability to detail various attack scenarios, such as Man-in-the-Middle (MITM) attacks, DDoS, and others. They also allow for testing defensive measures, such as lightweight cryptographic algorithms, for resilience against various types of threats under controlled conditions. This may include simulating interactions between devices, data transmission, and the application of security protocols. With the development of such simulation environments, researchers can quickly test new algorithms and architectural solutions, evaluate their effectiveness, and identify potential weaknesses without risking real systems. This also opens opportunities for building effective machine learning models capable of automatically identifying potential threats and adapting security strategies.

In the context of resource-efficient solutions, an important direction is also the development of artificial intelligence technologies for automatic threat detection and anomaly identification in MIoT systems. The integration of machine learning algorithms allows for the creation of adaptive security systems that not only respond to known attacks but also predict potential threats based on real-time analysis of large data sets.

Thus, the prospect of integrating quantum technologies, simulation environments, and artificial intelligence into MIoT security systems opens new horizons for enhancing network-level security and effectively utilizing the resources of medical devices. Further development in these areas will be a crucial step towards ensuring the reliable operation of MIoT systems.

8. Conclusion

The results of the conducted research confirmed the effectiveness of the proposed resource-efficient solutions for data protection at the network level of MIoT systems. Special attention was given to the use of lightweight cryptographic algorithms, such as LEA, and their advantages compared to traditional algorithms like AES-128. The testing demonstrated that lightweight algorithms provide fast encryption and low energy consumption, which is critically important for medical devices with limited resources. The use of LEA reduced the encryption time by almost three times compared to AES-128, with more than twice the energy savings. This shows that the proposed methods are not only effective in terms of security but also help preserve the energy resources of devices, extending their autonomous operation. Considering that many MIoT devices operate on batteries or have limited power, such reductions in energy consumption represent a significant advantage. Additionally, during the testing with LEA, a significantly lower CPU load was also observed, which is important for maintaining stable operation of devices in real-time. This advantage is critically significant in a medical context, as reducing the load on processing components will allow MIoT systems to respond more quickly to changes in patients' health conditions.

Undoubtedly, it is worth noting that while lightweight cryptographic algorithms demonstrate excellent results in terms of energy efficiency and speed, they may offer lower levels of security compared to more complex algorithms like AES-128. However, in the context of MIoT, where it is important to ensure a balance between security and efficiency, lightweight algorithms such as LEA offer an optimal solution.

Further research could focus on expanding the range of tested algorithms, including additional lightweight algorithms, and analyzing their effectiveness under different conditions. Investigating methods for integrating lightweight algorithms into real MIoT devices, taking into account their limited computational power, is also important.

9. Declaration on Generative AI

During the preparation of this work, the authors didn't use Generative AI.

References

[1] N. Akhtar, S. Rahman, H. Sadia, Y. Perwej, A holistic analysis of Medical Internet of Things (MIoT), Journal of Information and Computational Science 11(4) (2021) 209-222.

[2] K. Kakhi, R. Alizadehsani, H. D. Kabir, A. Khosravi, S. Nahavandi, U. R. Acharya, The internet of medical things and artificial intelligence: trends, challenges, and opportunities, Biocybernetics and Biomedical Engineering 42(3) (2022) 749-771.

[3] Internet of Medical Things (IoMT) Market Size, Share & Trends Analysis Report By End-use (Hospitals, Clinics), By Component (Software, Services), By Deployment (Cloud, On-premise), By Application, By Region, And Segment Forecasts, 2023-2030, 2022. URL: https://www.grandviewresearch.com/industry-analysis/internet-of-medical-things-iomt-market-report.

[4] Internet of Medical Things (IoMT) Market Size, Share & Industry Analysis, By Product (Stationary Medical Devices, Implanted Medical Devices, and Wearable External Medical Devices), By Application (Telemedicine, Medication Management, Patient Monitoring, and Others), By End-user (Healthcare Providers, Patients, Government Authorities, and Others), and Regional Forecast, 2024-2032, 2023. URL: https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844.

[5] IoT Medical Devices Market Size, Share & Trends [2028], 2023. URL: https://www.marketsandmarkets.com/Market-Reports/iot-medical-device-market-15629287.html.

[6] Y. Perwej, N. Akhtar, N. Kulshrestha, P. Mishra, A Methodical Analysis of Medical Internet of Things (MIoT) security and privacy in current and future trends, Journal of Emerging Technologies and Innovative Research 9(1) (2022) d346-d371.

[7] M. Al-Emran, S. I. Malik, M. N. Al-Kabi, A survey of Internet of Things (IoT) in education: Opportunities and challenges, in: A. Hassanien, R. Bhatnagar, N. Khalifa, M. Taha (eds), Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. Studies in Computational Intelligence, vol. 846. Springer, Cham, 2020, pp. 197-209. doi:10.1007/978-3-030-24513-9_12.

[8] S. Pal, M. Hitchens, T. Rabehaja, S. Mukhopadhyay, Security requirements for the internet of things: A systematic approach, Sensors 20(20) (2020) 5897.

[9] 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.

[10] T. Almehmadi, S. Alshehri, S. Tahir, A secure fog-cloud based architecture for MIoT, in: 2019 2nd International Conference on Computer Applications & Information Security, ICCAIS, IEEE, 2019, pp. 1-6.

[11] N. N. Thilakarathne, H. D. Weerasinghe, A. Welhenge, A Multilayered Hybrid Access Control Model for Cloud-Enabled Medical Internet of Things, in: Sustainable Advanced Computing: Select Proceedings of ICSAC 2021, Springer Singapore, Singapore, 2022, pp. 455-471.

[12] 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.

[13] P. B. Prince, S. J. Lovesum, Privacy enforced access control model for secured data handling in cloud-based pervasive health care system, SN Computer Science 1(5) (2020) 239.

[14] B. D. Deebak, F. Al-Turjman, M. Aloqaily, O. Alfandi, An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT, IEEE Access 7 (2019) 135632-135649.

[15] P. Kumar, G. P. Gupta, R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, Computer Communications 166 (2021) 110-124.

[16] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek, H. M. Alkhassawneh, A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things, IET communications 16(5) (2022) 421-432.

[17] A. Omotosho, B. Ayemlo Haruna, Mikail O. Olaniyi, Threat modeling of internet of things health devices, Journal of Applied Security Research 14(1) (2019) 106-121.

[18] J. P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: Limitations, issues and recommendations, Future Generation Computer Systems 105 (2020) 581-606.

[19] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, D. Abbasinezhad-Mood, Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme, Future Generation Computer Systems 100 (2019) 882-892.

[20] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, N. Z. Jhanjhi, Secure healthcare data aggregation and transmission in IoT – A survey, IEEE Access 9 (2021) 16849-16865.

[21] I. Rozlomii, A. Yarmilko, S. Naumenko, Data security of IoT devices with limited resources: challenges and potential solutions, in: Proceedings of the doors-2024: 4th Edge Computing Workshop, ceur-ws.org, vol. 3666, 2024, pp. 85-96.

[22] M. Rana, Q. Mamun, R. Islam, Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129 (2022) 77-89.

[23] S. S. Dhanda, B. Singh, P. Jindal, Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications, 112(3) (2020) 1947-1980.

[24] L. Sleem, R. Couturier, Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. Multimedia Tools and Applications, 80(11) (2021) 17067-17102.

[25] J. A. Chauhan, A. R. Patel, S. Parikh, N. ModiAn analysis of lightweight cryptographic algorithms for IoT-Applications, in: International Conference on Advancements in Smart Computing and Information Security, Springer Nature, Cham, Switzerland, 2022, pp. 201-216.

[26] S. Deng, M. Li, Y. Tang, S. Wang, S. Yan, Y. Zhang, Automated Detection of Ciphertext Side-channel Vulnerabilities in Cryptographic Implementations, in: 32nd USENIX Security Symposium, USENIX Security 23, 2023, pp. 6843-6860.