Journal of Edge Computing, 2025, Vol. **4**, Iss. 1, pp. 35–56 https://doi.org/10.55056/jec.748

Innovative resource-saving security strategies for IoT devices

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

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

Abstract. The astounding trend of increasing the number of connected IoT devices reflects the growing importance of this technology in industry, healthcare, the domestic sphere, and other sectors. However, with the expansion of IoT capabilities, the number of challenges also rises, particularly regarding the security of these devices, many of which are characterised by limited resources such as memory, power consumption, computational power, and network bandwidth. This article examines the key challenges associated with ensuring the security of IoT devices and proposes potential solutions and optimisation strategies that consider these limitations. The primary focus is developing and analysing lightweight cryptographic algorithms capable of providing robust data protection with minimal resource usage. The article also discusses efficient energy management strategies and optimising memory usage in IoT devices. Emphasis is placed on developing adaptive security mechanisms that can effectively respond to dynamic operational conditions and resource constraints. It is noted that further research and development should focus on creating integrated solutions that combine hardware, software, and managerial aspects to optimise the overall efficiency and security of IoT systems.[1]

Keywords: IoT, limited resources, cryptographic algorithms, energy efficiency, memory management, authentication algorithms, cyber threats

1. Introduction

Embedded Internet of Things (IoT) devices have gained widespread use in various sectors, including industry, agriculture, healthcare, transportation, household systems, and smart cities [47]. These devices provide process automation, environmental monitoring, efficient resource management, and improved quality of life. The ability of IoT devices to collect, process, and transmit data in real-time opens up new opportunities for enhancing productivity and creating innovative solutions across different fields [2].

Figure 1 shows a graph illustrating the growth in the number of embedded IoT devices over recent years. As can be seen, the number of such devices has steadily increased, demonstrating remarkable growth from 10.0 billion in 2019 to 16.6 billion in 2023. This trend reflects the growing importance of IoT devices in various sectors, including industry, household systems, healthcare, and other fields [24].

In modern understanding, the term “IoT devices” encompasses many devices connected to the Internet of Things network. These devices collect, process, and transmit data over the network. IoT devices can include large industrial sensors and small household devices that perform specific functions within a networked environment.

[1]This paper is the further development of our work [33] presented at the 4th Edge Computing Workshop.

0000-0001-5065-9004 (I. Rozlomii); 0000-0003-2062-2694 (A. Yarmilko); 0000-0002-6337-1605 (S. Naumenko)
inna-roz@ukr.net (I. Rozlomii); a-ja@ukr.net (A. Yarmilko); naumenko.serhii1122@vu.cdu.edu.ua (S. Naumenko)

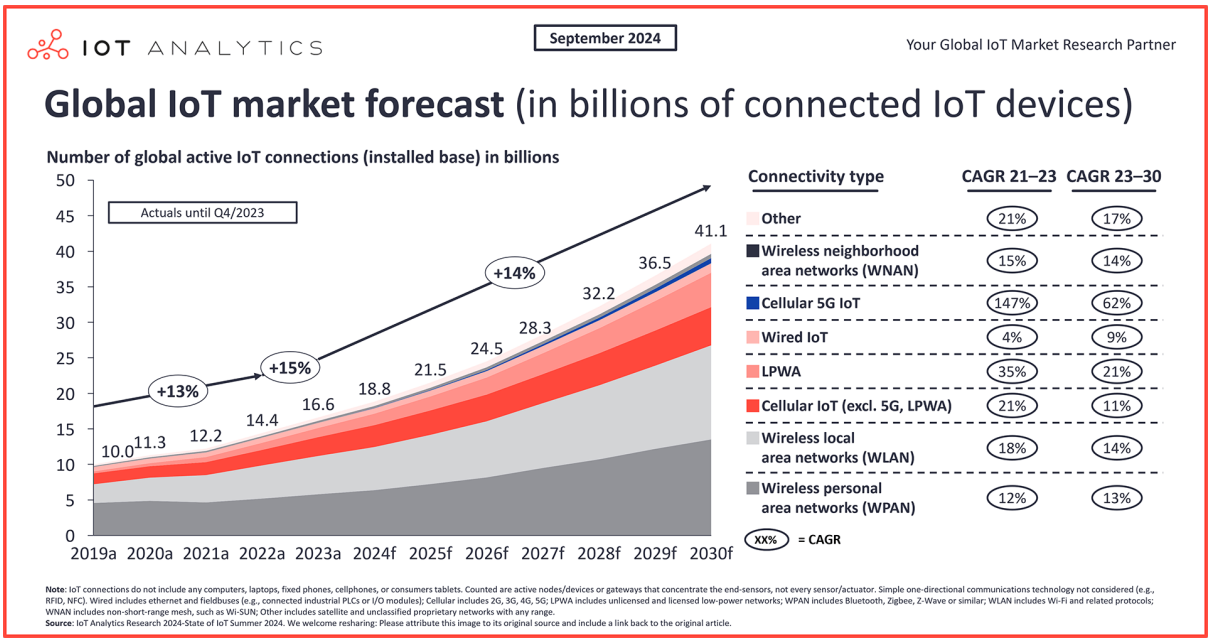

Figure 1: Growth in the number of embedded IoT devices from 2019 to 2023 (in billions) [41].

Embedded IoT devices are a subcategory of IoT devices. In addition to being network-connected, they have limited resources such as computational power, memory, and energy consumption. They are designed as embedded components for operation within larger systems, particularly in limited space or energy usage conditions, making them indispensable in distributed information systems in industries, healthcare, and other sectors.

Embedded IoT devices are compact, integrated devices embedded in various objects capable of collecting, processing, and utilizing data and exchanging it over a network without direct human involvement [23]. These devices provide automation and monitoring in various fields, from household systems to industrial processes, using their computational resources to perform their functions [19, 38].

The significance of embedded IoT devices lies in their ability to add intelligence and functionality to different systems, facilitating data collection, process automation, and productivity enhancement [8]. They have become an essential element in advancing technologies and the development of the connected world [6].

However, the security of embedded IoT devices has become a key issue limiting their application [11]. This problem arises from the imbalance between the potentially high functionality of such devices and their resource constraints [21]. The limited computational power and memory resources of embedded devices typically complicate the implementation of robust security mechanisms to prevent unauthorized access to data and control the flow of information processes [45]. This poses serious challenges in ensuring security, as these devices may become targets of external attacks with critical consequences of both technical and humanitarian-legal nature [18, 40].

The main challenges in ensuring the security of embedded IoT devices are their insufficient protection and vulnerability to cyberattacks due to limited support for encryption and authentication and inadequate capabilities for detecting and responding to potential threats.

This study aims to analyze the security challenges faced by resource-constrained embedded IoT devices and develop optimized cryptographic strategies that provide adequate data protection without excessively using the device's resources. The research focuses on adapting lightweight cryptographic algorithms to the constraints of limited

computational power, energy consumption, and memory, enabling improved security for these devices in real-world operational conditions.

2. Related works

Numerous studies are dedicated to the security issues of embedded IoT devices with limited resources [5, 29]. Many of them indicate that the physical constraints of such devices complicate the implementation of comprehensive security measures and are the primary cause of numerous vulnerabilities. In these security studies, the importance of embedded IoT device security has garnered significant interest due to its crucial role in daily life, industry, and infrastructure. Many works highlight the fundamental challenge of the mismatch between data protection needs and the limited resources of the devices.

Meneghello et al. [26] investigated the primary vulnerabilities of IoT devices, indicating that limited computational resources, memory, and power significantly impact the effectiveness of security measures. Their research showed that most devices cannot implement robust cryptographic algorithms due to these limitations, making them vulnerable to attacks.

Jiang, Lora and Chattopadhyay [17], justifying the importance of implementing lightweight cryptographic methods, conducted an experimental analysis of vulnerabilities in industrial IoT devices. They found that even minimal protective measures can significantly enhance security, but their implementation requires adaptation to the specific constraints of limited resources.

Tiburski et al. [44] proposed a lightweight security architecture based on virtualization and trust mechanisms for IoT devices. Their approach ensures the necessary level of protection with minimal resource consumption, which is critically essential for embedded systems with limited resources.

Notably, Rajesh et al. [30] presents an efficient, lightweight, symmetric encryption scheme for transmitting text files between embedded IoT devices. Their results showed that using optimized cryptographic methods can significantly reduce resource consumption without compromising the level of protection.

Rozlomii et al. [31], Yar et al. [46] proposed an authorization scheme for smart homes that provides a high level of security with limited computational resources. They emphasize the importance of developing efficient authentication algorithms that can operate under resource constraints.

Thus, the existing scientific and practical results indicate the need to develop and implement effective security methods for embedded IoT devices, considering their limited resources and the necessity for a high level of protection. Special attention should be given to creating adaptive authentication mechanisms and cryptographic protection optimally utilising the devices' available resources. Advancing these technologies is a key direction for future research to ensure reliable IoT system security in the face of dynamically evolving threats.

3. Architecture and constraints of embedded IoT devices

The resource constraints of embedded IoT devices arise from the need to create compact, energy-efficient, and cost-effective devices. Embedded IoT devices often need to operate autonomously, using limited power sources such as batteries or consuming minimal energy for prolonged operation [32]. Consequently, their components must be optimized to perform specific tasks with minimal resource expenditure.

From a security perspective, these constraints pose additional challenges. Ensuring reliable data protection and uninterrupted device operation becomes more complex due to the limited capacity to implement sophisticated cryptographic algorithms, process

large volumes of data, and maintain constant threat monitoring [36]. Therefore, it is necessary to develop specialized solutions that consider these limitations and effectively ensure the security of embedded IoT devices.

3.1. Architecture of embedded IoT devices

The architecture of embedded IoT devices includes three main components: sensors and actuators, data processors, and network interfaces [48]. Each of these components plays a critical role in the functioning of IoT systems, ensuring data collection, processing, and transmission.

3.1.1. Sensors and actuators

Sensors gather information from the surrounding environment by measuring temperature, humidity, light intensity, pressure, and motion. They are characterized by sensitivity, measurement range, accuracy, energy consumption, and data transmission speed. Conversely, actuators perform actions based on the received data and can be electromechanical, pneumatic, or hydraulic. They are characterized by response speed, positioning accuracy, power, and energy consumption.

Among the popular sensor models are the DHT22 for temperature and humidity measurement, MPU6050 for accelerometer and gyroscope measurements, and BH1750 for light intensity measurement. Actuators such as the SG90 servo motor, 28BYJ-48 stepper motor, and micro-pumps for fluid control are widely used in various IoT projects.

3.1.2. Data processors

Data processors include microcontrollers and specialized computing systems that process and analyze collected data. They are characterized by computational power, memory size, energy consumption, and support for various communication protocols. For example, the ESP32 supports Wi-Fi and Bluetooth, has a dual-core processor, and 520 KB of SRAM, while the Arduino Uno is based on the ATmega328P microcontroller, has 2 KB of SRAM, and 32 KB of flash memory. Raspberry Pi Zero W, a single-board computer with Wi-Fi and Bluetooth support, has 512 MB of RAM and a powerful Broadcom BCM2835 processor [12].

3.1.3. Network interfaces

Network interfaces communicate with the external environment through various protocols such as Wi-Fi, Bluetooth, LoRa, Zigbee, and NB-IoT. They are characterized by range, data transmission speed, energy consumption, and resistance to interference. Among the popular models are Wi-Fi modules ESP8266 and ESP32, Bluetooth modules HM-10 and HC-05, LoRa modules SX1276 and RFM95W, and Zigbee modules XBee S2C.

3.2. Primary functions of embedded IoT devices

Embedded IoT devices perform various core functions, ensuring efficient operation and network integration. These functions include data collection, processing, transmission, and actuator control. Each of these functions has its characteristics and requirements for the hardware and software components of the devices [25].

1. *Data collection* is a primary function of any IoT device. Embedded sensors gather information from the surrounding environment, such as temperature, humidity, light intensity, pressure, motion, etc. This process involves several stages:
    - sensor initialization – configuring and preparing sensors for data collection;
    - periodic data reading – regular retrieval of readings from the sensors;
    - preprocessing of data – filtering and normalization of data for further processing;

- data storage – storing collected data in internal memory or transmitting it to a data processor.

2. *Data processing* is the next step after their collection. This function involves analyzing and interpreting the gathered information to derive useful insights or determine necessary actions. Data processing may involve several stages:
   - data retrieval – obtaining data from internal memory or sensors in real-time;
   - processing algorithms – applying data processing and analysis methods such as filtering, aggregation, or machine learning;
   - action determination – making decisions based on processed data;
   - results storage – saving the processed results for further use or transmission.
3. *Data transmission* is a crucial function that facilitates communication between embedded IoT devices and other systems or devices. This includes transmitting data through network interfaces such as Wi-Fi, Bluetooth, LoRa, Zigbee, or NB-IoT. The key stages of this function include:
   - network connection – establishing a connection to the network using the appropriate protocol;
   - data transmission – sending collected and processed data to servers or other devices;
   - data reception – receiving data from other devices or systems for further processing;
   - security provision – encrypting and authenticating data to protect against unauthorized access.
4. *Actuator control* is the final function of embedded IoT devices, allowing interaction with the physical world based on collected and processed data. This includes:
   - command reception – receiving instructions from the data processor or other systems;
   - actuator initialization – preparing actuators for executing commands;
   - action execution – activating or adjusting actuators to perform necessary tasks;
   - feedback – providing feedback to the data processor about executing commands.

The listed functions of embedded IoT devices constitute the primary spectrum of their functional and technical advantages. Still, they have limitations associated with deployment platforms and methods of ensuring autonomy.

3.3. Resource constraints of embedded IoT devices

Embedded IoT devices often operate under strict resource constraints, significantly complicating their security and efficiency. The primary resources subject to limitations include computational power, energy consumption, memory, and network bandwidth. Let us examine them in more detail.

1. *Execution of complex computations due to limited computational power*. This may result in constraints on applying complex encryption algorithms and the performance of computationally intensive operations, reducing the device's security level.
2. *Memory.* The limited memory capacity in embedded devices complicates the storage of a large amount of data and software. This can reduce the available resources for storing encryption keys, user data, and other critical elements, increasing vulnerability to attacks.

3. *Power supply.* Embedded IoT devices often run on autonomous power sources or have limited power consumption. This limitation in power supply can lead to unforeseen interruptions in device operation or limit security capabilities, as the device may shut down or enter low-power mode, reducing its ability to detect and respond to potential threats.
4. *Network bandwidth.* Many IoT devices are connected to networks with limited bandwidth, which can result in data transmission delays and reduced overall system performance. This requires efficient data compression methods and optimization of network protocols to minimize traffic and ensure reliable communication.

The mentioned constraints affect embedded devices' capabilities in implementing robust security measures and pose challenges in ensuring reliability and data protection.

4. Vulnerabilities of the security systems in embedded IoT devices

One of the key issues in the field of embedded IoT devices is the presence of vulnerabilities that can be exploited for attacks and security breaches. Securing embedded IoT devices becomes crucial as these devices are used in various life domains, ranging from household systems to critical infrastructure [10, 20, 28]. However, they also become a heightened focus for cybercriminals due to a range of vulnerabilities:

1. *Inadequate authentication and authorization*. A low level of authentication can serve as a starting point for unauthorized access to the device. The absence of robust user identity verification methods, weak passwords, or simple authorization methods can be entry points for cyber-attacks [9]. This can occur due to inadequate determination of access rights to device functions or data. In the absence of authentication, the likelihood of a successful attack on the device can be described by the following formula:

$$P(A) = \frac{N_s}{N_t} \times 100\%, \tag{1}$$

   where $P(A)$ is the probability of an attack, N_s is the number of successful attacks, N_t is the total number of attack attempts.
2. *Insufficient cryptographic protection*. IoT devices' weak or outdated encryption algorithms make data more vulnerable to interception and compromise. Suppose encryption employs keys of insufficient length or is vulnerable to known attacks. In that case, there is a risk of compromising the confidentiality and integrity of data and threats to their availability. To determine the effectiveness of encryption, the Shannon encryption model can be utilized:

$$C = \log_2\left(1 + \frac{S}{N}\right), \tag{2}$$

   where C is the channel capacity, S is the signal power, N is the noise level.
3. *Insufficient software updates*: Limited memory in embedded devices can complicate the software update process. This creates a risk of temporary or permanent vulnerability of the device to new threats or vulnerabilities, as it may remain without updates to apply security patches or fix software defects that ensure security.

5. Security risks of embedded IoT devices

In the network of embedded IoT devices, ensuring security remains one of the main challenges. This is particularly crucial due to the limited resources characterizing these devices. Examining memory, energy consumption, and computational power issues, it can be observed that these aspects serve as potential security threats [15].

The limitation of memory in embedded systems complicates not only data storage but also the implementation of effective encryption methods. The reduced operational duration due to limited energy consumption becomes a starting point for potential DoS attacks [37]. Additionally, limited computational power complicates the application of robust encryption and authentication methods.

Considering memory, energy consumption, network bandwidth, and computational power, we can determine that:

- **Memory limitations** in embedded devices can lead to buffer overflows and constraints in storing encryption keys, complicating the cryptographic protection of information.
- **Energy supply** is a fundamental factor limiting the operational duration of devices and the risk of potential DoS attacks due to targeted expenditure of limited energy.
- **Limited computational power** complicates the application of complex encryption algorithms and may contribute to executing malicious code in case of insufficient input data validation.
- **Network bandwidth** is another crucial aspect that impacts the security of embedded IoT devices. Limited network bandwidth can pose several serious security risks, such as congestion, insufficient bandwidth, and denial-of-service attacks.

The discussed limitations expose risks that need to be carefully considered and adequately addressed in embedded IoT devices to ensure the reliability, confidentiality, and integrity of the processed data.

5.1. Risks due to limited power consumption

Limited memory capabilities can cause issues in implementing cryptographic protection for embedded devices due to buffer overflows and restricted capacity for key storage:

1. Buffer overflow allows embedding malicious code or executing code in vulnerable areas. The result is the emergence of vulnerabilities that attackers can exploit. Attacks leveraging these vulnerabilities may lead to system compromise, unauthorized code execution, or leakage of sensitive data.
2. Due to the limited memory capabilities of embedded IoT devices to store encryption keys, there is a risk of their compromise. This is due to the complexity of storing and managing encryption keys, which is critical for ensuring data security. Having diverse keys for various encryption tasks for system security is essential. However, providing the necessary volume of unique keys for data encryption may be challenging due to limited memory. Key management also becomes a challenge due to limited resources. For information security, keys must be efficiently stored, updated, and rotated. However, limited memory can restrict the capacity for storing and processing key information, complicating their effective management. Thus, the complex storage and management of keys can be a foundation for their compromise. If keys are not stored or managed correctly, they can become more accessible to attackers or increase the likelihood of system vulnerabilities to attacks aimed at obtaining these keys.

Considering the limited memory capabilities of embedded IoT devices, cryptographic protection may become vulnerable due to buffer overflows and difficulties in storing encryption keys. The structure of these issues is schematically illustrated in figure 2.

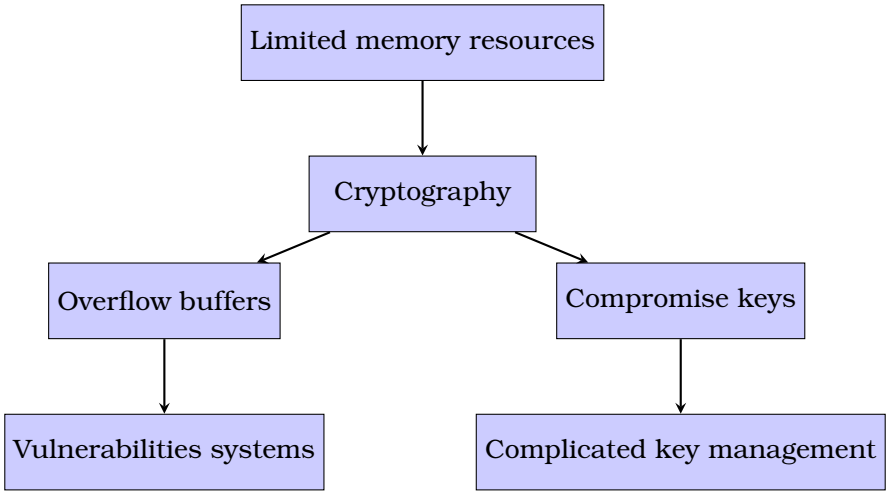

Figure 2: The relationship between memory constraints and the security of IoT devices.

5.2. Risks arising from memory limitations

Energy consumption of an embedded system may be insufficient for cryptographic protection due to the design features of autonomous IoT modules and the intentional unauthorized impact on their power components. Threats related to energy consumption pose a wide range of security risks for the system:

1. *Energy attacks* aimed at reducing the energy consumption of IoT devices pose a serious threat to their normal functioning. These attacks can be implemented by constantly activating devices, prompting them to consume excessive energy. The consequence of such excessive energy consumption can be the depletion of the device's battery, leading to its shutdown or disruption of regular operation. This can be problematic, especially for devices operating on batteries or in conditions of limited power supply. Continuous excessive energy consumption can decrease device performance and efficiency, making it more vulnerable to various attacks or limiting security capabilities due to insufficient energy for the normal operation of protective mechanisms.
2. Limited charge in an autonomous energy source can cause unforeseen *interruptions in the device's operation*, creating serious security risks. When energy becomes restricted, the device may abruptly shut down or transition into a low-power mode. Such interruptions in operation can decrease the device's reliability and may be exploited by malicious actors for attacks. As a result, data being processed or stored in the device at that moment may be lost or damaged. These unforeseen halts can create a window of opportunity for attacks on the device or its data, as they may be unavailable for protection or remain unprotected during such times.
3. *Reaction delays*. Limited energy consumption in embedded IoT devices aimed at energy conservation can significantly impact their response time when detecting threats or attacks. This can lead to delays in identifying anomalies or responding to potential threats in the network. For energy-saving purposes, a device may operate in a standby mode, during which it is inactive or does not perform specific operations. In this mode, it may be less responsive to changes or anomalous

situations, as it consumes minimal energy, affecting its ability to respond to real-time events. This delay in response can be critical in the case of rapidly evolving threats or attacks, where an immediate response is required to avoid potential consequences. Limited energy consumption may impede the detection or reaction to such events, increasing the risk to the system's security. These delays in detection or response can impact the overall reliability and security of the device in the face of persistent attacks or threats.

4. *Impact on encryption algorithms*. Encryption algorithms may be employed to ensure the security of IoT device data. However, their usage may be restricted in low energy consumption modes, and less effective algorithms may be selected [35]. This creates a risk of reducing the data protection level, as using less reliable encryption methods can make data more vulnerable to attacks by malicious actors. Limited energy consumption can affect the efficiency of encryption in embedded devices. The compromise between energy savings and encryption efficiency can increase devices' vulnerability to potential threats and cyber-attacks. In turn, the reduction in the level of data protection due to the use of less reliable encryption methods can complicate the recovery or protection of information in the event of attacks or unauthorized access to the device.
5. *Low battery levels* can significantly impact the effectiveness of cryptographic methods used to protect data. Cryptographic algorithms that demand substantial computational resources may operate unstably or lose efficiency due to limited energy supply. This can reduce the speed or accuracy of applying cryptographic methods, diminishing the level of data protection. With low battery charges, a device may lack sufficient power to implement complex encryption algorithms effectively, resulting in increased data processing times or even a decrease in the level of protection. Such unstable operation of cryptographic methods can compromise the device's security, making it more vulnerable to attacks.
6. *Recovery after power loss*. Restoring the operation of an embedded IoT device to its correct functional state can be challenging following a power loss. During sudden shutdowns or disconnections, the device may lose information about its previous state and current data. The difficulty or even impossibility of returning to the previous state directly affects its reliability and functionality.

Let us consider the effectiveness of protection against attacks when using an encryption algorithm where efficiency is denoted as E, the battery level is B, and the type of cryptographic methodology is C. One of the possible models of efficiency has the form of a linear function:

$$E = m \cdot B + c \cdot C, \tag{3}$$

where m and c are parameters reflecting the influence of the battery level and the type of cryptographic methodology, respectively.

Let us assume the values of the coefficients are as follows: $m = 0.5$ and $c = 0.8$. The battery level (B) varies from 1 to 10, and the cryptographic methodology parameter (C) can take values of 1 or 2. The possible values of data protection efficiency (E), calculated using model (1) and these parameters, are presented in table 1.

The linear model (3) can be adapted to more complex dependencies, following the example of a quadratic model:

$$E = a \cdot B^2 + b \cdot C^2 + d \cdot B \cdot C + e, \tag{4}$$

where a, b, d, e are coefficients reflecting the interaction of the battery level and the type of cryptographic methodology on the effectiveness of data protection.

Table 1
Evaluation of the energy-based attack protection efficiency model for an embedded device.

Charge level B	**Protection efficiency** E	
	C=1	C=2
1	$0.5 \cdot 1 + 0.8 \cdot 1 = 1.3$	$0.5 \cdot 1 + 0.8 \cdot 2 = 2.1$
2	$0.5 \cdot 2 + 0.8 \cdot 1 = 1.8$	$0.5 \cdot 2 + 0.8 \cdot 2 = 2.6$
3	$0.5 \cdot 3 + 0.8 \cdot 1 = 2.3$	$0.5 \cdot 3 + 0.8 \cdot 2 = 3.1$
4	$0.5 \cdot 4 + 0.8 \cdot 1 = 2.8$	$0.5 \cdot 4 + 0.8 \cdot 2 = 3.6$
5	$0.5 \cdot 5 + 0.8 \cdot 1 = 3.3$	$0.5 \cdot 5 + 0.8 \cdot 2 = 4.1$
6	$0.5 \cdot 6 + 0.8 \cdot 1 = 3.8$	$0.5 \cdot 6 + 0.8 \cdot 2 = 4.6$
7	$0.5 \cdot 7 + 0.8 \cdot 1 = 4.3$	$0.5 \cdot 7 + 0.8 \cdot 2 = 5.1$
8	$0.5 \cdot 8 + 0.8 \cdot 1 = 4.8$	$0.5 \cdot 8 + 0.8 \cdot 2 = 5.6$
9	$0.5 \cdot 9 + 0.8 \cdot 1 = 5.3$	$0.5 \cdot 9 + 0.8 \cdot 2 = 6.1$
10	$0.5 \cdot 10 + 0.8 \cdot 1 = 5.8$	$0.5 \cdot 10 + 0.8 \cdot 2 = 6.6$

Models (3) and (4) can be supported and refined through experiments, data analysis, and parameter tuning, considering the influence of various factors on the effectiveness of data protection at specific battery levels and specific types of cryptographic methodologies.

5.3. Risks due to limited computational power

Cryptographic protection algorithms, in general, are quite complex and resource-intensive regarding the computational resources of their technical platform [4]. Therefore, the insufficient computational power of IoT devices has several consequences for their security:

1. *Limited capacity for strong encryption application*. The incompatibility of the computational resources of the embedded device with the requirements of strong, computationally complex encryption algorithms creates a risk of resorting to weaker encryption methods. This limitation may compel the device to choose less resource-intensive computational methods, which, in turn, may have lower resistance to cyberattacks.
2. *Authentication failure due to resource constraints*. Computational limitations can diminish the suitability of an embedded device for implementing robust identity verification methods, such as biometric data or complex encryption algorithms, thereby increasing vulnerability to attacks. Additionally, the limited memory of embedded devices can complicate storing and managing authentication-related data, such as passwords, keys, or cyphers. This may lead to less secure methods for storing identification information or a reduction in the number of available authentication methods. Therefore, the challenge of implementing proper authentication in embedded devices is associated with the potential complexity of authentication algorithms and ensuring secure processes for storing and managing identity information. Moreover, the constraint on computational power may negatively impact the authentication process itself, resulting in the implementation of slower or less reliable authentication processes. The limited speed of the embedded device in processing authentication requests can make them less responsive to user requests in real-time or increase response times.

5.4. The risks arising from network bandwidth limitations

Network bandwidth capacity is a crucial aspect that impacts the security and efficiency of embedded IoT devices. Limited bandwidth can lead to several serious security risks. Let us delve deeper into these risks, including the mathematical models used for their analysis.

5.4.1. Network overload

A high traffic volume can overload the network, leading to data transmission delays or service denial (DoS attacks). Attackers may deliberately create excessive traffic to cause such overloads.

The use of Markov process models or queueing models, particularly the M/M/1 model, is proposed to analyse network overload.

In this model, the input packet stream is described by a Poisson distribution with a rate of (packets per second). At the same time, the service time follows an exponential distribution with a rate of (packets per second).

$$P_n = \left(1 - \frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)^n \tag{5}$$

where P_n is the probability of having n packets in the system. The probability of service denial (delay or packet loss) increases with the growth of $\frac{\lambda}{\mu}$. When $\lambda > \mu$, the system becomes unstable, leading to network overload.

5.4.2. Insufficient bandwidth

Due to limited bandwidth, securely transmitting large volumes of data is difficult, which may lead to the loss of important information or compromise. The $M/M/1/K$ queuing model is proposed to analyse insufficient bandwidth, where K is the maximum number of packets in the system.

In this model, the input packet stream is described by a Poisson distribution with a rate of λ, and the service time follows an exponential distribution with a rate of μ, with a limit on the number of packets in the system up to K.

$$P_{loss} = \frac{\left(\frac{\lambda}{\mu}\right)^K \left(1 - \frac{\lambda}{\mu}\right)}{1 - \left(\frac{\lambda}{\mu}\right)^{K+1}} \tag{6}$$

where P_{loss} is the packet loss probability due to insufficient bandwidth.

$$P_{success} = 1 - \frac{\left(\frac{\lambda}{\mu}\right)^K \left(1 - \frac{\lambda}{\mu}\right)}{1 - \left(\frac{\lambda}{\mu}\right)^{K+1}} \tag{7}$$

With a significant increase in P_{loss} (due to attacks or heavy traffic), the probability of successful transmission decreases exponentially, leading to substantial delays and data loss.

In summary, the discussed risks associated with network bandwidth are crucial for ensuring the security and efficiency of embedded IoT devices. Limited bandwidth can result in network overload, decreased ability to securely transmit data, susceptibility to availability attacks, and compromises between security and productivity. All listed risks must be considered to ensure the reliable operation of embedded IoT devices, and appropriate mathematical models should be used for their analysis and minimization.

6. Cryptographic models for risk analysis

In the context of security for embedded IoT devices, a key aspect is considering their resource constraints. These constraints directly impact the effectiveness of implementing security mechanisms and strategies. It is essential to realize that each type of constraint – memory, battery charge, or energy consumption – poses unique challenges and requires specific solutions [34]. As the analysis shows, memory, battery

Table 2
Impact of embedded device resource constraints on information security.

Type of constraint	Impact on information security
Memory limitation	Complicated storage and management of encryption keys. Limits resources available for access control and authentication.
Battery charge constraint	Creates the risk of unpredictable interruptions in the device's operation. Reduces cryptography efficiency due to low battery charge.
Limited power consumption	Leads to a transition to low-power mode, restricting the use of powerful encryption algorithms. Affects response speed to threats due to standby mode for energy conservation.

charge, and energy consumption constraints significantly influence the cryptographic protection of information in IoT devices (table 2).

Memory limitations often impact the device's ability to store encryption keys and other essential data, increasing the risk of unauthorized access and information leakage.

Meanwhile, battery charge limitations may lead to unforeseen disruptions in the device's operation, reducing its reliability and the effectiveness of protective mechanisms. Finally, limited energy consumption can restrict the application of resource-intensive protective algorithms, particularly in the field of cryptographic security.

Each aspect requires detailed consideration and analysis to ensure effective and adequate protection for embedded IoT devices.

6.1. Memory constraints

Memory constraints in IoT devices can pose a significant risk to data security. On the one hand, limited memory can complicate the storage of large amounts of data or complex software algorithms necessary for adequate cryptographic protection. On the other hand, insufficient memory can reduce the efficiency of key management, which is critically important for ensuring the security of communication processes. Memory limitations in IoT devices can lead to inadequate storage and management of encryption keys, increasing vulnerability to attacks.

The degree of impact of memory constraints on key storage, security management, and system vulnerabilities is illustrated in the diagram (figure 3). It is based on a conceptual analysis of memory constraints' impact on IoT devices' security. The percentages indicated on the diagram reflect widely accepted expert estimates in IoT cybersecurity based on their experience and analysis of current trends in IoT technology development. These data do not represent specific quantitative research but provide a general understanding of trends in the field.

6.2. Battery charge limitations

Battery charge limitations in IoT devices can cause disruptions in their operation, especially in critical situations. This may lead to a failure to perform essential security operations and unauthorized access to data. Additionally, a low battery charge can limit the effectiveness of encryption and other protective mechanisms. The limited battery life of IoT devices can result in unexpected shutdowns or reduced security functionality, increasing the risk of data leaks.

Let us define a function that relates the battery charge level to the runtime of security protocols. Let B be the initial battery charge level, and T be the duration of

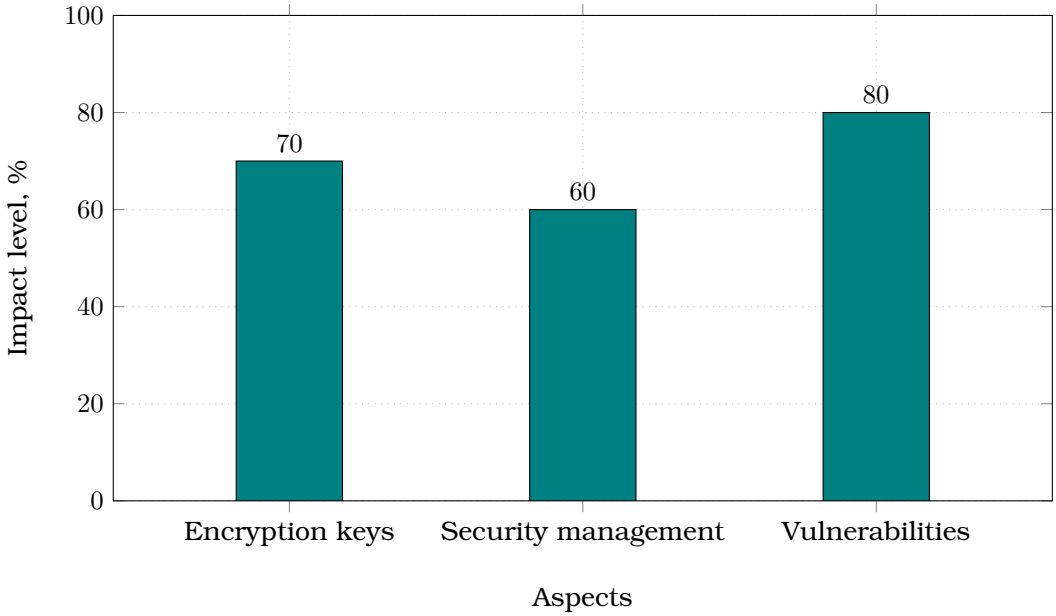

Figure 3: Impact of device memory constraints on its security.

security algorithm operation in hours. Then:

$$T = a \cdot \ln \ln B + b, \tag{8}$$

where a and b are constants based on the energy consumption characteristics of the device.

The diagram (figure 4) illustrates the impact of battery charge limitations on the activity of security protocols, the risk of data loss, and the constraints of protective mechanisms. This diagram is developed based on a qualitative analysis of the effects of battery charge limitations on IoT devices' security. The percentages on the diagram reflect estimated conclusions derived from theoretical considerations and expert opinions in this field, emphasizing the importance of considering energy aspects in developing protective strategies for IoT. The diagram shows that battery charge limitations have the most significant impact on the risk of data loss during interruptions in operation. This underscores the importance of developing energy-efficient solutions to ensure the reliability and continuity of security functions.

6.3. Limitations on energy consumption

Limitations on energy consumption in IoT devices can hinder the use of resource-intensive security algorithms, especially in cryptographic protection. This may lead to the selection of less powerful and, therefore, less secure encryption algorithms. Additionally, limited energy can slow detection and response to potential cyber threats. The difficulty of using complex cryptographic algorithms in IoT devices makes them vulnerable to advanced cyberattacks.

Let us model the efficiency of cryptographic algorithms about energy consumption. Let E represent the effectiveness of the applied algorithm's security properties, and P represent energy consumption. Then, the efficiency of cryptographic algorithms can be described by a polynomial function:

$$E = c_1 \cdot P^2 + c_2 \cdot P + c_3, \tag{9}$$

where c_1, c_2 and c_3 are coefficients determined based on the computational capabilities of the device.

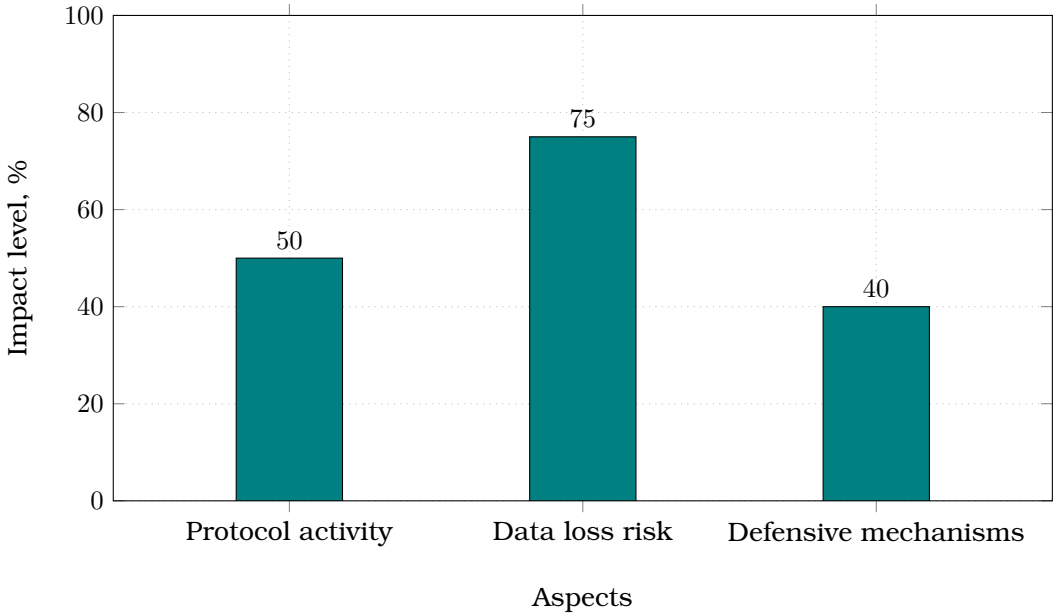

Figure 4: Impact of battery charge limitations on device security.

The figure 5 depicts the diagram of the impact of energy consumption constraints on the security of IoT devices. The data for this diagram were formulated based on expert discussions and an assessment of the potential consequences of limited energy consumption on the protective mechanisms of IoT devices. The percentage indicators reflect the generalized specialist opinion on the importance of this aspect in the context of the development and application of cryptographic security systems. The diagram shows that limited energy consumption most significantly affects the selection and effectiveness of secure algorithms. This emphasizes the need to develop energy-efficient cryptographic solutions with adequate security and constrained energy consumption.

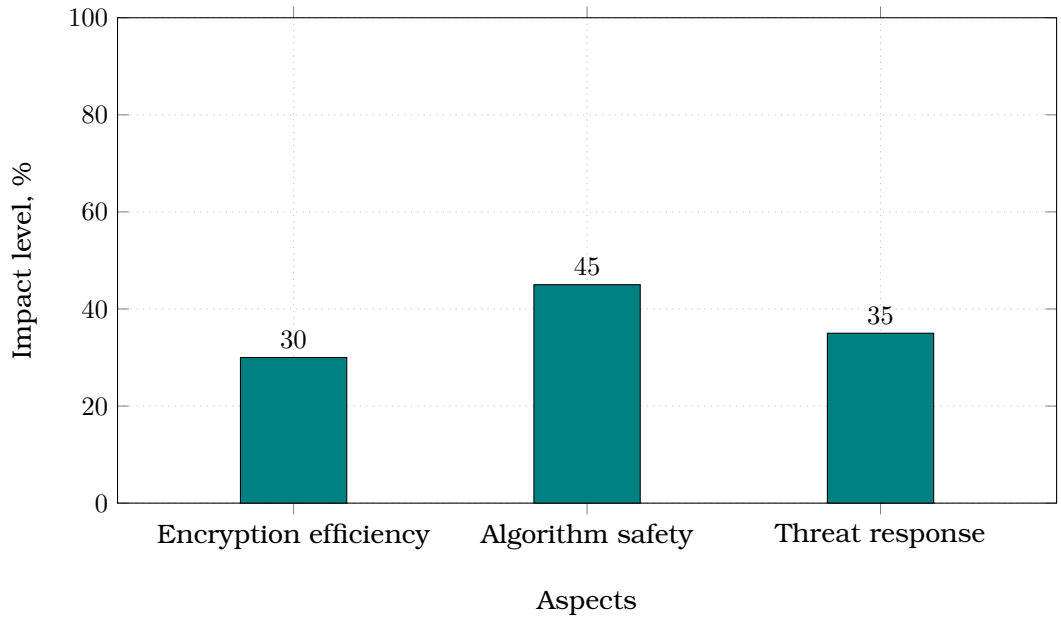

Figure 5: Impact of device energy consumption constraints on its security.

6.4. Bandwidth limitation

Network bandwidth limitation significantly impacts the security of embedded IoT devices. High traffic volume can overload the network, reducing the effectiveness of security protocols such as encryption and authentication. Data may not be transmitted promptly when the network is overloaded, opening opportunities for DoS attacks. Attackers can generate excessive traffic that overwhelms the network, making it unavailable to legitimate users.

Additionally, limited bandwidth can lead to data packet loss, especially during peak loads. Loss of critical data compromises the integrity and confidentiality of transmitted information, increasing the risk of unauthorized access or data manipulation. This also affects the effectiveness of security algorithms. Many, such as encryption and authentication, require stable and fast communication. Decreased bandwidth can reduce the efficiency of these algorithms, making the system more vulnerable to attacks.

Attackers can exploit limited bandwidth to launch DoS and DDoS (Distributed Denial of Service) attacks to block access to critical services or devices. This can seriously affect the operation of IoT systems, especially in critical applications such as medical devices or industrial control systems. Ensuring adequate bandwidth becomes evident when supporting the effective operation of security protocols and protection against potential cyber threats.

The impact of bandwidth limitation on various aspects of IoT device security is illustrated in the graph (figure 6). The percentage indicators reflect expert assessments of the importance of each element in the context of limited bandwidth. It illustrates the impact of bandwidth limitation on IoT device security, emphasizing the importance of considering this factor when developing security strategies for IoT systems.

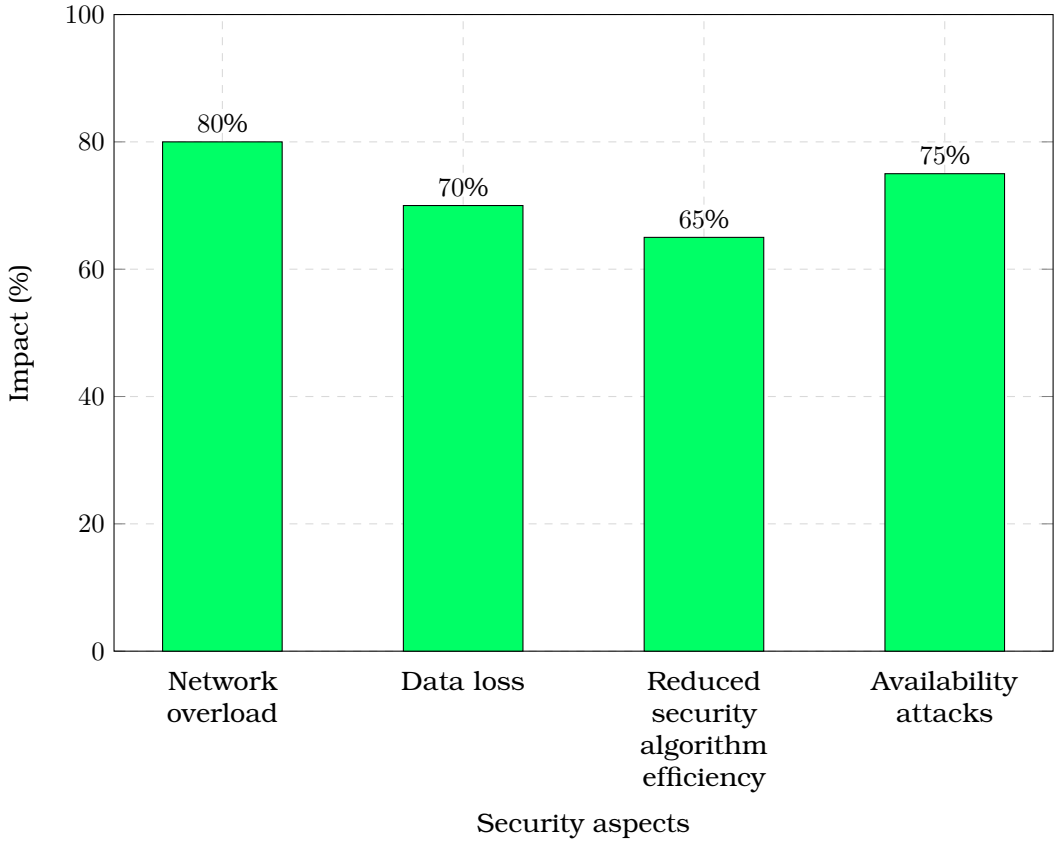

Figure 6: Impact of bandwidth limitation.

7. Strategies for optimizing security in IoT devices with limited resources

Optimizing IoT devices' limited resources becomes crucial for ensuring their security. This requires an innovative approach that considers both technical constraints and security needs. By focusing on key aspects of such limitations, such as memory, battery charge, and energy consumption, effective strategies can be developed to enhance the security level of IoT systems.

To evaluate the effectiveness of the proposed strategies for protecting resource-constrained IoT devices, quantitative metrics were used to measure reductions in energy consumption, memory savings, encryption execution speed, and authentication speed. The approaches, tools, and metrics applied for each indicator are described below, along with the results obtained.

7.1. Lightweight cryptographic algorithms

Emulators based on Arduino IDE and energy monitors such as the Power Profiler Kit II by Nordic Semiconductor were used to test lightweight cryptographic algorithms' energy efficiency and computational complexity. Test modules included lightweight crypto algorithms, such as SPECK and GIFT, adapted for computations on 8- and 16-bit microcontrollers like STM32F103 and ESP8266EX. Energy consumption metrics were determined by comparing these algorithms to baseline AES and RSA algorithms. Measurements demonstrated a 30% reduction in energy consumption compared to traditional cryptographic methods and a 40% decrease in computational complexity, as evidenced by the cyclic execution of test blocks.

7.2. Power management algorithms

The effectiveness of adaptive power-saving algorithms was evaluated using energy monitoring tools such as the INA219 for real-time power consumption monitoring. These algorithms dynamically adjusted energy usage depending on data processing intensity, reflected in the measured current consumption. Test results showed an average reduction in energy consumption of 25% and a 20% extension in device runtime, enabling sustained autonomous operation.

7.3. Memory usage optimization

Memory usage was assessed using the GNU Compiler Collection (GCC) with built-in memory analysis tools such as Valgrind and Memcheck, which tracked memory utilization during encryption operations. Optimizing cryptographic key storage methods resulted in a 35% reduction in memory requirements compared to baseline algorithms, allowing for more data to be stored without risking buffer overflows.

7.4. Adaptive security mechanisms

Adaptive security mechanisms were tested using the MATLAB Simulink simulation environment, which models changes in dynamic workload and resource constraints. Analysis revealed that adaptive algorithms reduce the computational load by 15% during low-demand periods, thereby decreasing peak energy consumption by 10%. This enables IoT devices to automatically adjust to changing conditions while maintaining the required level of security.

7.5. Authentication algorithms

Authentication speed was evaluated using the Crypto++ Library testing environment, which simulates computations on resource-constrained platforms. Lightweight authentication algorithms, such as HMAC-SHA1, demonstrated a 20% reduction in authentication time, improving overall system performance without compromising security. These measurements were performed under real-world device load conditions.

7.6. Optimized communication protocols

Communication protocols were assessed through simulations in the Network Simulator 3 (NS-3) environment, enabling performance analysis of network protocols under varying load conditions and limited bandwidth. A reduction in latency by 18% and improved data transmission stability confirmed the effectiveness of optimized protocols, which are critical for reliable operation in resource-constrained environments.

8. Discussion

In light of the conducted analysis, the need for further research on the security of resource-constrained IoT devices becomes evident, encompassing both technical and practical aspects. One of the key directions for future studies is developing and implementing optimized algorithms that consider the specific limitations of IoT devices, such as low computational power and limited memory. Advancing more efficient algorithms can significantly reduce device workloads without compromising security levels. This is particularly critical for devices operating in sensitive environments, such as medical and industrial systems [7, 13].

A promising avenue is the design of lightweight yet reliable cryptographic algorithms capable of providing high levels of security while utilizing minimal resources [27, 43]. Future research could focus on developing algorithms that optimize memory and energy usage while offering protection against emerging threats, such as quantum attacks or hardware-level attacks on device components.

Equally important is creating flexible and adaptive security systems that adjust to changing resource constraints and evolving threats [1]. This includes adaptive authentication and encryption protocols that automatically adjust security parameters based on current operational conditions [14]. Research in this area could aim to develop algorithms capable of dynamically modifying security levels and computational complexity according to the device's environment.

Special attention should be given to energy-efficient technologies, as energy is one of the most critical constraints for IoT devices [27, 43]. Enhancing device autonomy without increasing their size or cost can significantly improve the reliability of IoT systems in real-world conditions. Promising research areas include integrating energy-harvesting technologies from the surrounding environment and intelligent energy management systems, enabling devices to operate longer with minimal resource expenditure [14].

Additionally, future research could address interaction aspects between various IoT system components to improve their coherence while ensuring higher overall security and efficiency [16]. Considering resource constraints and security requirements, developing methods that optimize coordination between devices is crucial [3].

The application of generative AI in IoT security is an emerging field with significant potential. López Delgado and López Ramos [22] provide a comprehensive survey on generative AI solutions in IoT security, highlighting their ability to enhance automated threat detection and response. However, they also note challenges such as occasional inaccuracies, high training costs, and potential misuse by cybercriminals. Further research is needed to address these issues and fully harness the power of generative AI in IoT security [22].

Addressing the unique security challenges of resource-constrained IoT devices requires a multifaceted approach that integrates technical innovations, strategic planning, and consideration of real-world deployment scenarios [39, 49]. By focusing on key aspects such as lightweight cryptography, adaptive security mechanisms, energy efficiency, and component interaction optimization, future research can significantly enhance the security and reliability of IoT systems in the face of evolving threats and

resource limitations [42].

9. Conclusions

It is important to recognize that effective security requires a multidimensional approach to ensuring security for IoT devices with limited resources. This approach should integrate technical innovations and strategic planning. Considering the constraints in memory, power consumption, and computational power, developing lightweight cryptographic algorithms that utilize minimal resources becomes a priority to ensure reliable data protection.

Another crucial aspect is adapting security systems to the changing operational conditions of IoT devices. Security systems should be flexible, adaptive, and capable of maintaining a high level of security despite resource limitations. This includes technical aspects and operational resource management, especially energy and memory.

Innovations in authentication algorithms and energy-efficient technologies are essential for enhancing the autonomy and reliability of IoT devices. Further research should focus on developing solutions that efficiently operate under resource constraints while providing reliable protection against current and future cyber threats.

The emerging field of Generative AI offers significant potential for enhancing IoT security. As highlighted by López Delgado and López Ramos [22], Generative AI can improve automated threat detection and response capabilities. However, challenges such as inaccuracies, high training costs, and potential misuse must be addressed through further research to realize the benefits of Generative AI in IoT security fully.

Given the rapid advancement of technologies and the constant growth of cyber threats, continuous updating and adaptation of security mechanisms are integral parts of a security assurance strategy. Updating security solutions in response to new threats will help maintain high protection while expanding the possibilities of applying IoT technologies in various domains.

Author contributions: Conceptualization, Inna Rozlomii and Andrii Yarmilko; data curation, Inna Rozlomii; investigation, Inna Rozlomii, Andrii Yarmilko, Serhii Naumenko; writing – original draft: Inna Rozlomii, Andrii Yarmilko, Serhii Naumenko. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data availability statement: No new data were created or analysed during this study. Data sharing is not applicable.

Conflicts of interest: The authors declare no conflict of interest.

Declaration on generative AI: During the preparation of this work, the authors used ChatGPT-4o in order to draft content, generate a literature review, and improve writing style and content enhancement. Further, the authors used Grammarly in order to: grammar and spelling check. After using these tools, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Aboelmaged, M., Shisha, A. and Ghany, M.A.A.E., 2021. High-Performance Data Compression-Based Design for Dynamic IoT Security Systems. *Electronics*, 10(16), p.1989. Available from: https://doi.org/10.3390/electronics10161989.

[2] Afzal, B., Umair, M., Shah, G.A. and Ahmed, E., 2019. Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Generation Computer Systems*, 92, pp.718–731. Available from: https://doi.org/10.1016/j.future.2017.12.002.

[3] Ahmed, S.F., Islam, M.R., Nath, T.D., Ferdosi, B.J. and Hasan, A.S.M.T., 2019. G-TBSA: A Generalized Lightweight Security Algorithm for IoT. *2019 4th International Conference on Electrical Information and Communication Technology, EICT 2019*. Institute of Electrical and Electronics Engineers Inc. Available from: https://doi.org/10.1109/EICT48899.2019.9068848.

[4] Al-Sharekh, S.I. and Al-Shqeerat, K.H., 2019. Security Challenges and Limitations in IoT Environments. *IJCSNS International Journal of Computer Science and Network Security*, 19, pp.193–199. Available from: http://paper.ijcsns.org/07_book/201902/20190224.pdf.

[5] Ammar, M., Russello, G. and Crispo, B., 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, pp.8–27. Available from: https://doi.org/10.1016/j.jisa.2017.11.002.

[6] Balyk, N., Leshchuk, S. and Yatsenyak, D., 2023. Design and implementation of an IoT-based educational model for smart homes: a STEM approach. *Journal of Edge Computing*, 2, pp.148–162. Available from: https://doi.org/10.55056/jec.632.

[7] Bokhari, A.H., Inoue, Y., Kato, S., Yoshioka, K. and Matsumoto, T., 2021. Empirical Analysis of Security and Power-Saving Features of Port Knocking Technique Applied to an IoT Device. *Journal of Information Processing*, 29, pp.572–580. Available from: https://doi.org/10.2197/ipsjjip.29.572.

[8] Chanal, P.M. and Kakkasageri, M.S., 2020. Security and Privacy in IoT: A Survey. *Wireless Personal Communications*, 115, pp.1667–1693. Available from: https://doi.org/10.1007/s11277-020-07649-9.

[9] Chifor, B.C., Bica, I., Patriciu, V.V. and Pop, F., 2018. A security authorization scheme for smart home internet of things devices. *Future Generation Computer Systems*, 86, pp.740–749. Available from: https://doi.org/10.1016/j.future.2017.05.048.

[10] Davis, B.D., Mason, J.C. and Anwar, M., 2020. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, 7, pp.10102–10110. Available from: https://doi.org/10.1109/JIOT.2020.2983983.

[11] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P. and Bashir, A.K., 2022. A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, 33, p.e3935. Available from: https://doi.org/10.1002/ett.3935.

[12] Didi, Z. and El Azami, I., 2022. IoT, Comparative Study Between the Use of Arduino Uno, Esp32, and Raspberry Pi in Greenhouses. *Digital Technologies and Applications, ICDTA 2022*. Springer International Publishing, *Lecture Notes in Networks and Systems*, vol. 455, pp.718–726. Available from: https://doi.org/10.1007/978-3-031-02447-4_74.

[13] Ghazi Sami, T.M., Zeebaree, S.R.M. and Ahmed, S.H., 2024. Designing a New Hashing Algorithm for Enhancing IoT Devices Security and Energy Management. *International Journal of Intelligent Systems and Applications in Engineering*, 12(4s), pp.202–215. Available from: https://ijisae.org/index.php/IJISAE/article/view/3783.

[14] Gupta, P. and Chhabra, J., 2016. IoT based Smart Home design using power and security management. In: B. Kumar, P.K. Kapur, J.S. Jassi and G. Singh, eds. *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*. Institute of Electrical and Electronics Engineers Inc., pp.6–10. Available from: https://doi.org/10.1109/ICICCS.2016.7542317.

[15] Jabraeil Jamali, M.A., Bahrami, B., Heidari, A., Allahverdizadeh, P. and Norouzi, F., 2020. *IoT Architecture*. Springer International Publishing, pp.9–31. Available

from: https://doi.org/10.1007/978-3-030-18468-1_2.

[16] Jain, A., Singh, T. and Sharma, S.K., 2021. Security as a solution: An intrusion detection system using a neural network for IoT enabled healthcare ecosystem. *Interdisciplinary Journal of Information, Knowledge, and Management*, 16, pp.331–369. Available from: https://doi.org/10.28945/4838.

[17] Jiang, X., Lora, M. and Chattopadhyay, S., 2020. An experimental analysis of security vulnerabilities in industrial IoT devices. *ACM Transactions on Internet Technology*, 20, pp.1–24. Available from: https://doi.org/10.1145/3379542.

[18] Jony, A.I. and Arnob, A.K.B., 2024. A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset. *Journal of Edge Computing*, 3(1), pp.28–42. Available from: https://doi.org/10.55056/jec.648.

[19] Klochko, O.V., Fedorets, V.M., Mazur, M.V. and Liulko, Y.P., 2023. An IoT system based on open APIs and geolocation for human health data analysis. *CTE Workshop Proceedings*, 10, pp.399–413. Available from: https://doi.org/10.55056/cte.567.

[20] Korenivska, O.L., Benedytskyi, V.B., Andreiev, O.V. and Medvediev, M.G., 2023. A system for monitoring the microclimate parameters of premises based on the Internet of Things and edge devices. *Journal of edge computing*, 2(2), pp.125–147. Available from: https://doi.org/10.55056/jec.614.

[21] Lobanchykova, N.M., Pilkevych, I.A. and Korchenko, O., 2022. Analysis and protection of IoT systems: Edge computing and decentralized decision-making. *Journal of Edge Computing*, 1(1), pp.55–67. Available from: https://doi.org/10.55056/jec.573.

[22] López Delgado, J.L. and López Ramos, J.A., 2024. A Comprehensive Survey on Generative AI Solutions in IoT Security. *Electronics*, 13(24), p.4965. Available from: https://doi.org/10.3390/electronics13244965.

[23] Maitra, S. and Yelamarthi, K., 2019. Rapidly Deployable IoT Architecture with Data Security: Implementation and Experimental Evaluation. *Sensors*, 19, p.2484. Available from: https://doi.org/10.3390/s19112484.

[24] Marton, A., 2023. State of IoT – Spring 2023, Report by IoT Analytics, Safepay Systems. Available from: https://iotac.eu/state-of-iot-spring-2023-by-iot-analytics/.

[25] Marwedel, P., 2022. *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*. 4th ed. Springer. Available from: https://doi.org/10.1007/978-3-030-60910-8.

[26] Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A., 2019. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6, pp.8182–8201. Available from: https://doi.org/10.1109/JIOT.2019.2935189.

[27] Mohanty, S.N., Ramya, K.C., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S.K. and Khanna, A., 2020. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, 102, pp.1027–1037. Available from: https://doi.org/10.1016/j.future.2019.09.050.

[28] Nikitchuk, T.M., Vakaliuk, T.A., Chernysh, O.A., Korenivska, O.L., Martseva, L.A. and Osadchyi, V.V., 2022. Non-contact photoplethysmographic sensors for monitoring students' cardiovascular system functional state in an IoT system. *Journal of Edge Computing*, 1(1), pp.17–28. Available from: https://doi.org/10.55056/jec.570.

[29] Rachit, Bhatt, S. and Ragiri, P.R., 2021. Security trends in Internet of Things: A survey. *SN Applied Sciences*, 3, p.121. Available from: https://doi.org/10.1007/s42452-021-04156-9.

[30] Rajesh, S., Paul, V., Menon, V.G. and Khosravi, M.R., 2019. A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. *Symmetry*, 11, p.293. Available from: https://doi.org/10.3390/sym11020293.

[31] Rozlomii, I., Kosenyuk, H., Naumenko, S. and Mikhailovsky, P., 2023. Modeling a microcontroller-based sensor system in the game simulation "SmartHome" using data encryption. *Computer-Integrated technologies: education, science, production*, 53, pp.292–299. Available from: https://doi.org/10.36910/6775-2524-0560-2023-53-43.

[32] Rozlomii, I., Symonyuk, V., Naumenko, S. and Mykhailovskyi, P., 2024. A security model of interconnected computing devices based on a lightweight encryption scheme for IoT. *Computer-Integrated technologies: education, science, production*, 55, pp.191–198. Available from: https://doi.org/10.36910/6775-2524-0560-2024-55-24.

[33] Rozlomii, I., Yarmilko, A. and Naumenko, S., 2024. Data security of IoT devices with limited resources: challenges and potential solutions. In: T.A. Vakaliuk and S.O. Semerikov, eds. *Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine, April 5, 2024*. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3666, pp.85–96. Available from: https://ceur-ws.org/Vol-3666/paper13.pdf.

[34] Rozlomii, I., Yarmilko, A., Naumenko, S. and Mykhailovskyi, P., 2023. IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. In: N. Shakhovska, M. Kovác, I. Izonin and S. Chrétien, eds. *Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine, Bratislava, Slovakia, November 17-19, 2023*. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3609, pp.145–156. Available from: https://ceur-ws.org/Vol-3609/paper12.pdf.

[35] Rozlomii, I., Yarmilko, A., Naumenko, S. and Mykhailovskyi, P., 2024. Hardware encryptors and cryptographic libraries for optimizing security in IoT. In: A. Pakstas, Y.P. Kondratenko, V. Vychuzhanin, H. Yin and N. Rudnichenko, eds. *Proceedings of the 12th International Conference Information Control Systems & Technologies (ICST 2024), Odesa, Ukraine, September 23-25, 2024*. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3790, pp.99–109. Available from: https://ceur-ws.org/Vol-3790/paper09.pdf.

[36] Rozlomii, I.O., Simonyuk, V.P., Naumenko, S.V. and Mykhaylovskyi, P.V., 2024. Adaptive Cryptography for Energy-Efficient Security of IoT Devices. *Issues in Modeling and Design Automation*, 1(19), pp.77–83. Available from: https://pmap.donntu.edu.ua/sites/upload/articles/pmap_2024-no119end-78-84.pdf.

[37] Shammar, E.A. and Zahary, A.T., 2020. The Internet of Things (IoT): a survey of techniques, operating systems, and trends. *Library Hi Tech*, 38, pp.5–66. Available from: https://doi.org/10.1108/LHT-12-2018-0200.

[38] Shapovalov, Y.B., Bilyk, Z.I., Usenko, S.A., Shapovalov, V.B., Postova, K.H., Zhadan, S.O. and Antonenko, P.D., 2023. Harnessing personal smart tools for enhanced STEM education: exploring IoT integration. *Educational Technology Quarterly*, 2023(2), pp.210–232. Available from: https://doi.org/10.55056/etq.604.

[39] Shayer, K.S., Medul, M.H., Badoruzzaman, M., Islam Shuvo, J., Rabbu, M. and Mahmudul Haque, F.M., 2024. An Integrated Framework for Enhanced Learning Environments: IoT-Driven Smart Classrooms with Multi-Layered Security Protocols and Adaptive Infrastructure. *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems: Innovation for Sustainability, iCACCESS 2024*. Institute of Electrical and Electronics Engineers Inc.

Available from: https://doi.org/10.1109/iCACCESS61735.2024.10499605.

[40] Shen, S., Zhang, K., Zhou, Y. and Ci, S., 2020. Security in edge-assisted Internet of Things: challenges and solutions. *Science China Information Sciences*, 63, p.220302. Available from: https://doi.org/10.1007/s11432-019-2906-y.

[41] Sinha, S., 2024. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. Available from: https://iot-analytics.com/number-connected-iot-devices/.

[42] Sonoli, S. and Keerthi, C., 2023. IoT Based Lineman Security System Using Controlled Switchover With Transmission Line Fault Identification. *IEEE 1st International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics, AIKIIE 2023*. Institute of Electrical and Electronics Engineers Inc. Available from: https://doi.org/10.1109/AIKIIE60097.2023.10389864.

[43] Spina, M.G. and De Rango, F., 2023. Lightweight, Dynamic and Energy Efficient Security Mechanism for constrained IoT devices using CoAP. *Proceedings - IEEE Consumer Communications and Networking Conference, CCNC*. Institute of Electrical and Electronics Engineers Inc., vol. 2023-January, pp.1123–1128. Available from: https://doi.org/10.1109/CCNC51644.2023.10059854.

[44] Tiburski, R.T., Moratelli, C.R., Johann, S.F., Neves, M.V., Matos, E. de, Amaral, L.A. and Hessel, F., 2019. Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices. *IEEE Communications Magazine*, 57, pp.67–73. Available from: https://doi.org/10.1109/MCOM.2018.1701047.

[45] Yang, K., Blaauw, D. and Sylvester, D., 2017. Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey. *IEEE Micro*, 37, pp.72–89. Available from: https://doi.org/10.1109/MM.2017.4241357.

[46] Yar, H., Imran, A.S., Khan, Z.A., Sajjad, M. and Kastrati, Z., 2021. Towards smart home automation using IoT-enabled edge-computing paradigm. *Sensors*, 21(14), p.4932. Available from: https://doi.org/10.3390/s21144932.

[47] Yarmilko, A., Rozlomii, I. and Naumenko, S., 2024. Dependability of Embedded Systems in the Industrial Internet of Things: Information Security and Reliability of the Communication Cluster. *International Scientific-Practical Conference "Information Technology for Education, Science and Technics"*. Springer Nature Switzerland, Cham, pp.235–249. Available from: https://doi.org/10.1007/978-3-031-71804-5_16.

[48] Yu, M., Zhuge, J., Cao, M., Shi, Z. and Jiang, L., 2020. A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. *Future Internet*, 12(27). Available from: https://doi.org/10.3390/fi12020027.

[49] Zhydka, O., Riabyi, M., Fesenko, A., Kydyralina, L. and Okhrimenko, T., 2024. Research on data transmission technologies and information security in IoT networks. In: P. Zhezhnych, O. Markovets, A. Petrushka and S. Gnatyuk, eds. *Proceedings of the 3rd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA 2024), Lviv, Ukraine, October 31, 2024*. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3851. Available from: https://ceur-ws.org/Vol-3851/paper15.pdf.