Data security of IoT devices with limited resources: challenges and potential solutions

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

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

Abstract

Integration of the Internet of Things (IoT) into various application domains not only expands capabilities but also brings forth a multitude of challenges. These challenges revolve around the security of IoT devices, many of which are characterized by limited resources such as memory, power consumption, and computational power. This article examines key challenges associated with ensuring the security of IoT devices and proposes potential solutions and strategies adapted to resource constraints. Emphasis is placed on the development and analysis of lightweight cryptographic algorithms capable of providing robust data protection with minimal resource utilization. Strategies for efficient energy management and memory usage optimization are also discussed, critical for ensuring the stable and uninterrupted operation of IoT devices. The article highlights the necessity of developing adaptive security mechanisms that can effectively respond to dynamic operational conditions and resource constraints. The key importance of continuously updating security mechanisms to adapt to changing conditions and to guard against new and future cyber threats is underscored. In addition to technical aspects, the importance of strategic planning and innovation in IoT security is also illuminated. It is noted that further research and development should focus on creating integrated solutions that combine hardware, software, and managerial aspects to optimize overall efficiency and security of IoT systems. This article contributes to the understanding and resolution of security issues in IoT devices operating under resource constraints. It provides a broad overview of existing challenges and opportunities while suggesting directions for future research and development in this dynamically evolving field.

Keywords

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

1. Introduction

Embedded Internet of Things (IoT) devices are compact, integrated devices embedded in various objects capable of collecting, processing, and utilizing data, as well as exchanging it over a network without direct human involvement [1]. These devices provide automation and monitoring in various fields, from household systems to industrial processes, using their own computational resources to perform their functions [2, 3].

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 [4]. They have become an essential element in advancing technologies and the development of the connected world [5].

However, the security of embedded IoT devices has become a key issue limiting their application [6]. This problem arises from the imbalance between the potentially high functionality of such devices and their resource constraints [7]. 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 [8]. 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 [9, 10].

doors-2024: 4th Edge Computing Workshop, April 5, 2024, Zhytomyr, Ukraine

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)

Overcoming challenges related to the security of embedded IoT devices becomes a critical task in the context of their widespread integration into our everyday living spaces and industrial environments. The limited resources of these devices pose not only technical challenges but also serious potential consequences for user safety and infrastructure security. Failure to address the issue of limited resources and inadequate protection may lead to uncontrolled widespread access to confidential information, destruction of critical systems, or even the use of devices for malicious purposes.

The main security challenges of embedded IoT devices are associated with their inadequate protection and vulnerability to cyber attacks due to limited support for encryption and authentication, as well as insufficient capabilities for detecting and responding to potential threats. The aim of this research is to develop effective cryptographic protection strategies for embedded IoT devices with limited resources.

In the context of researching the security of embedded IoT devices, it is important to identify development perspectives aimed at ensuring their security and reliability. The development of effective cryptographic protection strategies is a key element of this process. Applying modern encryption and authentication methods will improve the reliability and accountability of embedded devices, providing a high level of protection in conditions of limited resources.

2. Related works

There are numerous studies dedicated to the security issues of embedded IoT devices with limited resources [11, 12]. 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 [13]. In these security studies, the importance of embedded IoT device security has garnered significant interest due to their crucial role in daily life, industry, and infrastructure. Many works highlight the fundamental challenge of mismatch between data protection needs and the limited resources of the devices [14].

Security of embedded IoT devices has been the subject of many works investigating vulnerability issues related to limited computational capabilities, restricted memory capacity, and limited power supply [15, 16]. These studies have demonstrated that resource constraints impact the effectiveness of cryptographic protection and authentication processes, making devices vulnerable to external threats.

A significant research theme has been cryptographic protection strategies with limited resources [17]. Previous research has shown the low efficiency of certain cryptographic methods and proposed the use of lightweight encryption and authentication methods that require fewer resources [18, 19]. However, some studies suggest that lightweight methods may have their own limitations and require a balance between efficiency and security [20]. Awareness of these aspects is crucial for developing optimal cryptographic protection strategies for embedded IoT devices with limited resources.

Further research should focus on effective methods to ensure the security of embedded IoT devices, considering resource constraints and the requirement for a high level of protection. Emphasizing efficient authentication and cryptographic mechanisms that take into account limited resources is identified as a key direction for future scientific research in this area.

3. Capabilities of embedded devices and their resource limitations

The architecture of embedded IoT devices is presented as the interaction of three main components [21]:

1. Sensors and actuators – components that provide data collection and transmission. Sensors gather information from the environment (temperature, humidity, etc.), while actuators perform corresponding actions (e.g., turning devices on/off).
2. Data processor is responsible for processing and analyzing the collected data. This can be a microcontroller or a specialized computing system.
3. Network interface facilitates communication with the external environment through various network protocols such as Wi-Fi, Bluetooth, LoRa, Zigbee, etc.

The primary functions of embedded IoT devices include [22]:

1. Data collection – obtaining information from sensors.
2. Data processing – analyzing and processing the acquired data to perform defined tasks.
3. Actuator control – sending signals to actuators to execute specific actions.

The typical properties of embedded IoT devices, which form the core spectrum of their functional and technical advantages, are accompanied by limitations related to deployment platforms and methods of ensuring autonomy. In general, these limitations encompass the following aspects [23]:

1. Computational power: Embedded IoT devices have limited capability for complex computations due to restricted computational power. This may lead to constraints in applying advanced encryption algorithms and performing 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 may result in a reduction of available resources for storing encryption keys, user data, and other critical elements, increasing vulnerability to attacks.
3. Power supply: mbedded IoT devices are often powered by autonomous energy 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 power off or enter a low-power mode, reducing its ability to detect and respond to potential threats.

These outlined limitations impact the capabilities of embedded devices in implementing robust security measures and pose a challenge in ensuring data reliability and 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 a crucial task as these devices are used in various life domains, ranging from household systems to critical infrastructure [15, 24, 25]. 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, the use of weak passwords, or simple authorization methods can be entry points for cyber-attacks. 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: The use of weak or outdated encryption algorithms in IoT devices makes data more vulnerable to interception and compromise. If encryption employs keys of insufficient length or is vulnerable to known attacks, there is a risk of compromising the confidentiality and integrity of data, as well as threats to their availability. To determine the effectiveness of encryption, the Shannon encryption model can be utilized:

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

   where C – the channel capacity, S – the signal power, N – 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.

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. Additionally, limited computational power complicates the application of robust encryption and authentication methods.

Examining memory, energy consumption, 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 the execution of malicious code in case of insufficient input data validation.

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 creates the possibility of embedding malicious code or executing code in vulnerable areas. The result is the emergence of vulnerabilities that can be exploited by attackers. Attacks leveraging these vulnerabilities may lead to system compromise, unauthorized code execution, or leakage of sensitive data.
2. As a result of 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 in the processes of storing and managing encryption keys, which are critical elements for ensuring data security. Typically, for system security, it is important to have diverse keys for various encryption tasks. However, due to limited memory, it may be challenging to provide the necessary volume of unique keys for data encryption.
3. Key management also becomes a challenge due to limited resources. For information security, keys need to 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 serve as a foundation for their compromise. If keys are not stored or managed properly, it can make them 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.

5.2. Risks arising from memory limitations

Energy consumption of an embedded system may be insufficient for the operation of cryptographic protection, both due to the design features of autonomous IoT module and 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. 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 normal operation. This can be problematic, especially for devices operating on batteries or in conditions of limited power supply. Continuous excessive energy consumption can lead to a decrease in device performance and efficiency, making it more vulnerable to various types of attacks or limiting security capabilities due to insufficient energy for the normal operation of protective mechanisms.
2. Interruptions in Operation. Limited charge in an autonomous energy source can cause unforeseen interruptions in the device's operation, creating serious security risks. When energy becomes limited, the device may abruptly shut down or transition into a low-power mode. Such interruptions in operation can lead to a decrease in 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 a minimal amount of 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 security of the system. 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. To ensure the security of IoT device data, encryption algorithms may be employed. However, in low energy consumption modes, their usage may be restricted, and less effective algorithms may be selected. This creates a risk of reducing the level of data protection, as the use of 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 be a factor in increasing the vulnerability of devices 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 lead to a reduction in 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 effectively implement complex encryption algorithms, resulting in increased data processing times or even a decrease in the level of protection. Such unstable operation of cryptographic methods can compromise the security of the device, 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. This is because, 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's 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's 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.

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	0.5·1+0.8·1=1.3	0.5·1+0.8·2=2.1
2	0.5·2+0.8·1=1.8	0.5·2+0.8·2=2.6
3	0.5·3+0.8·1=2.3	0.5·3+0.8·2=3.1
4	0.5·4+0.8·1=2.8	0.5·4+0.8·2=3.6
5	0.5·5+0.8·1=3.3	0.5·5+0.8·2=4.1
6	0.5·6+0.8·1=3.8	0.5·6+0.8·2=4.6
7	0.5·7+0.8·1=4.3	0.5·7+0.8·2=5.1
8	0.5·8+0.8·1=4.8	0.5·8+0.8·2=5.6
9	0.5·9+0.8·1=5.3	0.5·9+0.8·2=6.1
10	0.5·10+0.8·1=5.8	0.5·10+0.8·2=6.6

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.

Models (3), (4) can be supported and refined through experiments, data analysis, and parameter tuning, taking into account 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 in terms of the computational resources of their technical platform. Therefore, 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 the storage and management of authentication-related data, such as passwords, keys, or ciphers. This may lead to the use of 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 both 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. Overall, the rejection of robust authentication methods decreases the device's level of protection.

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 important to realize that each type of constraint – whether it's memory, battery charge, or energy consumption – poses unique challenges and requires specific solutions [26]. As the analysis shows, memory, battery charge, and energy consumption constraints significantly influence the cryptographic protection of information in IoT devices (table 2).

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

Type of constraint	Impact on information security
Memory limitation	Complicates 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.

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 of these aspects 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 one hand, limited memory can complicate the storage of large amounts of data or complex software algorithms necessary for effective 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 1). It is based on a conceptual analysis of the impact of memory constraints on these security aspects of IoT devices. The percentages indicated on the diagram reflect widely accepted expert estimates in the field of IoT cybersecurity, based on their experience and analysis of current trends in IoT technology development. These data do not represent specific quantitative research but rather provide a general understanding of trends in the field.

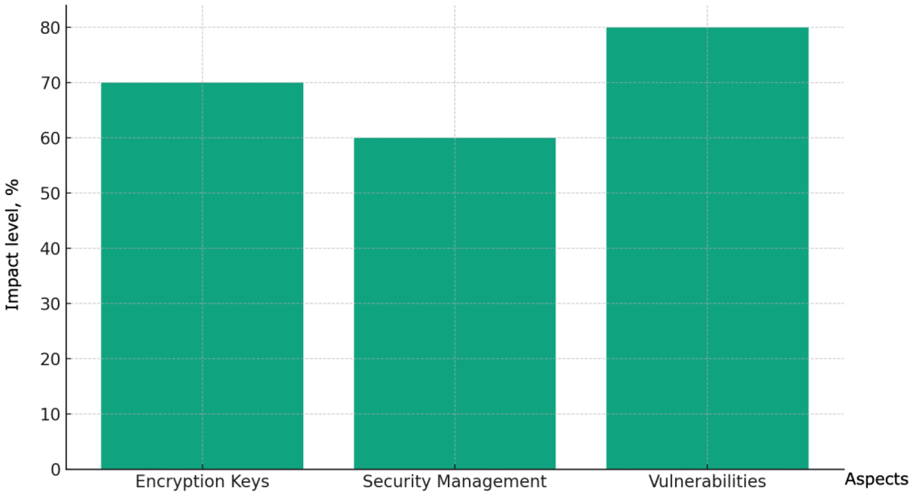

Figure 1: Impact of device memory constraints on its security.

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's 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 security algorithm operation in hours. Then:

$$T = a \cdot \ln ln(B) + b, \tag{5}$$

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

The diagram (figure 2) 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 that battery charge limitations may have on the security aspects of IoT devices. 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 the development of 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 be an obstacle to using resource-intensive security algorithms, especially in the field of cryptographic protection. This may lead to the selection of less powerful, and therefore less secure, encryption algorithms. Additionally, limited energy can

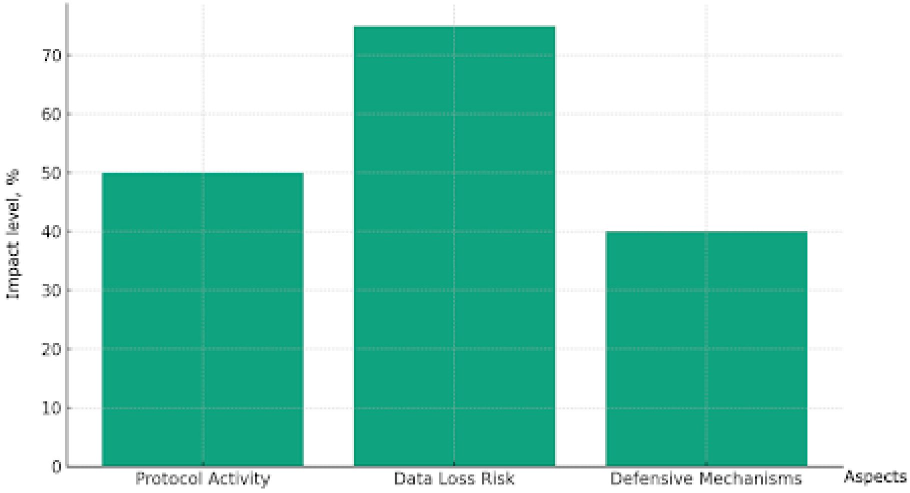

Figure 2: Impact of battery charge limitations on device security.

slow down the processes of detecting and responding to potential cyber threats. The difficulty of using complex cryptographic algorithms in IoT devices makes them vulnerable to advanced cyber-attacks.

Let's model the efficiency of cryptographic algorithms in relation to 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:

$$E = c_1 \cdot P^2 + c_2 \cdot P + c_3, \tag{6}$$

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

The figure 3 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 potential consequences of limited energy consumption on the protective mechanisms of IoT devices. The percentage indicators reflect the generalized expert 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 for the development of energy-efficient cryptographic solutions that can provide an adequate level of security with constrained energy consumption.

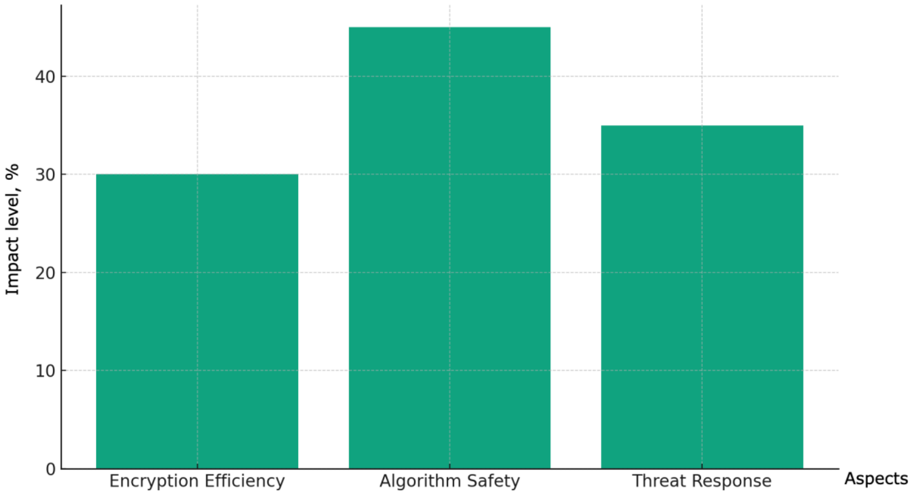

Figure 3: Impact of device energy consumption constraints on its security.

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

In the context of ensuring the security of IoT devices, optimizing their limited resources becomes crucial. This requires an innovative approach that takes into account 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.

1. Lightweight Cryptographic Algorithms: Development and use of cryptographic algorithms that require minimal resources for execution but still provide reliable data protection.
2. Efficient Energy Management Algorithms: Implementation of algorithms that optimize energy consumption without compromising security can ensure longer device runtime and security system reliability.
3. Memory Usage Optimization: Development of methods for efficient utilization of limited memory space, including compact storage of encryption keys and using memory for security functions.
4. Adaptive Security Mechanisms: Creation of security systems capable of adapting to changing resource constraints to maintain an optimal level of protection in different operating conditions.
5. Improvement of Authentication Algorithms: Implementation of effective authentication algorithms that provide a high level of security with limited computational resources.
6. Secure Communication Protocols: Development of specialized communication protocols for IoT that are optimized for efficient resource utilization and ensure reliable data protection.

These strategies form the foundation for ensuring the security of IoT devices operating in resource-constrained environments. They enable a balance between security needs and constraints in memory, energy consumption, and operational resources, providing effective protection against potential threats.

8. Discussion

In light of the presented analysis, it is crucial to delve deeper into the discussion of the perspectives for further research in the field of IoT security with constrained resources. One of the key directions is the development and implementation of more efficient algorithms that consider the specificity of IoT devices. This includes not only technical aspects but also taking into account the diversity of applications of IoT devices in various industries.

The need for improvement in cryptographic protection methods is evident, especially in the context of limited memory and computational resources. The development of lightweight yet robust cryptographic algorithms can be key to enhancing overall security. Additionally, there is a necessity to develop flexible and adaptive security systems capable of effectively operating under resource constraints and quickly adapting to new threats and challenges.

Significant potential lies in research on energy-efficient technologies for IoT devices. Energy is a critical resource for many IoT systems, so developing methods for efficient energy management can significantly increase the autonomy and reliability of devices. It is also essential to consider the interaction between different components of IoT systems to optimize overall efficiency and security.

9. Conclusions

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

Adapting security systems to the changing operational conditions of IoT devices is another crucial aspect. Security systems should be flexible, adaptive, and capable of maintaining a high level of security despite resource limitations. This includes not only technical aspects but also operational resource management, especially concerning energy and memory.

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

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 a high level of protection while expanding the possibilities of applying IoT technologies in various domains.

10. Authors contribution

The authors confirm contribution to the paper as follows: study conception and design: I. Rozlomii, A. Yarmilko; data collection: I. Rozlomii; analysis and interpretation of results: I. Rozlomii, A. Yarmilko, S. Naumenko; draft manuscript preparation: I. Rozlomii, A. Yarmilko, S. Naumenko. All authors reviewed the results and approved the final version of the manuscript.

References

[1] S. Maitra, K. Yelamarthi, Rapidly Deployable IoT Architecture with Data Security: Implementation and Experimental Evaluation, Sensors 19 (2019) 2484. doi:10.3390/s19112484.

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

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

[4] P. M. Chanal, M. S. Kakkasageri, Security and Privacy in IoT: A Survey, Wireless Personal Communications 115 (2020) 1667–1693. doi:10.1007/s11277-020-07649-9.

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

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

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

[8] K. Yang, D. Blaauw, D. Sylvester, Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey, IEEE Micro 37 (2017) 72–89. doi:10.1109/MM.2017.4241357.

[9] S. Shen, K. Zhang, Y. Zhou, S. Ci, Security in edge-assisted Internet of Things: challenges and solutions, Science China Information Sciences 63 (2020) 220302. doi:10.1007/s11432-019-2906-y.

[10] A. I. Jony, A. K. B. Arnob, A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset, Journal of Edge Computing (2024). doi:10.55056/jec.648.

[11] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices, IEEE Internet of Things Journal 6 (2019) 8182–8201. doi:10.1109/JIOT.2019.2935189.

[12] M. Ammar, G. Russello, B. Crispo, Internet of Things: A survey on the security of IoT frameworks, Journal of Information Security and Applications 38 (2018) 8–27. doi:10.1016/j.jisa.2017.11.002.

[13] X. Jiang, M. Lora, S. Chattopadhyay, An experimental analysis of security vulnerabilities in industrial IoT devices, ACM Transactions on Internet Technology 20 (2020) 1–24. doi:10.1145/3379542.

[14] Rachit, S. Bhatt, P. R. Ragiri, Security trends in Internet of Things: A survey, SN Applied Sciences 3 (2021) 121. doi:10.1007/s42452-021-04156-9.

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

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

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

[18] S. Rajesh, V. Paul, V. G. Menon, M. R. Khosravi, A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices, Symmetry 11 (2019) 293. doi:10.3390/sym11020293.

[19] B. C. Chifor, I. Bica, V. V. Patriciu, F. Pop, A security authorization scheme for smart home internet of things devices, Future Generation Computer Systems 86 (2018) 740–749. doi:10.1016/j.future.2017.05.048.

[20] M. Parmar, P. Shah, Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application, International Journal of Electrical and Computer Engineering (IJECE) 13 (2023) 4422–4431. doi:10.11591/ijece.v13i4.pp4422-4431.

[21] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, F. Norouzi, IoT Architecture, in: Towards the Internet of Things: Architectures, Security, and Applications, Springer International Publishing, Cham, 2020, pp. 9–31. doi:10.1007/978-3-030-18468-1_2.

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

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

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

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

[26] I. Rozlomii, A. Yarmilko, S. Naumenko, P. Mykhailovskyi, IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography, CEUR Workshop Proceedings 3609 (2023) 145–156. URL: https://ceur-ws.org/Vol-3609/paper12.pdf.