IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography

Inna Rozlomii[a], Andrii Yarmilko[a], Serhii Naumenko[a], and Pavlo Mykhailovskyi[a]

[a] *Bohdan Khmelnytsky National University of Cherkasy, 81, Shevchenko Blvd., Cherkasy, 18031, Ukraine*

Abstract

The article focuses on the important and timely issue of data security in medical IoT smart implants. With the proliferation of the Internet of Things in healthcare, new opportunities and challenges have arisen. Smart implants embedded in the human body for monitoring and treating various medical conditions are becoming increasingly common, but they also require enhanced information security measures. The article analyzes threats associated with smart implants that could potentially impact the confidentiality and integrity of patients' medical data. Aspects such as unauthorized access to implants, interception and alteration of data transmission, and the possibility of attacks on the implant's hardware are discussed. Considerable attention is given to the concept of lightweight cryptography and its application in the field of medical implants. Modern encryption and authentication methods can play a critical role in ensuring data security in IoT smart implants. The article explores the possibilities of applying cryptographic algorithms that are not only effective but also have low computational requirements, which is particularly important for embedded systems with limited resources. Additionally, the article discusses the implementation of lightweight cryptography in medical implants and provides practical recommendations for developers and manufacturers of smart implants on implementing cryptographic solutions to ensure information security.

Keywords 1

Smart implants, information security, cryptography, confidentiality, integrity, availability, security threats, lightweight cryptography, medical data, authentication, cybersecurity, health monitoring, digital signatures, hash functions, encryption, cryptographic key management, redundant hashing

1. Introduction

Over the past decade, medicine has witnessed significant advancements through the integration of cutting-edge technologies with the healthcare sector. One of the most innovative fields is the use of smart implants in Internet of Things (IoT) systems for monitoring, treatment, and enhancing patients' health [1, 2]. These implants, directly embedded in the human body, offer immense possibilities in the realm of medical diagnostics and therapy. However, they also bring forth new challenges regarding their secure usage, as they create a new reality in terms of information security within medical IoT systems [3, 4].

IoT Smart Implants are miniature medical devices equipped with sensors, actuators, and the ability to communicate via wireless networks. They can be employed for health tracking, treatment automation, and even internal surgical interventions. Smart implants fundamentally transform medical practice, providing healthcare professionals and patients with precise, real-time information about the body's condition.

IDDM'2023: 6th International Conference on Informatics & Data-Driven Medicine, November 17 - 19, 2023, Bratislava, Slovakia
EMAIL: inna-roz@ukr.net (Inna Rozlomii); a-ja@ukr.net (Andrii Yarmilko); naumenko.serhii1122@vu.cdu.edu.ua (Serhii Naumenko); mykhailovskyi.pavlo1123@vu.cdu.edu.ua (Pavlo Mykhailovskyi)
ORCID: 0000-0001-5065-9004 (Inna Rozlomii); 0000-0003-2062-2694 (Andrii Yarmilko); 0000-0002-6337-1605 (Serhii Naumenko); 0009-0008-4324-1724 (Pavlo Mykhailovskyi)

The adoption of IoT Smart Implants offers several significant advantages [5]. They enable real-time technology for health monitoring and maintenance, automate treatment processes, and provide unprecedented comfort to patients. Moreover, they allow patients to receive personalized medical care, continually monitor their health, and contribute to early disease detection. Healthcare providers, in turn, gain access to objective and structured information, aiding in more accurate diagnoses and the development of more effective treatment plans. From a medical perspective, smart implants open up new horizons in patient care and life-saving.

However, alongside these advantages, the implementation of IoT Smart Implants also poses substantial challenges in terms of information security [6, 7]. With increased interconnectivity and the exchange of medical information, information security becomes a key factor in preventing potential threats that could have serious consequences for patients [8]. Issues related to the confidentiality, integrity, and availability of medical data become highly relevant [9]. The information collected and exchanged between implants and medical systems must be securely protected against unauthorized access and abuse [10]. Numerous challenges also exist concerning the security of the implant itself during data exchange with other devices and systems [11]. In this context, one of the most critical tasks for this innovative direction is the development and implementation of reliable protection methods for IoT Smart Implants. Additionally, there is a demand for security methods that do not impose significant computational burdens on embedded systems with their inherent resource limitations [12].

Currently, the relevance of research into the information security of IoT smart implants is of paramount importance, as we are witnessing rapid developments in medical IoT technologies and a growing number of embedded medical devices exchanging confidential medical information [13]. As a result, the opportunity to improve the diagnosis and treatment of various diseases simultaneously creates new points of access for potential privacy and security threats to patients.

The purpose of this study is to address information security issues in medical IoT smart implants, including threat analysis, the development of secure solutions, and the provision of practical recommendations to ensure the confidentiality and integrity of medical data and devices. In this article, we explore lightweight cryptography methods that allow for the preservation of the confidentiality, integrity, and availability of medical data in modern medical applications. We also delve into crucial aspects of this problem and propose practical solutions to enhance the security of IoT Smart Implants in the medical field.

2. Related works

Ensuring information security in the context of IoT smart implants is an ongoing and highly relevant issue that has been extensively studied by researchers. Previous research has provided important insights into the threats and opportunities in this field. For example, works [14, 15] have conducted a general overview of security issues in implanted medical devices, including an analysis of potential threats to the confidentiality of medical data, system integrity, and device access.

One important research direction is access control to implanted medical devices [13]. This area involves the development of methods and systems that ensure only authorized access to the functionality and data of the implant. Research efforts also focus on the development of distributed data management systems within these systems to ensure secure and reliable transmission and storage of personal medical data [10, 12]. The security of wireless medical devices, including Smart Implants, is also of interest to researchers [6].

Research [16] offers a comprehensive review of security and privacy issues for embedded medical devices. The work examines potential threats that may arise during communication between implants and other medical devices and provides security recommendations.

The study in [17] concentrates on network and communication security issues for wireless embedded medical devices. Research includes an analysis of existing security protocols and the development of new methods to protect data from unauthorized access.

Article [18] focuses on the application of lightweight cryptography to ensure the security and confidentiality of data in medical implants. It proposes approaches to reduce computational overhead while maintaining a high level of security.

Authors in [19] propose a new secure wireless communication protocol for medical implants. They address authentication, confidentiality, and data integrity issues and provide methods to address them.

In [20], the issues of data protection and privacy during the transmission of information from medical implants to healthcare systems are discussed. The article offers solutions to ensure the confidentiality and integrity of patient data.

These reviewed studies constitute an important foundation for our work and provide valuable insights into the field of information security for medical IoT smart implants.

3. Research methodology

The methodology employed in this research is based on mathematical models for the analysis of information security in medical IoT smart implants and the development of protection strategies. The methodology includes the following key steps:

1. Formalization of the research object.

This stage involves formalizing the research object using mathematical models. The mathematical model describes the system comprising medical IoT smart implants and security measures. The model encompasses parameters such as data volumes, transmission speeds, the structure of implants, and security parameters like encryption keys and authentication.

2. Mathematical modeling of threats and vulnerabilities.

At this stage, mathematical modeling of potential threats and vulnerabilities of the system is conducted. The issues addressed during this stage include considering possible attack scenarios and assessing the impact of these threats on the security of medical data. Mathematical models help estimate the probability of threats occurring and determine their potential consequences.

3. Development of cryptographic models and algorithms.

The final stage involves the development of mathematical models and algorithms for cryptographic protection of medical IoT smart implants. These models include a mathematical description of encryption, authentication, and other cryptographic mechanisms used to ensure data confidentiality and integrity.

4. Formalization of the system of medical IoT smart implants

The applied mathematical model allows us to describe the medical IoT system and its information security measures. It enables us to mathematically abstract the real object of research and determine the key parameters that affect the security of this system.

Parameters of the mathematical model:

1. Data volume (D): This parameter defines the volume of medical data generated and transmitted between smart implants and medical systems. The expression can be as follows:

$$D = D_{in} + D_{out}$$

where D_{in} – is the volume of incoming data (e.g., biometric measurements), and D_{out} – is the volume of outgoing data (commands and instructions for implants).

2. Transmission speed (R): The data transmission rate between implants and medical systems. This parameter is measured in bits per second (bps).

3. Implant structure (I): Description of the structure of smart implants, including their architecture, functions, and dependencies between components.

4. Security parameters (S): Parameters responsible for system security, such as encryption keys (K), authentication methods (A), and other cryptographic parameters.

With the help of the above parameters, we can construct a mathematical model of the system that describes the relationships between them. For example, the transmission speed (R) can be related to data volume (D) and transmission time (t) in the following way:

$$R = \frac{D}{t}, \quad (1)$$

where t is determined by system parameters and data transmission algorithms.

The resulting mathematical model allows us to quantitatively assess and analyze various aspects of the security of medical IoT smart implants using formulas, equations, and tables. This approach helps

us systematize and objectively study the research object for further analysis of threats and the development of security measures.

5. Threats to the information security of smart implants

As previously mentioned, threats to the information security of smart implants pose a significant challenge in the context of modern medicine and the Internet of Things (IoT) [21, 22]. Since these intelligent medical devices are capable of collecting, processing, and transmitting medical data, their vulnerability to various threats can jeopardize not only the confidentiality of patient data but also the patients' own health. Some of the key threats to the information security of smart implants and possible consequences of their exploitation are presented in Table 1. Security measures, such as cryptographic protection and access control, are crucial to prevent these threats and ensure the reliability and safety of medical implants.

Table 1
Threats to the Information security of Smart implants and potential consequences of their implementation

Threat	Potential Consequences
Unauthorized data access	Leakage of confidential medical data
Viruses and malware	Damage or loss of implant functionality
Network connection attacks	Loss of communication with medical systems
Authentication and authorization attacks	Unauthorized alteration of implant parameters and control
Physical access to the implant	Damage or unauthorized control of the implant
Alteration of implant functionality	Loss of control over patient treatment

The next stage of the research involves mathematically modeling potential threats and vulnerabilities in the medical IoT smart implant system and assessing their impact on the security of medical data. Mathematical models, formulas, and tabular representations are used for this purpose, allowing for a systematic analysis of information threats and their consequences.

Probability-based approaches are used for modeling threats. Let $P(t)$ – be the probability of a specific threat T occurring. The mathematical model can include formulas that determine the probabilities of specific attacks or vulnerabilities. For example:

$$P(A) = \frac{N_A}{N}, \tag{2}$$

where N_A – is the number of attempts when attack A occurred, and N – is the total number of attempts.

To assess the consequences of attacks and vulnerabilities, mathematical models can be used to describe the loss of confidentiality, integrity, and data availability. For example, to assess the loss of confidentiality, you can use the following formula:

$$C_L = \frac{I_{before} - I_{after}}{I_{before}} \times 100\%, \tag{3}$$

where C_L – is the level of confidentiality loss, I_{before} – is the information before the attack, I_{after} – is the information after the attack.

Assessing the probabilities of threats and their impacts on security is an important stage in the analysis of the security of medical IoT smart implant systems. To do this, you can create a table that includes the probabilities of threats and their impact levels (Table 2).

In Table 2, for each threat, the probability of its occurrence (P) and the impact level on security (C) are determined. The probability can range from 0 to 1, where 0 is the minimum probability, and 1 is the maximum. The impact level can also take values from 0 to 1, where 0 represents minimal impact, and 1 represents maximum impact.

Table 2
Example of assessing the probability of threats and their consequences

Threats	Probability (P)	Impact Level (C)
Unauthorized access to implants	0.15	0.30
Loss of authentication data	0.10	0.25
Attack on cryptographic key	0.08	0.40
Loss of implant functionality	0.12	0.20

With the help of this table, you can calculate the overall risk for the system using the following formula:

$$Risk = \sum_{i=1}^{n} P_i \cdot C_i, \quad (4)$$

where P_i – is the probability of the *i*-th threat, C_i – is the impact level of the *i*-th threat, and n – is the number of threats.

The proposed method of formalization helps identify the most significant threats and directs attention to their management and protection.

Thus, mathematical modeling allows for a systematic analysis of potential threats and vulnerabilities in the system of medical IoT smart implants and provides an objective approach to assessing their impact on data security.

6. Mechanisms for ensuring information security of smart implants

Working directly inside the patient, Smart implants require the highest level of protection against threats and unauthorized access. Therefore, effective information security measures during their development and operation are critically important. Below are key security mechanisms and their implementations that ensure the security and confidentiality of medical data, as well as the reliability of the implant itself.

1. Cryptography: Used to protect against unauthorized access and ensure the confidentiality of medical data. Lightweight cryptographic algorithms, such as Elliptic Curve Cryptography (ECC), are used in implementation to reduce computational load on the implant.
2. Authentication Methods: Employed to verify the legitimacy of the implant and users. These methods may be based on biometric data, PIN codes, and digital signatures to confirm identity.
3. Access Control: Rules and restrictions on access to the implant's functionality are established to ensure security. This protection mechanism is implemented by assigning different levels of access for medical personnel and patients.
4. Physical Protection: Protective casings and biometric identifiers are used to prevent physical access to the implant.
5. Monitoring and Attack Detection: Reliable monitoring and anomaly detection systems track the implant's activity and respond to suspicious activity or attacks, allowing for swift responses to potential threats.

A mathematical model for securing the information of IoT Smart implants can be formulated based on the following principles.

Let:

D – be the set of medical data stored on Smart implants;

K – be the set of encryption and authentication keys used to protect data;

U – be the set of users who have access to Smart implants;

F – be the function that determines users' access rights to individual data elements;

P – be the set of potential information security threats, such as communication attacks, physical access, attacks on cryptographic methods, etc.

Then, the mathematical model can be represented as follows:

1. D (medical data) – it is the object of protection. For each element $d \in D$, there exists an encryption key $k_D \in K$, used to protect data d. Other keys may be used for authentication and authorization of data access.
2. U (users) – represented as entities who have access to data on Smart implants. Each user $u \in U$ has their own identifier and access rights determined by the function F. For example, $F(u,d)$ determines whether the user u has access to data d.
3. K (keys) – used for encryption, authentication, and authorization. The set of keys K includes encryption keys, authentication keys, and other keys for data protection.
4. P (potential threats) – this is the set of possible information security threats that may occur in the system. For each threat $p \in P$ there is a probability of its occurrence and consequences for security.

The model defines the interaction between data, users, keys, and potential threats. The mathematical model can be augmented with the following formula to assess the threat p for a specific user-data pair u and d:

$$R(u,d,p) = Probability\ of\ Threat\ Occurrence \times Severity\ of\ Consequences, \quad (5)$$

where $Probability\ of\ Threat\ Occurrence$ – is the likelihood that threat p may happen for a specific user u and data d, $Severity\ of\ Consequences$ – is a measure of how serious the consequences of the threat can be for security.

This formula allows for the evaluation of threats and assigning priorities for data protection on Smart implants.

6.1. Lightweight cryptography methods

To ensure the security and confidentiality of medical data, traditional cryptographic approaches can be used. However, classical cryptographic methods can be cumbersome to implement on embedded devices with limited resources, such as Smart implants. Therefore, lightweight cryptography methods become an interesting solution for ensuring the security and confidentiality of data in such systems.

The means of protecting Smart implants can be based on various technologies and methods.

1. Using lightweight encryption: Compared to complex encryption algorithms that require significant computational resources, lightweight cryptographic algorithms, such as lightweight block ciphers or stream ciphers, use fewer resources and can be more practical for Smart implants [28]. To secure information on IoT Smart implants, especially in conditions of limited computational resources, lightweight encryption algorithms are used. These algorithms provide a high level of confidentiality and allow for data protection against unauthorized access. In particular, the following cryptographic algorithms are used for encrypting data on IoT Smart implants:

- AES-CCM (Advanced Encryption Standard – Counter with CBC-MAC) is a combination of symmetric encryption (AES) and authentication (CCM) methods [28]. It allows for simultaneous encryption and authentication of data, ensuring their confidentiality and integrity. Each fixed-size block P, such as 128 bits, is encrypted using AES in Counter (CTR) mode with a key K and a sequential block number N. The result of encryption is the ciphertext block C. To ensure data integrity and authentication, Cipher Block Chaining Message Authentication Code (CBC-MAC) is used. CBC-MAC is computed over the ciphertext C using the same key K. The obtained code (MAC) is appended to the ciphertext. The resulting MAC and nonce N are also appended to the ciphertext C for further authentication and integrity verification. The encrypted data, along with the MAC and nonce, can be transmitted over a secure channel or stored on the IMD (Implantable Medical Device). The mathematical model of AES-CCM encryption includes several fundamental operations: addition (XOR), operations over Galois fields, AES-CTR encryption, and Message Authentication Code (MAC) computation. Decryption is performed by a set of analogous operations in reverse order
- ChaCha20-Poly1305 is a modern asymmetric stream cipher and password-based authentication method (AEAD) based on two primary operations. The first operation, ChaCha20, is a stream cipher used for encrypting and decrypting data. It relies on activation

and deactivation operations and provides high data processing speed. The ChaCha20 formula looks like this:

$$ChaCha20(key, nonce, counter, block) \rightarrow keystream.$$

The second operation, Poly1305, is an authentication function used to ensure data integrity and message authentication. It utilizes a key and a message to generate an authentication code (MAC), which is appended to the encrypted message. The Poly1305 formula looks like this:

$$Poly1305(key, message) \rightarrow MAC.$$

The combination of these two operations ensures the security and integrity of data transmitted over the network. The key advantage of the ChaCha20-Poly1305 encryption for medical IoT devices and implants is its efficiency and low computational resource requirements, allowing for reliable data protection on devices with limited capabilities.

- Serpent. This is a symmetric block cipher designed to provide a high level of security for data encryption. The Serpent algorithm is based on double substitution, permutation, and computations using large keys and data. Key operations in the Serpent algorithm involve a significant number of bitwise operations, such as XOR, AND, OR, and bit shifts. Although Serpent is considered a more complex block cipher, it can also be configured for use in IoT devices with limited resources. The Serpent algorithm is known for its high resistance to cryptographic attacks and high computational efficiency on devices with limited resources.
- Blowfish – it is a symmetric block cipher based on the Feistel network, which includes sequential rounds of permutation and data substitution operations [29]. It is flexible in terms of key and block size, making it practical for various applications, including IoT device security.
- ECC (Elliptic Curve Cryptography) is a modern cryptographic method used to ensure the confidentiality, integrity, and authentication of data in various areas of information security, including cryptocurrency systems, network and communication security, and other fields. ECC is based on mathematical structures known as elliptic curves. Elliptic curves are geometric objects defined by equations of the form $y^2 = x^3 + ax + b$, where a and b – are constants. These curves have some unique properties that make them useful for cryptography. The key advantages of ECC include a high level of security with short keys (compared to other cryptographic methods like RSA), computational efficiency, and the ability to work with limited resources, including smart implants.

Table 3 provides a comparison of the parameters of these mentioned ciphers. These algorithms can be configured to meet various needs in terms of data volume, resources, and security levels for specific IoT smart implants.

Table 3

Lightweight encryption algorithms

Algorithm	Type	Key Size	Security Level	Efficiency
AES-CCM	Block Cipher	28 bits	High	High
ChaCha20-Poly1305	Stream Cipher	256 bits	High	High
Serpent	Block Cipher	128, 192 or 256 bits	Very High	Medium
Blowfish	Block Cipher	32-448 bits	High	High
ECC	Elliptic Curve	256, 384 bits	Very High	High

For AES-CCM, the number of operations is relatively high because the algorithm includes additional authentication and data encryption operations. This results in a significant number of operations during data processing. The algorithm has medium complexity due to the need to perform a large number of operations required for data encryption and authentication. The number of operations for ChaCha20-Poly1305 is typically moderate, as this algorithm uses a stream cipher and some authentication operations. Lower complexity due to a smaller number of operations compared to other algorithms ensures faster data encryption. Serpent is known for its high number of operations because this algorithm uses more encryption rounds to provide a high level of security. High complexity due to a large number of operations required for each data block leads to significant encryption delays. Blowfish requires a moderate number of operations as it uses many

iterations for data encryption. It is characterized by moderate algorithm complexity because the total number of operations is not significant enough to significantly impact encryption speed. ECC requires a small number of operations because this algorithm is based on computing points on an elliptic curve. Thus, despite the high complexity in the field of mathematical computations, the overall number of operations is small, allowing for fast data encryption.

2. Use of lightweight authentication algorithms. To ensure communication security and data integrity, lightweight authentication algorithms such as HMAC (Hash-based Message Authentication Code) with efficient hash functions are employed.

3. Use of data anonymization methods. Simplified data anonymization methods are used to protect user privacy, ensuring data confidentiality even in cases where data is transmitted or processed in central systems.

4. Minimization of the key set. Managing a large number of cryptographic keys can be challenging on constrained devices. Using methods that allow bypassing the need for numerous keys simplifies the information security system.

5. Employment of group authentication methods. Group authentication methods are used to protect access to Smart implants, where multiple devices are authenticated as a single unit, streamlining the process and reducing computational costs.

6. Ensuring key protection. As in other systems, key security is critical to information security. Using methods to secure keys (such as hardware key storage) is an essential part of lightweight cryptography.

6.2. Error correction codes

In addition to data and communication security, the ability of the system to correct errors in the transmission and processing of information is extremely important. The primary goal of using error correction codes in medical implanted devices is to ensure the integrity and accuracy of the transmission of medical data and information. In the field of medicine, this is particularly important, as the accuracy and reliability of data can impact patients' lives.

To ensure reliable and corrected data transmission in IoT Smart implants, Hamming, Reed-Solomon, Reed-Muller, and turbo codes are recommended for use.

Hamming codes are a type of error correction codes that can detect and correct single-bit errors in transmitted data. They are especially useful in situations where a low signal level or losses can cause errors in transmission. Thanks to Hamming codes, an implant can correct an error before it causes serious problems. Hamming code can be represented as D – for input data and R – for control bits. Then DR will look like $(d_1, d_2, \dots, d_k, r_1, r_2, \dots, r_m)$, where m – is the number of additional bits added for error correction.

Reed-Solomon codes are more complex error correction codes capable of detecting and correcting multiple errors in data transmission. They are typically used in situations where very high transmission reliability is crucial, including medical implants. For Reed-Solomon codes with parameters n and k, the input data D is represented as a vector $(d_1, d_2, \dots, d_k)$, and the codeword C will have the form $(d_1, d_2, \dots, d_k, c_1, c_2, \dots, c_{n-k})$, where each c_i s calculated using Reed-Solomon polynomials.

Reed-Muller codes are codes based on Boolean function theory and are used to correct errors in multidimensional data. They provide a high level of error correction and error detection and can be useful in situations where medical implants transmit complex information. Reed-Muller codes are represented as matrix operations, where the input data D is multiplied by the matrix corresponding to the codeword C. The resulting value of C is the sum of these multiplications, including modulo addition operators.

Turbo codes are one of the most efficient error correction codes and are typically used in high-speed and reliable data transmission systems. Turbo codes are represented as iterative decoding processes that use previous results to improve error correction. This includes using input data, results from previous iterations, and turbo code decoding algorithms to enhance data transmission accuracy.

The mentioned error correction codes can significantly enhance the reliability of information exchange in IoT Smart implants, allowing for error detection and correction during data transmission. Users can have confidence that their data remains intact and inaccessible to unauthorized access.

In some cases, it may be effective to use a combination of Hamming and Reed-Solomon codes. For example, initially using Hamming codes to detect and correct single-bit errors and then Reed-Solomon codes to protect against more complex errors.

Therefore, error correction codes, such as Hamming and Reed-Solomon codes, are reliable tools for ensuring data integrity and protecting IoT Smart implants from transmission errors. Using them in combination can provide the highest level of reliability and information security in such a system.

Additionally, to detect intrusions or unauthorized changes in an IoT smart implant system, the use of redundant hashing methods is proposed. This method is built on the principles of Hamming codes and is based on creating linear hash code systems. To control and ensure the integrity of a message, it needs to be represented as a set of fixed-length blocks. These blocks are interpreted as a sequence of data blocks, to which control (additional) blocks are added as needed to protect the data's integrity. The addition of control blocks is performed according to the construction rules of redundant codes, depending on the required error correction properties of the resulting code.

This redundant hashing method based on Hamming codes is an important tool for detecting and preventing intrusions and attacks on IoT smart implant systems. It helps ensure a high level of information security and reliability in such systems.

7. Conclusions

In the article, the main threats to information security associated with the use of smart implants in medicine are analyzed. This issue is constantly growing due to both the general technical complexity of the systems and components used in modern medical practice and the potential deliberate actions to seize or alter medical data. Therefore, further progress in this field should take into account the latest trends in cybersecurity and continuously improve security measures for smart implants to address new threats.

With the growth of IoT in the healthcare sector, research and development of methods for integrating smart implants into the overall IoT network become crucial. Practical steps in this direction involve standardizing protocols and developing access control systems that ensure security at the network level. Further research may not only involve the application of existing cryptographic methods but also actively focus on creating new algorithms and approaches specifically adapted to the unique requirements of medical smart implants. This includes the development of cryptographic solutions that not only effectively protect patient data from unauthorized access but also have low computational requirements. Special attention should be given to optimizing the encryption and authentication processes in embedded systems with limited resources, which are characteristic of smart implants.

These studies can be directed towards the development of not only practical technical solutions but also the creation of standards and recommendations for smart implant manufacturers regarding the mandatory use of cryptographic protection methods and the integration of these solutions into medical practice. Such a comprehensive approach will contribute to ensuring maximum information security for patients using medical smart implants.

The use of lightweight cryptography in IoT smart implant systems can help ensure a high level of security and confidentiality of medical data without imposing unnecessary burdens on embedded devices with limited resources. The potential of these methods allows for securing information and the functionality of smart implants, which is essential for the successful implementation of these technologies in medical practice.

However, it is important to note that the selection of specific lightweight cryptography methods and their integration into the system should be the subject of careful analysis and risk assessment. Each smart implant may have unique security requirements, and a solution that is suitable for one device may be incompatible with another. Therefore, it is necessary to consider the specific characteristics of each case and use appropriate protection methods to achieve the highest level of information security in medical IoT smart implants. During the implementation of lightweight

cryptography in smart implants, a thorough analysis of threats and risk assessment that could impact the security of medical data and implant functionality is necessary. This analysis helps identify optimal cryptographic solutions and protection methods that align with specific needs and operational conditions.

So, the implementation of lightweight cryptography in medical IoT smart implants is a complex but necessary task to ensure the security and confidentiality of medical data. It requires a combination of technical expertise, risk analysis, and an individual approach to each device. This research is limited in scope, analyzing only certain aspects of information security and cryptography directly related to IoT smart implants. This means that there are additional aspects and opportunities in the field of cryptographic protection that fall beyond its boundaries. Further research may include an expanded analysis of other aspects of cryptography and consideration of a wider range of scenarios for the use of IoT smart implants to enhance overall security and efficiency of these systems.

In summary, the contribution of this article to the field of cryptography and information security in the context of IoT smart implants is seen in the clear identification of key challenges related to data security, as well as the analysis of possible ways to implement lightweight cryptography. The research aims to formulate specific recommendations for enhancing the security and information protection in IoT smart implant systems and will contribute to the development of new data protection strategies in the Internet of Things field, improving the security of these systems in the future.

8. References

[1] R. Somasundaram, M. Thirugnanam, Review of security challenges in healthcare internet of things, Wireless Networks 27 (2021) 5503-5509.

[2] J. Sametinger, J. Rozenblit, R. Lysecky, P. Ott, Security challenges for medical devices, Communications of the ACM 58(4) (2015) 74-82.

[3] K. Katzis, R. W. Jones, G. Despotou, The challenges of balancing safety and security in implantable medical devices, in: Unifying the Applications and Foundations of Biomedical and Health Informatics, IOS Press, 2016, pp. 25-28.

[4] A. Tabasum, Z. Safi, W. AlKhater, A. Shikfa, Cybersecurity issues in implanted medical devices, in: 2018 International Conference on Computer and Applications (ICCA), IEEE, 2018, pp. 1-9.

[5] C. Brito, L. Pinto, V. Marinho, S. Paiva, P. Pinto, A review on recent advances in implanted medical devices security, in: 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2021, pp. 1-6.

[6] L. Pycroft, T. Z. Aziz, Security of implantable medical devices with wireless connections: The dangers of cyber-attacks, Expert Review of Medical Devices 15(6) (2018) 403-406.

[7] Z. E. Ankaralı, A. F. Demir, M. Qaraqe, Q. H. Abbasi, E. Serpedin, H. Arslan, R. D. Gitlin, Physical layer security for wireless implantable medical devices, in: 2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), IEEE, 2015, pp. 144-147.

[8] Y. Isler, L. T. Olcuoglu, M. Yeniad, Data security and privacy issues of implantable medical devices, Natural and Engineering Sciences 3(3) (2018) 12-22.

[9] T. Yaqoob, H. Abbas, M. Atiquzzaman, Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review, IEEE Communications Surveys & Tutorials 21(4) (2019) 3723-3768.

[10] L. Wu, X. Du, M. Guizani, A. Mohamed, Access control schemes for implantable medical devices: A survey, IEEE Internet of Things Journal 4(5) (2017) 1272-1283.

[11] T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga, H. Marquering, Solutions for mitigating Cybersecurity risks caused by legacy software in medical devices: a scoping review, IEEE Access 8 (2020) 84352-84361.

[12] K. H. Han, W. S. Bae, Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices, Cluster Computing 19 (2016) 2335-2341.

[13] Y. Yang, X. Zheng, C. Tang, Lightweight distributed secure data management system for health internet of things, Journal of Network and Computer Applications 89 (2017) 26-37.

[14] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, A review of security challenges, attacks and resolutions for wireless medical devices, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 1495-1501.
[15] V. Hassija, V. Chamola, B. C. Bajpai, S. Zeadally, Security issues in implantable medical devices: Fact or fiction?, Sustainable Cities and Society 66 (2021) 102552.
[16] C. Camara, P. Peris-Lopez, J. E. Tapiador, Security and privacy issues in implantable medical devices: A comprehensive survey, Journal of biomedical informatics 55 (2015) 272-289.
[17] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, K. Saleem, Ideas and challenges for securing wireless implantable medical devices: A review, IEEE Sensors Journal 17(3) (2016) 562-576.
[18] A. Sivasangari, A. Ananthi, D. Deepa, G. Rajesh, X. M. Raajini, Security and privacy in wireless body sensor networks using lightweight cryptography scheme, in: Security and privacy issues in IoT devices and sensor networks, Academic Press, 2021, pp. 43-59.
[19] S. Challa, M. Wazid, A. K. Das, M. K. Khan, Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions, IEEE Consumer Electronics Magazine 7(1) (2017) 57-65.
[20] N. Garg, M. S. Obaidat, M. Wazid, A. K. Das, D. P. Singh, Spcs-ioteh: Secure privacy-preserving communication scheme for iot-enabled e-health applications, in: ICC 2021-IEEE International Conference on Communications, IEEE, 2021, pp. 1-6.
[21] H. Mrabet, S. Belguith, A. Alhomoud, A. Jemai, A survey of IoT security based on a layered architecture of sensing and data analysis, Sensors 20(13) (2020) 3625.
[22] D. Zaldivar, A. T. Lo'Ai, F. Muheidat, Investigating the security threats on networked medical devices, in: 2020 10th annual computing and communication workshop and conference (CCWC), IEEE, 2020, pp. 0488-0493.
[23] C. Camara, P. Peris-Lopez, J. M. De Fuentes, S. Marchal, Access control for implantable medical devices, IEEE Transactions on Emerging Topics in Computing 9(3) (2020) 1126-1138.
[24] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, Encryption for implantable medical devices using modified one-time pads, IEEE Access 3 (2015) 825-836.
[25] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M. A. Orgun, S. C. Mukhopadhyay, Finger-to-heart (F2H): Authentication for wireless implantable medical devices, IEEE journal of biomedical and health informatics 23(4) (2018) 1546-1557.
[26] S. Kulaç, M. H. Sazli, H. G. Ilk, External relaying based security solutions for wireless implantable medical devices: A review, in: 2018 11th IFIP wireless and mobile networking conference (WMNC), IEEE, 2018, pp. 1-4.
[27] L. Wu, J. Du, Designing novel proxy-based access control scheme for implantable medical devices, Computer Standards & Interfaces 87 (2024) 103754.
[28] T. Belkhouja, A. Mohamed, A. K. Al-Ali, X. Du, M. Guizani, Light-weight encryption of wireless communication for implantable medical devices using henon chaotic system, in: 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, 2017, pp. 1-6.
[29] T. Belkhouja, X. Du, A. Mohamed, A. K. Al-Ali, M. Guizani, Symmetric encryption relying on chaotic henon system for secure hardware-friendly wireless communication of implantable medical systems, Journal of Sensor and Actuator Networks 7(2) (2018) 21.
[30] S. Sarkar, J. Jiang, W. H. Ki, C. Y. Tsui, A 16-bit Encrypted On-chip Embedded System for Implantable Medical Devices, in: 2022 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2022, pp. 195-199.
[31] S. Suhail, R. Hussain, A. Khan, C. S. Hong, On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions, IEEE Internet of Things Journal 8(1) (2020) 1-17.
[32] J. Sivakumar, S. Nayak, A. N. Doss, IoT: Effective Authentication System (EAS) using Hash based Encryption on RFID Attacks, International Journal of Engineering and Management Research 10 (2020).
[33] S. Kumari, M. Singh, R. Singh, H. Tewari, Signature based Merkle Hash Multiplication algorithm to secure the communication in IoT devices, Knowledge-Based Systems 253 (2022) 109543.

[34] A. Yarmilko, I. Rozlomii, H. Kosenyuk, Hash method for information stream's safety in dynamic cooperative production system, in: S. Shkarlet et al. (Eds): Mathematical Modeling and Simulation of Systems, volume 344 of Lecture Notes in Networks and Systems, Springer, Cham, 2022, pp. 173-183. doi.org/10.1007/978-3-030-89902-8_14.