An In-Depth Analysis of Security Flaws in Advanced Authentication Protocols for the Internet of Medical Things

Haewon Byeon
Department of Future Technology, Korea University of Technology and Education (KOREA TECH), Cheonan 31253, South Korea

***Abstract*—This study evaluates a four-factor authentication protocol designed for IoT healthcare systems, identifying several key vulnerabilities that could compromise its security. The analysis highlights risks associated with node cloning, insider threats, biometric data security, session management, and scalability. To address these vulnerabilities, the study proposes a series of enhancements, including the implementation of Physical Unclonable Functions (PUFs) to prevent node cloning and the use of advanced encryption techniques, such as homomorphic encryption, to protect biometric data. Additionally, the adoption of role-based access control (RBAC) and attribute-based access control (ABAC) systems can mitigate insider threats by limiting user permissions. Optimizing session management through strict expiration and key rotation policies can maintain session integrity, while lightweight cryptographic algorithms and adaptive power management techniques enhance scalability and resource utilization. Future research directions include exploring quantum-resistant cryptographic algorithms and developing adaptive security policies leveraging artificial intelligence. These efforts are essential for maintaining the protocol's resilience against evolving threats and ensuring the secure operation of IoT-based healthcare systems.**

***Keywords*—Four-factor authentication; IoT Healthcare security; physical unclonable functions; quantum-resistant cryptography; biometric data protection**

I. Introduction

The Internet of Medical Things (IoMT) represents a significant advancement in the convergence of healthcare and technology. By interconnecting medical devices and healthcare systems through the internet, IoMT enables real-time monitoring, diagnosis, and treatment, ultimately improving patient outcomes and operational efficiency (Fig. 1). These technologies facilitate continuous patient monitoring and provide healthcare professionals with timely data, reducing the need for frequent hospital visits and enabling early intervention in critical situations [1].

As IoMT becomes more integrated into healthcare infrastructures, the security and privacy of sensitive medical data have emerged as paramount concerns. The data generated and transmitted by IoMT devices is highly sensitive, often containing personal health information that, if compromised, could lead to severe consequences for both patients and healthcare providers [2]. This necessitates robust security measures to protect against unauthorized access, data breaches, and cyber threats.

Authentication protocols play a critical role in securing IoMT systems by ensuring that only authorized users and devices can access sensitive data. Traditional authentication methods, typically based on single or dual-factor systems, have proven inadequate in the face of sophisticated cyber-attacks [3]. As a result, there is a growing need for more advanced authentication protocols that can provide comprehensive security in IoMT environments.

The development of four-factor authentication protocols presents a promising solution to these challenges [4]. By incorporating multiple authentication factors—such as knowledge-based (passwords), possession-based (smart cards), inherence-based (biometric data), and contextual (location or device-specific attributes)—these protocols offer enhanced security by requiring multiple forms of verification [5]. This layered approach significantly reduces the risk of unauthorized access, as an attacker would need to compromise all four factors to gain entry.

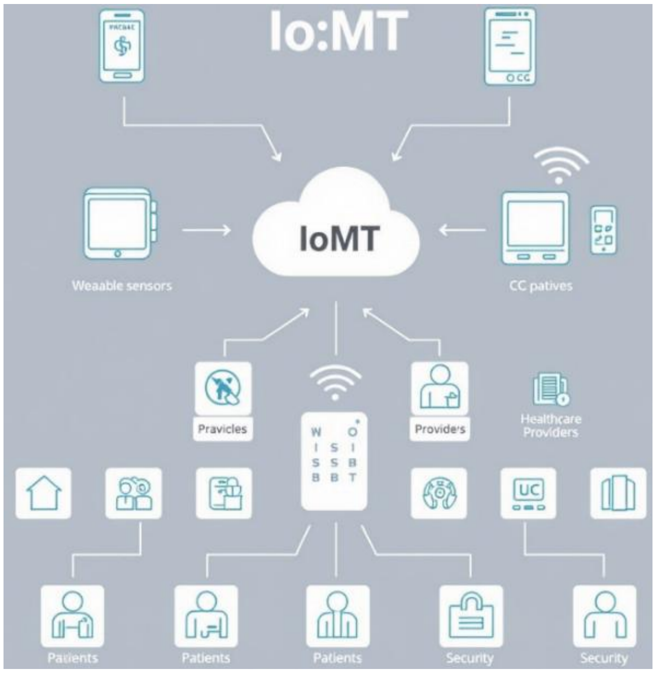

Fig. 1. The concept of Internet of Medical Things (IoMT).

Despite their potential, implementing four-factor authentication protocols in IoMT systems presents several challenges. The resource-constrained nature of many IoMT devices limits their ability to execute complex cryptographic operations, necessitating the development of efficient, lightweight protocols. Additionally, the dynamic nature of healthcare environments requires authentication systems to be adaptable, maintaining security even as devices frequently join and leave the network. Furthermore, ensuring compliance with stringent healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), is critical for maintaining patient trust and protecting healthcare providers from legal liabilities.

This research aims to conduct a comprehensive analysis of a proposed four-factor authentication protocol designed for IoMT [5]. The primary objective is to identify and scrutinize five key security vulnerabilities within the protocol that could compromise its effectiveness. By examining the protocol's architecture and operational phases, this study seeks to uncover potential weaknesses and propose strategies for enhancement.

The paper is structured as follows: Section I presents a literature review of existing authentication protocols and their limitations. Section II outlines the methodology employed for vulnerability detection, including the analytical methods and tools used for cryptanalysis and security testing. Section III discusses the identified vulnerabilities in detail, while Section IV proposes improvements to enhance the protocol's security and efficiency. Finally, Section V and VI concludes with a summary of the findings and their implications for IoMT authentication systems. Through this investigation, the study aims to contribute to the development of more secure and efficient authentication protocols that effectively protect sensitive medical data while supporting the continued integration of IoMT in healthcare.

A. Literature Review

1) Existing authentication protocols: The proliferation of the Internet of Things (IoT) in healthcare has necessitated the development of robust authentication protocols to secure sensitive medical data. Traditional single-factor and two-factor authentication methods have proven inadequate against sophisticated cyber threats, prompting the exploration of more comprehensive solutions [6]. In response, four-factor authentication protocols have emerged, integrating multiple layers of security to mitigate unauthorized access and data breaches [7].

Four-factor authentication protocols typically combine knowledge-based factors (e.g., passwords), possession-based factors (e.g., smart cards), inherence-based factors (e.g., biometric data), and contextual or environmental factors (e.g., device location or usage patterns) [8]. This multi-layered approach significantly enhances security by requiring multiple forms of verification, thereby reducing the likelihood of successful attacks. For instance, even if an attacker obtains a user’s password, they would still need to overcome other authentication barriers to gain access [9].

Recent advancements in authentication technologies have focused on optimizing these protocols for resource-constrained IoT environments. Lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC) and lightweight encryption standards, have been employed to balance security and efficiency [10]. These algorithms provide strong encryption with reduced computational overhead, making them suitable for IoT devices with limited processing power and energy resources.

Despite their strengths, existing four-factor authentication protocols face several challenges. The integration of multiple authentication factors can lead to increased complexity and user friction, potentially impacting usability and compliance [11]. Additionally, the dynamic nature of healthcare environments, where devices frequently join and leave the network, requires authentication systems to be adaptive and resilient [12]. Ensuring user privacy and compliance with stringent healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), remains a critical consideration.

2) Related works: Recent studies [13, 14] have highlighted various security vulnerabilities within IoT-based healthcare authentication systems. One major concern is the risk of sensor node capture attacks, where adversaries physically access devices to extract sensitive information [13]. To address this, researchers have proposed the use of Physical Unclonable Functions (PUFs) as an additional layer of security [14]. PUFs leverage the intrinsic physical variations of semiconductor devices to generate unique identifiers, making them resistant to cloning and physical attacks.

Another significant vulnerability is the potential for replay attacks, where attackers intercept and retransmit valid authentication messages to deceive the system [15]. To mitigate this risk, protocols have incorporated time-stamping and nonce-based mechanisms to ensure message freshness and authenticity [16]. These measures help prevent attackers from reusing captured messages to gain unauthorized access.

Previous studies [17, 18] also underscores the importance of protecting biometric data, which, once compromised, cannot be easily replaced or revoked [17]. Advanced encryption techniques and secure transmission protocols have been proposed to safeguard biometric information against interception and misuse [18].

Interoperability and scalability are additional challenges that must be addressed to ensure seamless integration and operation of IoT healthcare systems [19]. The diverse range of IoT devices and platforms necessitates standardized protocols that can facilitate communication and data exchange across different systems.

In summary, the literature emphasizes the need for continued research and innovation in the development of secure, efficient, and user-friendly authentication protocols for IoT healthcare systems. By addressing the identified vulnerabilities and challenges, the healthcare industry can enhance the security and privacy of patient data, ultimately improving trust and outcomes in digital healthcare environments.

II. Methodology

A. Framework for Analysis

The methodology for analyzing the proposed four-factor authentication protocol for the IoMT [5] involves a comprehensive framework designed to identify and evaluate potential security vulnerabilities. This framework integrates theoretical analysis, mathematical modeling, and practical testing to ensure a thorough security assessment.

B. Analytical Methods for Vulnerability Detection

The initial phase of analysis involves a detailed examination of the protocol's architecture, focusing on its critical components: initialization, mutual authentication, session key establishment, and data protection. Formal security models and logical proofs are employed to assess the protocol's resilience against various attack vectors. One such method is the application of Burrows-Abadi-Needham (BAN) logic, which helps verify the authenticity and freshness of messages exchanged within the protocol:

$$P \mid\equiv X \quad \text{(P believes X)}$$

$$P \mid\Rightarrow X \quad \text{(P has jurisdiction over X)}$$

$$(X) \quad \text{(X is fresh)}$$

These logical expressions formalize the assumptions made during the protocol's execution, ensuring that it meets its intended security objectives.

C. Cryptanalysis and Security Testing Tools

For cryptanalysis, the study utilizes advanced tools such as the Automated Validation of Internet Security Protocols and Applications (AVISPA). AVISPA provides a platform for modeling the protocol's interactions and simulating potential attacks, including replay, man-in-the-middle, and impersonation attacks. The tool employs a high-level protocol specification language (HLPSL) to evaluate the protocol's security properties.

In addition, the Random Oracle Model (ROM) is used to ensure the integrity of cryptographic functions, particularly for verifying hash-based operations and ensuring collision resistance. This involves modeling cryptographic hash functions as random oracles to simulate their ideal behavior:

$$H(m) = RO(m)$$

where $H(m)$ represents the hash of message (*m*), and (RO) denotes the random oracle.

D. Mathematical Modeling of Protocol Operations

The analysis incorporates mathematical modeling to evaluate key cryptographic operations, such as key generation and exchange. The protocol employs elliptic curve cryptography (ECC) for secure key exchanges:

$$K_{session} = g^{ab} p$$

where (g) is a generator point, and (*a*) and (*b*) are private keys of the communicating entities. This session key ensures secure communication between devices.

E. Analysis of the Proposed Protocol

The proposed four-factor authentication protocol for IoT healthcare systems [5] is designed to provide robust security through a multi-layered authentication process, incorporating initialization, mutual authentication, session key establishment, and data protection phases.

III. Overview of the Protocol

A. Initialization Phase

The protocol begins with the initialization phase, where cryptographic parameters are established. Each device generates a unique identifier and a corresponding key pair using elliptic curve cryptography (ECC). The public key is calculated as:

$$K_{public} = g^{k_{private}} p$$

where (g) is the generator point on the elliptic curve, $(k_{private})$ is the private key, and (p) is a prime modulus. This setup ensures that each device has a secure cryptographic foundation for subsequent operations.

B. Mutual Authentication Phase

During this phase, devices authenticate each other using a combination of ECC and hash functions. Each device computes an authentication token by hashing its identity and a session-specific random nonce:

$$AuthToken = h(ID \parallel Nonce)$$

where *h( )* is a secure hash function. This token verifies the device's authenticity, ensuring that only legitimate devices can participate in the network.

C. Session Key Establishment

Once mutual authentication is successful, a secure session key is established between the device and the server. The session key is derived from the ECC-based key exchange process:

$$K_{session} = g^{ab} p$$

where (a) and (b) are private keys of the communicating entities. This ensures that each session is secured with a unique key, providing confidentiality and integrity for data exchanged between the device and the server.

D. Data Protection Phase

The final phase involves securing data transmission using the established session key. Messages are encrypted as follows:

$$C = E_{K_{session}}(M)$$

where (C) is the ciphertext and (M) is the plaintext message. This encryption ensures that sensitive medical data remains confidential and protected from unauthorized access.

E. Identified Vulnerabilities

Vulnerability to Node Impersonation using Session Key Leakage

1) Problem: While the paper emphasizes mutual authentication, it inadvertently provides a vector for node impersonation. An adversary can intercept public messages and compute the session key.

a) The paper states that the gateway computes session key $sks = (sk \oplus N3) \oplus R3$, which implies a dependency of the sensor's session key on the gateway's variables and exposes a way to derive it. Note that the doctor also derives the key as $sk * = (sk* \oplus N2) \oplus PWD$.

b) The adversary can intercept M and derive R to compute the session key using sk which has been used by gateway to produce sks.

2) Impact: The adversary can impersonate legitimate nodes, leading to unauthorized access, data manipulation, or disruption of medical services.

3) Mathematical formulation: The paper states that the doctor will calculate session key sk as $sk * = (sk* \oplus N^2) \oplus PWD$. If we take another perspective of generating session key, the gateway calculates the sensor node session key $sks = (sk \oplus N) \oplus R$, where sk is the session key, N is a random number and R is another derived random number. But since the attacker has eavesdropped and learned G' which has been generated as $G = RG (RSNRG) + N$, which will help the attacker to compute R= and the session key sks by guessing the password.

4) Improvement: Session keys must be computed with a hash operation using all participating entities secrets, a key agreement approach must be followed to make it secure for each party. Also, public key cryptography can be considered to enhance security for all involved entities.

F. Password Vulnerability (Re-used Random Numbers)

1) Problem: The paper states that HPWD = h(PWDR). If an attacker gets the value HPWD for a user then, it is possible to guess the password using a brute force method. The paper doesn't specify a different process of updating the password, which means there is a chance that the random values used with the password remain constant, leading to the possibility that HPWD value of the user remains static. As a result, it becomes vulnerable to attacks such as dictionary or brute force password guessing.

2) Mathematical formulation: Since random number R, remains the same during each authentication process, if the attacker compromises HPWD and knows R, he can use brute force attack to guess PWD. For example, when an attacker tries all password values from his/her dictionary list and computes the resultant HPWD value from $HPWD = h(PWD \| R)$, when they have achieved the matching value, the password of the user is compromised.

3) Impact: A compromised password leads to full control over the user account and the ability to compromise the system.

4) Improvement: Each user has to generate a new random number with each new session. A password update process must be added and made mandatory to change the password periodically. This ensures that the password is not leaked and remains fresh. Multi-factor authentication can also help to prevent password leakage attacks.

G. Susceptibility to Impersonation and Data Modification Attacks

1) Problem: The protocol, as written, is susceptible to impersonation and data modification attacks since, all information such as temporary keys and identities are exchanged over a public channel, and those values can be used by an attacker to impersonate. An attacker can intercept and use public messages to act as legitimate users or devices.

2) Mathematical formulation: The protocol does not use Message Authentication Codes (MAC) or digital signatures. Suppose the sensor node receives a message {G, DTID,GW, Gw, and SKs }, and the user receives $\{\mu,\eta,sku,GW\}$. The attacker can intercept any of these messages, and they can either replay, drop, or modify them and, since message integrity is not protected, the recipient has no way to identify it.

3) Impact: An adversary can intercept and replay, drop, or modify messages. This can lead to several types of attacks.

a) An attacker can act as a gateway and can obtain the data, and can then, modify or drop the information.

b) An attacker can manipulate the information received by the user device and the sensor node device.

4) Improvement: Adding MACs or digital signatures to each message transmitted or received can ensure integrity. Moreover, an additional time stamp or nonce can also be used to verify the freshness of the messages.

H. Lack of Proper Revocation Mechanism

1) Problem: While the paper mentions a revocation phase, it doesn't specify how devices are removed or deactivated when compromised, nor how the data or secret keys associated with these nodes are handled. The removal process lacks proper security and can be exploited by adversaries if they have compromised a valid user. Also, the addition of new nodes can be attacked if an intruder starts acting as a legitimate user or a sensor node. This leaves the system vulnerable to a situation where compromised nodes can persist.

2) Impact: The lack of proper revocation can compromise the integrity and reliability of the whole system. Once a node is compromised, it should not be able to perform future operations or compromise the network. If proper revocation methods are not implemented, an attacker can easily compromise the whole system.

3) Improvement: A well-defined, secure, and well-implemented revocation mechanism is essential for managing compromised nodes. The security mechanism must delete/remove all previous keys and credentials from the network and the node. The new node added to the system should have different identities, credentials and keys, different from the compromised one.

This paper presented an approach towards secure authentication in the medical IoT field. The proposed protocol has potential to provide a secure environment and is more lightweight compared to existing solutions. However, the vulnerabilities mentioned above can be exploited by an adversary and can lead to severe security breaches. Addressing these flaws by implementing stronger cryptographic practices, adding proper message integrity checks, and better key management practices is necessary for ensuring real-world security for medical devices.

4) Proposed improvements: To enhance the security and performance of the proposed four-factor authentication protocol for IoT healthcare systems, several improvements are recommended. These enhancements aim to address the identified vulnerabilities and ensure robust protection against unauthorized access and data breaches.

IV. Security Enhancements

A. Node Cloning/Replication Prevention

To mitigate the risk of node cloning attacks, the protocol should incorporate mechanisms for device attestation and verification. This could involve using Physical Unclonable Functions (PUFs) to generate unique, hardware-based identifiers for each device. PUFs leverage the inherent physical variations of semiconductor devices to create unclonable identifiers, providing a strong defense against node replication attacks. Additionally, implementing regular device health checks and network monitoring can help detect and respond to unauthorized node activity.

B. Strengthening Insider Attack Defenses

To protect against insider threats, the protocol should enhance its access control measures by implementing role-based access control (RBAC) and attribute-based access control (ABAC) systems. These systems limit user permissions based on their roles and attributes, ensuring that users can only access the resources necessary for their duties. Furthermore, incorporating user behavior analytics and anomaly detection can help identify suspicious activities and potential insider threats, enabling timely intervention.

C. Biometric Data Security

Enhancing the security of biometric data involves implementing advanced encryption techniques and secure transmission protocols. Homomorphic encryption allows computations to be performed on encrypted data without revealing the data itself, providing strong protection for biometric information. Additionally, secure multi-party computation (SMPC) can enable collaborative data processing while preserving privacy. These techniques ensure that biometric data remains confidential and protected against interception during transmission and storage.

D. Improving Session Management

To prevent unauthorized access and maintain session integrity, the protocol should implement strict session expiration and key rotation policies. Session keys should be refreshed regularly, and sessions should automatically expire after a predetermined period of inactivity. This approach reduces the risk of session hijacking and ensures that only active, authenticated sessions are maintained. Furthermore, incorporating ephemeral key exchanges can provide additional security by ensuring that session keys are unique and short-lived.

E. Optimizing Scalability and Resource Utilization

Addressing scalability and resource constraints requires optimizing cryptographic operations to reduce computational overhead. Implementing lightweight cryptographic algorithms, such as the Advanced Encryption Standard (AES) in its lightweight form, can significantly decrease energy consumption and processing time. Additionally, employing adaptive power management techniques, such as duty cycling and dynamic voltage scaling, can extend battery life and maintain device performance. These optimizations ensure that IoT devices can efficiently perform necessary tasks without draining resources.

V. Future Research Directions

A. Exploring Quantum-Resistant Cryptography

As quantum computing capabilities advance, exploring quantum-resistant cryptographic algorithms will be essential to future-proof the protocol against potential quantum threats. Algorithms such as lattice-based cryptography and hash-based signatures could offer security that withstands quantum attacks, ensuring long-term protection of sensitive data.

B. Developing Adaptive Security Policies

Leveraging artificial intelligence and machine learning to develop adaptive security policies could provide real-time threat detection and response. By analyzing network traffic patterns and user behavior, AI-driven systems can dynamically adjust security measures, offering a proactive approach to maintaining security.

C. Enhancing Privacy-Preserving Technologies

Further exploration of privacy-preserving techniques, such as differential privacy and secure enclave technologies, will enhance user privacy and data protection. These techniques can ensure that sensitive information remains confidential, even in the face of sophisticated attacks.

D. Addressing Interoperability Challenges

Research into standardized protocols and cross-platform communication frameworks could facilitate seamless integration and operation of diverse IoT healthcare systems. Ensuring interoperability across different devices and platforms is essential for creating a cohesive and efficient IoT ecosystem.

By implementing these proposed improvements and pursuing ongoing research directions, the protocol can provide robust protection against evolving threats and maintain the integrity and confidentiality of IoT-based healthcare systems. These efforts offer a comprehensive approach to addressing current vulnerabilities and preparing for future security challenges in the digital healthcare landscape.

VI. Conclusion

In conclusion, the analysis of the proposed four-factor authentication protocol for IoT healthcare systems has identified several critical vulnerabilities, including node cloning risks, insider threats, biometric data security concerns, session management weaknesses, and scalability challenges. By implementing the recommended security enhancements, such as the use of Physical Unclonable Functions, advanced encryption techniques, and optimized session management, the protocol can significantly improve its security posture. These measures ensure robust protection of sensitive medical data, fostering trust in IoT-enabled healthcare environments. As the IoT landscape continues to evolve, ongoing research into quantum-resistant cryptography and adaptive security measures will be crucial in maintaining the protocol's resilience against emerging threats.

ACKNOWLEDGMENT

This research through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF- RS-2023 00237287).

REFERENCES

[1] Monteiro, A. C. B., França, R. P., Arthur, R., and Iano, Y. An overview of the internet of medical things (IoMT): Applications, benefits, and challenges. Security and Privacy Issues in Internet of Medical Things, pp. 83-98, 2023.

[2] Hireche, R., Mansouri, H., and Pathan, A. S. K. Security and privacy management in Internet of Medical Things (IoMT): A synthesis. Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 640-661, 2022.

[3] Khatiwada, P., and Yang, B. An overview on security and privacy of data in IoMT devices: performance metrics, merits, demerits, and challenges. pHealth 2022, pp. 126-136, 2022.

[4] Singh, A. K., and Garg, A. Authentication protocols for securing IoMT: current state and technological advancements. Securing Next-Generation Connected Healthcare Systems, pp. 1-29, 2024.

[5] Khajehzadeh, L., Barati, H., and Barati, A. A lightweight authentication and authorization method in IoT-based medical care. Multimedia Tools and Applications, pp. 1-40, 2024.

[6] Suleski, T., and Ahmed, M. A data taxonomy for adaptive multifactor authentication in the internet of health care things. Journal of Medical Internet Research, vol. 25, p. e44114, 2023.

[7] Rangwani, D., and Om, H. Four-factor mutual authentication scheme for health-care based on wireless body area network. The Journal of Supercomputing, vol. 78, no. 4, pp. 5744-5778, 2022.

[8] Aburbeian, A. M., and Fernández-Veiga, M. Secure Internet Financial Transactions: A framework integrating multi-factor authentication and Machine Learning. AI, vol. 5, no. 1, pp. 177-194, 2024.

[9] Awadh, W. A., Alasady, A. S., and Hashim, M. S. A multilayer model to enhance data security in cloud computing. Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 2, pp. 1105-1114, 2023.

[10] Thakor, V. A., Razzaque, M. A., and Khandaker, M. R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, vol. 9, pp. 28177-28193, 2021.

[11] Rangwani, D., and Om, H. A robust four-factor authentication protocol for resource mining. Arabian Journal for Science and Engineering, vol. 48, no. 2, pp. 1947-1971, 2023.

[12] Sodhro, A. H., Awad, A. I., van de Beek, J., and Nikolakopoulos, G. Intelligent authentication of 5G healthcare devices: A survey. Internet of Things, vol. 20, p. 100610, 2022.

[13] Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N. Z., Yassine, A., and Hossain, M. S. An intelligent healthcare system using IoT in wireless sensor network. Sensors, vol. 23, no. 11, p. 5055, 2023.

[14] Al-Meer, A., and Al-Kuwari, S. Physical unclonable functions (PUF) for IoT devices. ACM Computing Surveys, vol. 55, no. 14s, pp. 1-31, 2023.

[15] Nadeem, M., Arshad, A., Riaz, S., Zahra, S. W., Dutta, A. K., and Almotairi, S. A secure architecture to protect the network from replay attacks during client-to-client data transmission. Applied Sciences, vol. 12, no. 16, p. 8143, 2022.

[16] Babu, E. S., Dadi, A. K., Singh, K. K., Nayak, S. K., Bhoi, A. K., and Singh, A. A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system. Expert Systems, vol. 39, no. 10, p. e12941, 2022.

[17] Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., and Valli, C. Biometrics for internet-of-things security: A review. Sensors, vol. 21, no. 18, p. 6163, 2021.

[18] Mihailescu, M. I., and Nita, S. L. A searchable encryption scheme with biometric authentication and authorization for cloud environments. Cryptography, vol. 6, no. 1, p. 8, 2022.

[19] Pathak, N., Misra, S., Mukherjee, A., and Kumar, N. HeDI: Healthcare device interoperability for IoT-based e-health platforms. IEEE Internet of Things Journal, vol. 8, no. 23, pp. 16845-16852, 2021.