# Comprehensive Vulnerability Analysis of Three-Factor Authentication Protocols in Internet of Things-Enabled Healthcare Systems

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

***Abstract*—This study evaluates a three-factor authentication protocol designed for IoT healthcare systems, identifying several key vulnerabilities that could compromise its security. The analysis reveals weaknesses in single-factor authentication, time synchronization, side-channel attacks, and replay attacks. To address these vulnerabilities, the study proposes a series of enhancements, including the implementation of multi-factor authentication (MFA) to strengthen user verification processes and the inclusion of timestamps or nonces in messages to prevent replay attacks. Additionally, the adoption of advanced cryptographic techniques, such as masking and shuffling, can mitigate side-channel attacks by minimizing information leakage during encryption. The use of message authentication codes (MACs) ensures communication integrity by verifying message authenticity. These improvements aim to fortify the protocol's security framework, ensuring the protection of sensitive medical data. Future research directions include exploring adaptive security policies leveraging artificial intelligence and optimizing cryptographic operations to enhance efficiency. These efforts are essential for maintaining the protocol's resilience against evolving threats and ensuring the secure operation of IoT-based healthcare systems.**

***Keywords*—Three-factor authentication; IoT healthcare security; multi-factor authentication; side-channel attack mitigation; replay attack prevention**

## I. Introduction

The advent of the Internet of Things (IoT) has revolutionized numerous sectors, with healthcare emerging as one of the most transformative fields. IoT-enabled healthcare systems, commonly referred to as the Internet of Medical Things (IoMT), leverage interconnected medical devices to facilitate real-time monitoring, data collection, and analysis [1]. These systems enhance patient care by enabling continuous health monitoring, remote diagnosis, and timely medical interventions. However, the integration of IoT in healthcare also introduces significant security challenges, particularly concerning the protection of sensitive patient data from unauthorized access and cyber threats [2].

In response to these challenges, robust authentication protocols are paramount to ensure that only authorized users and devices can access sensitive medical information. Traditional authentication methods, often based on single or dual factors, have proven inadequate in the face of sophisticated cyber-attacks [3]. Consequently, three-factor authentication protocols have gained prominence as a more secure alternative [4]. These protocols typically combine knowledge-based (e.g., passwords), possession-based (e.g., smart cards), and inherence-based (e.g., biometric data) factors to provide a comprehensive security framework [4].

Despite their enhanced security, three-factor authentication protocols in IoT healthcare systems must address several challenges. The resource-constrained nature of many IoT devices limits their ability to execute complex cryptographic operations, necessitating the development of efficient, lightweight protocols [5]. Additionally, the dynamic and distributed nature of IoT networks requires authentication systems to be adaptable, maintaining security even as devices frequently join and leave the network [6]. Furthermore, 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), is critical [7].

This research aims to conduct a comprehensive analysis of an efficient three-factor authentication protocol designed for IoT healthcare systems [5]. The primary objective is to identify and scrutinize four 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 II presents a literature review of existing authentication protocols and their limitations. Section III outlines the methodology employed for vulnerability detection, including the analytical methods and tools used for cryptanalysis and security testing. Section IV discusses the identified vulnerabilities in detail, and proposes improvements to enhance the protocol's security and efficiency. Finally, Section V concludes with a summary of the findings and their implications for IoT-based healthcare authentication systems.

## II. Literature Review

### A. Current Authentication Protocols

The integration of the Internet of Things (IoT) into healthcare has necessitated the development of robust authentication protocols to protect sensitive medical data. Three-factor authentication schemes have gained prominence in

this context due to their enhanced security capabilities (Fig. 1). These protocols typically combine knowledge-based (e.g., passwords), possession-based (e.g., smart cards), and inherence-based (e.g., biometric features) factors to create a layered security framework [8].

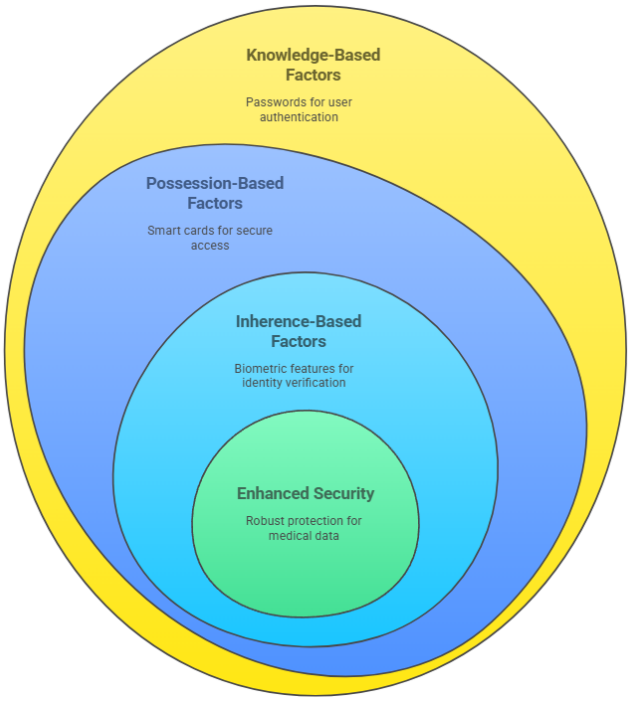


Fig. 1. Three-factor authentication in IoT healthcare security.

Despite their strengths, three-factor authentication protocols face significant challenges in IoT environments. The resource-constrained nature of many IoT devices limits their ability to execute complex cryptographic operations, necessitating the development of efficient, lightweight protocols [9]. Additionally, the dynamic and distributed nature of IoT networks requires authentication systems to be adaptable, maintaining security even as devices frequently join and leave the network [10].

Recent advancements in three-factor authentication protocols have focused on enhancing security while minimizing resource consumption. For instance, some protocols leverage elliptic curve cryptography (ECC) to provide strong security with reduced computational overhead [11]. Others incorporate advanced biometric recognition techniques, such as iris scanning, to enhance user authentication without physical contact, addressing both security and usability concerns [12].

### B. Related Works

The literature on IoT-based healthcare authentication systems reveals various vulnerabilities that necessitate ongoing research and innovation. One significant area of concern is the risk of sensor capture attacks, where adversaries gain physical access to devices and extract sensitive information. To mitigate this risk, some studies have proposed the integration of Physical Unclonable Functions (PUFs) as an additional authentication factor, providing a hardware-based layer of security resistance to cloning and physical attacks [13].

Another critical issue is the vulnerability of smart cards to theft and information extraction. While smart cards play a crucial role in safeguarding authentication schemes, their susceptibility to loss and unauthorized access poses a significant risk [14]. Research efforts have focused on developing secure storage and transmission mechanisms to protect the data stored on smart cards and ensure the integrity of the authentication process [15].

The literature also highlights the importance of privacy-preserving techniques in enhancing the security of IoT-based healthcare systems. Techniques such as zero-knowledge proofs and ring signatures have been proposed to protect user privacy while maintaining the transparency and auditability benefits of blockchain-based authentication [16].

In summary, the literature underscores the potential of three- factor authentication protocols to enhance security in IoT healthcare systems. However, addressing the identified vulnerabilities and challenges is crucial for realizing their full potential. Continued research and innovation in this field will play a vital role in securing the future of digital healthcare [17].

## III. Methodology

### A. Framework for Analysis

The methodology for analyzing the proposed three-factor authentication protocol for IoT in healthcare systems [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 analysis begins with a structured examination of the protocol's architecture, focusing on its critical components: registration, authentication, and session key establishment. 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 to 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 [5].

### C. 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:

$$K_{session} = g^{ab} \backslash \text{modp}$$

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 [5].

## IV. Analysis of the Proposed Protocol

### A. Overview of the Protocol

The proposed three-factor authentication protocol for IoT in healthcare systems is designed to enhance security through a series of robust cryptographic operations. The protocol is divided into several key phases: registration, authentication, and session key establishment. .

*1) Registration phase:* This phase initiates the secure setup of the system, where devices and users are registered with the central server. Each IoT device generates a random number $(a_i)$ and computes a pseudo-identity $(PID_i = h(ID_i \| a_i))$, where, $(h(\ ))$ is a secure hash function and $(ID_i)$ is the device's unique identifier (Fig. 2). The registration message sent to the server includes these parameters, ensuring that the device's identity is securely bound to its registration process [5].

| User $U_i$ | Gateway node $GW$ |
|---|---|
| Chooses $ID_i$, $PW_i$ and random number $r_i$<br>Also imprints $B_i$ at the sensor device<br>Computes $RPW_i = h(ID_i \| PW_i \| r_i)$,<br>$F_i = H(B_i \| r_i)$<br>$\xrightarrow{\{ID_i, RPW_i, F_i\}}$ | |
| | Produces a dynamic identity $DID_i$ and $R_g$<br>Calculates $A_i = h(DID_i \| X_G \| ID_g) \oplus h(RPW_i \| F_i)$,<br>$C_i = R_g \oplus h(DID_i \| X_G \| ID_g)$,<br>$D_i = h(RPW_i \| R_g \| F_i)$<br>Issue smartcard $\{A_i, C_i, D_i, DID_i, H(\cdot), h(\cdot)\}$<br>$\xleftarrow{Smartcard}$ |
| Compute $R_n = r_i \oplus h(ID_i \| PW_i \| H(B_i))$ and stores it into smartcard | |

Fig. 2. Overview of the protocol's user registration phase.

| User $U_i$ | Gateway node $GW$ | Sensor node $SN_j$ |
|---|---|---|
| | Computes $M_1 = M_1 \oplus h(DID_i \| X_G \| ID_g)$, $R_g = C_i \oplus h(DID_i \| X_G \| ID_g)$<br>Decrypts $M_2$ as $(ID_i \| SID_j \| T_1 \| A_i) = D_{h(M_1 \| R_g)}(M_2)$<br>If $T_2 - T_1 \leq \triangle T$ holds, Ok; Else quits.<br>Computes $h(RPW_i \| F_i) = A_i \oplus h(DID_i \| X_G \| ID_g)$,<br>$M'_3 = h(ID_i \| SID_j \| h(RPW_i \| F_i))$<br>If $M'_3 \stackrel{?}{=} M_3$ holds, Ok; Else quits.<br>Computes $X_{GS} = h(SID_i \| X_G)$,<br>$K_j = h(X_{GS} \| Y_G \| X_G)$.<br>$M_4 = E_{h(X_{GS} \| K_j)}(ID_g \| ID_i \| M_i \| A_i \| T_3)$,<br>$M_5 = N_i \oplus h(T_3 \| h(RPW_i \| F_i))$,<br>$M_6 = h(ID_i \| N_i \| T_3 \| ID_g)$<br>$\xrightarrow{\{M_1, M_4, M_5, M_6\}}$ | |
| | | Decrypts $M_4$ using $X_{GS}$ and $K_j$<br>As $(ID_g \| ID_i \| M_i \| A_i \| T_3) = D_{h(X_{GS} \| K_j)}(M_4)$<br>If $T_4 - T_3 \leq \triangle T$ holds, Ok; Else quits.<br>$h(RPW_i \| F_i) = M_1 \oplus M_i \oplus A_i$,<br>$N_i = h(T_3 \| h(RPW_i \| F_i)) \oplus M_5$.<br>$M'_6 = h(ID_i \| N_i \| T_3 \| ID_g)$<br>If $M'_6 \stackrel{?}{=} M_6$ holds, Ok; Else quits.<br>Calculates $M_7 = V_i \oplus h(M_i \| N_i)$,<br>$SK = h(h(RPW_i \| F_i) \| M_i \| N_i \| V_i))$,<br>$M_8 = h(SK \| ID_i \| ID_g \| T_5)$.<br>$\xleftarrow{\{M_7, M_8, T_5\}}$ |
| | Checks $T_6 - T_5 \leq \triangle T$.<br>Computes $T_i = M_7 \oplus h(M_i \| N_i)$, $SK' = h(h(RPW_i \| F_i) \| M_i \| N_i \| V_i))$,<br>$M'_8 = h(SK' \| ID_i \| ID_g \| T_5)$. $SN_j$<br>If $M'_8 \stackrel{?}{=} M_8$ holds, Ok; Else quits.<br>Computes $C_i^n = R_g \oplus h(DID_i^n \| X_G \| ID_g)$ and updates the database $\{DID_i^n, C_i^n\}$<br>Computes $M_9 = E_{h(RPW_i \| F_i)}(C_i^n \| N_i \| V_i \| DID_i^n)$ and $M_{10} = h(SK \| C_i^n \| DID_i^n)$.<br>$\xleftarrow{\{M_9, M_{10}\}}$ | |
| Decrypts $(C_i^n \| N_i \| V_i \| DID_i^n) = D_{h(RPW_i \| F_i)}(M_9)$, and computes $SK' = h(h(RPW_i \| F_i) \| M_i \| N_i \| V_i))$,<br>$M'_{10} = h(SK' \| C_i^n \| DID_i^n)$<br>If $M'_{10} \stackrel{?}{=} M'_{10}$ holds, replaces $DID_i$ with $DID_i^n$ and $C_i$ with $C_i^n$. | | |

Fig. 3. Overview of the protocol's user authentication phase.

*2) Authentication phase:* During this phase, mutual authentication between the IoT device and the central server is established. The protocol employs elliptic curve cryptography (ECC) for secure key exchanges (Fig. 3). Each device computes an authentication token using a hash of its identity and a session-specific random nonce:

$$\text{AuthToken} = h(ID_i \parallel \text{Nonce}_i)$$

This token is used to verify the device's authenticity, ensuring that only legitimate devices can participate in the network [5].

*3) Session key establishment:* Once authentication is successful, a secure session key is established between the device and the server. The session key ($K_{session}$) is derived from the ECC-based key exchange process:

$$K_{session} = g^{ab} \backslash \text{mod} p$$

where, ( g ) is a generator point on the elliptic curve, and ( 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 [5].

### B. Identified Vulnerabilities

Off-line Password Guessing Attack:

- Problem: The protocol aims to prevent off-line password guessing attacks, but an attacker can leverage leaked information from the registration phase (e.g., Regi = h(IDi || R₁ || HPWi), Ai = R; ⊕ HPWi, Ci = Bi ⊕ h(IDi ⊕ R; ⊕ HPWi)) and perform an off-line attack. Given a compromised HPWi, an attacker can try to guess PWi* such that h(IDi ⊕ PWi*) == HPWi.
- Attack Success Probability: The probability of a successful off-line guessing attack, given a limited password space and number of guesses is:

P(success) ≈ 1 - (1 - 1/|Password Space|)^N

where, |Password Space| is the size of the possible password set and N is the number of trials.

- Impact: If successful, the attacker gains the user's password and can compromise the authentication process.
- Improvement: Adding a salt to the password hashing process or implementing rate limiting on password attempts could mitigate this vulnerability. Multi-factor authentication could also strengthen security.

### C. User Impersonation Attack

- Problem: An attacker, knowing {TID, Regi, Ai, Ci, h()} from a compromised gateway node (GW), can create a forged login message {TID, IDsN, CID, M*, M, T₁} that successfully imitates a user during the login phase. Here, CID = IDi ⊕ h(TIDi || R || T₁), and M* = h(IDi || B || R₁ || T₁), and M = h(R || T₁) ⊕ R₁ where, R is derived as R = D₁ ⊕ h(TID; || K).
- Forgery: Attacker A can compute a valid looking B via B = C; ⊕ h(ID; ⊕ R ⊕ HPW* ) and since she also calculates ID, R and R1 based on intercepted information, the created messages M* and M will also be valid as calculated by M* = h(ID; || B || R1 || T₁)andM = h(R || T₁) ⊕ R₁ respectively.
- Impact: The GW accepts the forged messages. The system falsely authenticates the attacker as the legitimate user, allowing unauthorized data access or manipulation.
- Improvement: Using a keyed hash function (HMAC) or digital signatures involving a shared secret or private key for generating the messages CID, M*, and M would provide better message integrity and authentication. Adding randomness or time-related components could also enhance the security of the login phase.

### D. Known Session-Key Temporary Information Attack

- Problem: If temporary session values (R₁, R₂, and R₃) are compromised, an attacker can compute the session key, SK. The paper indicates SK = h(h(ID; || R₁ || R2) || R2 || R3).
  - This can be rewritten as SK = h(h(ID; || R₁ || R2) || R2 || R3) if R₁, R₂ and R₃ are compromised,
  - Then, an attacker can compute session key as SK = h(M' || R₂ || R₃) which is possible using values from captured messages, M4 = h(ID; || R₁ || R2) ⊕ SKGW_SN; and M5 = R2 ⊕ h(SKGW_SN;) if attacker can guess the identity.
- Vulnerable Calculation: Since M4 and M5 are sent over public channels and attacker knows, SKGW_SN; i.e., the secret parameter of GW and SNj, then temporary key can be computed as shown below.
- R₂ = M5 ⊕ h(SKGW_SN;) *h(ID; || R1 || R2) = M4 ⊕ SKGW_SN;
- SK = h(h(ID; || R1 || R2) || R2 || R3) = h(M' || R₂ || R₃) * The above calculation clearly shows how an attacker can get the session key SK.
- Impact: Session key compromise allows an attacker to decrypt data or modify messages within the compromised session.
- Improvement: Deriving the session key using all participant's secret values and not relying on temporary variables, and making sure R1, R2 and R3 are not sent in clear could mitigate the risk. Use of ephemeral keys within a key agreement protocol instead of relying on random numbers is recommended.

### E. Revelation of Secret Parameter SKGW_SN

- Problem: A legal, but malicious, user A who intercepts messages between GW and SN, can calculate SKGW_SN; Given messages {TID, IDsN, CID, M1, M2, T1}, {M3, M4, M5}, and {M7, M8}, A can calculate the secret parameter using R2 = M5 ⊕

h(SKGW_SN;) and SKGW_SN; = M4 ⊕ h(ID; || $R_1$ || $R_2$). Given the above values, A can compute SKGW_SN;

- Attack: By intercepting M4 = h(ID; || $R_1$ || R2) ⊕ SKGW_SN;, and M5 = R2 ⊕ h(SKGW_SN;) and knowing R2 by computation from message {M7, M8} $R_2$ = M5 ⊕ h(SKGW_SN;) and calculating h(ID; || R1 || R2) as well, A can compute the secret parameter SKGW_SN;.
- Impact: Knowing SKGW_SN; allows an attacker to compromise the authentication and key exchange between GW and SN. It can lead to a gateway node or a sensor node impersonation attacks.
- Improvement: Key derivation functions should be designed with proper key secrecy and key derivation must not expose parameters used in further computations.
- Using Keyed Hash functions such as HMAC would be preferable for generating the values SKGW_SN; and SK.
- The long-term secret keys of the system should not be used directly for generating the session key as used in the paper.

While this paper aims to enhance security with a three-factor authentication mechanism, the proposed protocol contains several critical vulnerabilities that can be exploited by a determined attacker. The vulnerabilities outlined above highlight the importance of carefully designing cryptographic protocols to avoid such weaknesses. By addressing these flaws and following best practices in cryptographic engineering, it's possible to create robust protocols that better protect sensitive data and systems.

### *F. Proposed Improvements*

To address the vulnerabilities identified in the proposed three-factor authentication protocol for IoT healthcare systems, several improvements are recommended. These enhancements are designed to fortify the protocol against unauthorized access and ensure the protection of sensitive medical data.

First, to mitigate the weaknesses associated with single-factor authentication, it is crucial to implement multi-factor authentication (MFA). This enhancement involves combining traditional password-based authentication with additional factors such as biometrics (e.g., fingerprint or iris recognition) and possession-based tokens (e.g., smart cards). By requiring multiple forms of verification, MFA significantly reduces the risk of unauthorized access, as an attacker would need to compromise all authentication factors to gain entry.

Second, to prevent time synchronization attacks, the protocol should incorporate timestamps or nonces into each message. This modification ensures that replayed messages are detected and rejected, enhancing the protocol's resilience against replay attacks. For instance, each message can be appended with a unique timestamp or a random nonce:

$$M = \text{HID}, B1, Y1, A1, V1, \text{TS}$$

or

$$M = \text{HID}, B1, Y1, A1, V1, \text{Nonce}$$

This enables the server to validate these elements, confirming message freshness and authenticity.

Third, to protect against side-channel attacks, it is essential to minimize information leakage during cryptographic operations. Techniques such as masking and shuffling can be employed to obscure correlations between power consumption and cryptographic computations. Masking involves adding random values to intermediate computations, while shuffling changes the order of operations to make it difficult for attackers to predict the sequence of computations. These techniques increase the difficulty of deducing cryptographic keys from side-channel information.

Fourth, to prevent replay attacks and ensure communication integrity, the use of message authentication codes (MACs) is recommended. By appending a MAC to each message:

$$M = \text{data}, \text{MAC}(\text{data}, SK)$$

the recipient can verify the MAC to ensure that the message has not been tampered with. This enhancement prevents attackers from modifying or retransmitting messages without detection, maintaining the integrity of the communication channel.

Fifth, to enhance the protocol's scalability and efficiency, optimizing cryptographic operations is necessary. Implementing lightweight cryptographic algorithms, such as the Advanced Encryption Standard (AES) in its lightweight form, can significantly reduce 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.

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

## V. CONCLUSION

In conclusion, the analysis of the proposed three-factor authentication protocol for IoT healthcare systems highlights critical vulnerabilities, including single-factor authentication weaknesses, time synchronization issues, side-channel attack risks, and replay attack susceptibility. By implementing recommended security enhancements, such as multi-factor authentication, timestamps, and advanced cryptographic techniques, the protocol can significantly improve its security posture [18-20]. These measures ensures robust protection of sensitive medical data, fostering trust in IoT-enabled healthcare environments. As the IoT landscape continues to evolve, ongoing research into adaptive security measures and lightweight cryptographic algorithms will become crucial in maintaining the protocol's resilience against emerging threats.

## ACKNOWLEDGMENT

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

## REFERENCES

[1] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, S. P. Thipperudraswamy, Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare, Biosensors, vol. 12, no. 8, p. 562, 2022.

[2] S. Selvaraj and S. Sundaravaradhan, Challenges and opportunities in IoT healthcare systems: a systematic review, SN Applied Sciences, vol. 2, no. 1, p. 139, 2020.

[3] M. T. Ahvanooey, M. X. Zhu, Q. Li, W. Mazurczyk, K. K. R. Choo, B. B. Gupta, M. Conti, Modern authentication schemes in smartphones and IoT devices: An empirical survey, IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7639-7663, 2021.

[4] K. Renuka, S. Kumari, X. Li, Design of a secure three-factor authentication scheme for smart healthcare, Journal of Medical Systems, vol. 43, no. 5, p. 133, 2019.

[5] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, F. Wu, An enhanced three-factor based authentication protocol using wireless medical sensor networks for healthcare monitoring, Journal of Ambient Intelligence and Humanized Computing, pp. 1-22, 2024.

[6] S. Kumar and A. kumar Keshri, An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model, Knowledge-Based Systems, vol. 299, p. 112052, 2024.

[7] A. Schmidt, Regulatory challenges in healthcare IT: Ensuring compliance with HIPAA and GDPR, Academic Journal of Science and Technology, vol. 3, no. 1, pp. 1-7, 2020.

[8] P. Soni, A. K. Pal, S. H. Islam, An improved three-factor authentication scheme for patient monitoring using WSN in remote healthcare system, Computer Methods and Programs in Biomedicine, vol. 182, p. 105054, 2019.

[9] M. N. Khan, A. Rao, S. Camtepe, Lightweight cryptographic protocols for IoT-constrained devices: A survey, IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, 2020.

[10] A. Hamarsheh, An adaptive security framework for internet of things networks leveraging SDN and Machine Learning, Applied Sciences, vol. 14, no. 11, p. 4530, 2024.

[11] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, N. Kumar, A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers, The Journal of Supercomputing, vol. 74, no. 12, pp. 6428-6453, 2018.

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

[13] C. Labrado and H. Thapliyal, Design of a piezoelectric-based physically unclonable function for IoT security, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2770-2777, 2018.

[14] C. Shouqi, L. Wanrong, C. Liling, H. Xin, J. Zhiyong, An improved authentication protocol using smart cards for the Internet of Things, IEEE Access, vol. 7, pp. 157284-157292, 2019.

[15] F. Kausar, Iris based cancelable biometric cryptosystem for secure healthcare smart card, Egyptian Informatics Journal, vol. 22, no. 4, pp. 447-453, 2021.

[16] K. Azbeg, O. Ouchetto, S. J. Andaloussi, Access control and privacy-preserving blockchain-based system for diseases management, IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1515-1527, 2022.

[17] T. V. Le, C. F. Lu, C. L. Hsu, T. K. Do, Y. F. Chou, W. C. Wei, A novel three-factor authentication protocol for multiple service providers in 6G-aided intelligent healthcare systems, IEEE Access, vol. 10, pp. 28975-28990, 2022.

[18] T. Suleski, M. Ahmed, W. Yang, E. Wang, A review of multi-factor authentication in the Internet of Healthcare Things, Digital Health, vol. 9, p. 20552076231177144, 2023.

[19] A. M. Mostafa, M. Ezz, M. K. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani, W. Said, Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication, Applied Sciences, vol. 13, no. 19, p. 10871, 2023.

[20] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, H. A. Alkhzaimi, Cryptography algorithms for enhancing IoT security, Internet of Things, vol. 22, p. 100759, 2023.