Cryptanalysis and Countermeasures of the Authentication Scheme for Mobile Healthcare Environments

1st Hyeonjung Jang
Department of Electronic Engineering
Kyungpook National University
Daegu, Korea
jungi1713@knu.ac.kr

2nd Chaeeon Kim
Department of Electronic Engineering
Kyungpook National University
Daegu, Korea
chaeon@knu.ac.kr

3rd Deokkyu Kwon
Department of Electronic Engineering
Kyungpook National University
Daegu, Korea
kdk145@knu.ac.kr

4th Youngho Park
Department of Electronic Engineering
Kyungpook National University
Daegu, Korea
parkyh@knu.ac.kr

***Abstract*—The mobile healthcare provides numerous advantages, such as enabling timely and accurate diagnosis of patients' health and supporting personalized medical services. Nevertheless, mobile healthcare systems remain vulnerable to various security attacks because sensor data is transmitted through public channels. Such data typically contains patients' sensitive information. Hence, a robust mutual authentication scheme is required to guarantee that only authorized entities can access patients' personal data. In 2025, Saleem et al. proposed a secure authentication scheme for mobile healthcare system. While they asserted their scheme provides mutual authentication between patients and medical professionals, we find some security flaws in their scheme. Saleem et al.'s scheme is vulnerable to insider and ephemeral secret leakage (ESL) attack, and they cannot guarantee user anonymity and untraceability in authentication phase. Therefore, we demonstrate weaknesses of Saleem et al.'s protocol through informal analysis and provide countermeasures for mutual authentication.**

***Index Terms*—mutual authentication, healthcare, key exchange, insider attack, security.**

I. Introduction

Mobile healthcare refers to mobile network to deliver medical services using mobile device such as smartphones, tablets and laptops. It enables patients to receive healthcare anytime, anywhere [1]. Mobile healthcare offers telemedicine services in which body sensors connect with medical systems to provide continuous care. It can improve convenience, enhance efficiency, and foster sustainability in patient's daily life [2]. The patient's sensor can continuously capture diverse biometric signals, such as heart rate, blood pressure, body temperature, electrocardiograms (ECG), and electrogastrograms (EGG) [3]. The data are transmitted in real time to healthcare providers including physicians, nurses, pharmacists, and health insurance companies, enabling timely and accurate diagnosis of patients' health conditions [4]. Based on this data, healthcare providers can deliver personalized treatments and predictive healthcare services [5]. A typical hospital system is a physician-centered service that requires a patient to visit the hospital in person. However, mobile healthcare facilitates the realization of patient-centered medical services through telemedicine system [6]. Consequently, mobile healthcare not only enhances patient's quality of life but also improves the efficiency and sustainability of medical systems by enabling remote monitoring, telemedicine, and moblity-enabled medical services.

Although mobile healthcare offers many advantages, several challenges remain. In the mobile healthcare, large amounts of sensor data are collected on mobile devices [7]. Continuous sensing, transmission, and on-device processing cause substantial power demands [8]. Therefore, low power design and energy optimization are essential. There are also security threats related to privacy. Due to the nature of wireless transmission, there are risks of data tampering, tracking, and jamming [9]. Since sensor data include user's sensitive health information, the communication via public channel is prone to exposure to various security attacks [10], [11]. It is thus required to ensure the mutual authentication, confidentiality, and integrity of data [12]. To cope with these challenges, secure communication should be ensured by establishing session keys through lightweight authentication between patients and healthcare providers.

Recently, Saleem et al. [13] proposed an authentication and key exchange scheme for the mobile healthcare environment. They uses lightweight cryptography such as exclusive-OR and hash functions in authentication scheme. Their scheme is based on a physical unclonable function (PUF) and advanced

This research was supported by the Regional Innovation System & Education(RISE) Glocal 30 program through the Daegu RISE Center, funded by the Ministry of Education(MOE) and the Daegu, Republic of Korea.(2025-RISE-03-001).

encryption standard (AES) to defend against physical attacks. They claimed that their authentication scheme is efficient and secure. However, we find that their scheme is vulnerable to insider and ESL attack. Moreover, their scheme does not guarantee user anonymity and untraceability, and also suffers from a correctness problem. These vulnerabilities are significant threats in healthcare environments where patient privacy is important. Therefore, we conduct cryptanalysis of Saleem et al.'s scheme through informal analysis and offer countermeasures to overcome security flaws of their scheme.

II. System Model

Fig. 1 shows the system model of the Saleem et al.'s scheme. The system model consists of three entities: the medical server (MS), the medical gateway (MGW_j), and the user (U_i). Under the control of MS, MGW_j and U_i establish a session key to exchange patient's data securely. MGW_j refers to patient's mobile device connected to the patient's sensors. The roles of each entity are described as follows.

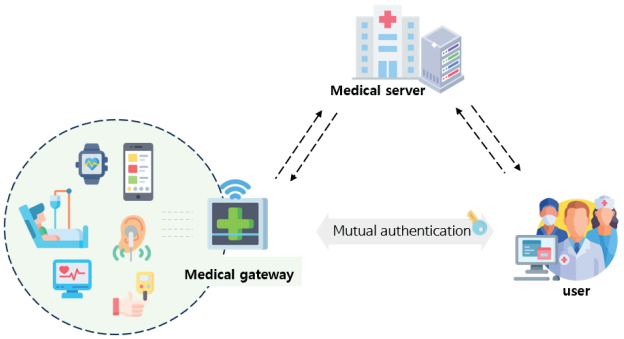

Fig. 1. System model.

- **Medical server (MS):** The MS is located at the center of MGW_j and U_i, and functions as both a data repository and an authentication server. The MS is assumed to have sufficient computational resources [14].
- **Medical gateway (MGW_j):** The MGW_j is a terminal mobile device wirelessly connected to the patient's sensors. The patient's wearable sensors collect real-time data such as heart rate, blood pressure, and body temperature.
- **User (U_i):** The U_i typically refers to a healthcare provider such as a doctor, nurse, or pharmacist who uses a personal portable device to access and remotely monitor patient data stored in the medical server.

III. Review of Saleem et al.'s Scheme

We review Saleem et al.'s authentication scheme for mobile healthcare environments. The notations used in their protocol are summarized in Table I. Their scheme consists of three phases: (i) user registration, (ii) medical gateway registration, and (iii) authentication.

TABLE I
Notations of Saleem et al.'s Scheme

Notation	Description
U_i, MS, MGW_j	User, Medical server, Medical gateway
ID_i, PW_i, bio	Real identity, password, biometric of U_i
PID_i, GID_j	Pseudo identity of U_i and MGW_j
mk	Master key of MS
k_i, k_j	U_i, MGW_j's shared key with MS
$E_{(k,\pi)}(\cdot), D_{(k,\pi)}(\cdot)$	CBC-based AES encryption and decryptin
π	Initialize vector for CBC-based AES
$PUF(\cdot)$	Physical unclonable function
cha, res	Challenge/response value of MGW_j
SK	Session key
$h(\cdot)$	Hash function
$\oplus, \|\|$	exclusive-or, and concatenate operation
r_k	Random number
T_k	Timestamp

A. User Registration Phase

U_i must register with MS before authentication. After registration, MS provides the necessary values to U_i for the authentication phase. The server securely stores the values of U_i using AES encryption. The detailed step are illustrated in Fig 2.

User (U_i)	Medical Server (MS)
$\xrightarrow{\{ID_i\}}$	Generates PID_i and k_i Stores ID_i, k_i in AES encrypted form
	$\xleftarrow{\{PID_i, k_i\}}$
Generate PW_i, bio Computes $(x_i, hd) = Gen(bio)$ $A_i = h(h(ID_i) + h(ID_i\|\|PW_i\|\|bio)) \bmod q$ $k_i' = k_i \oplus ID_i \oplus x_i$ Stores $\{hd, A_i, k_i', PID_i\}$	

Fig. 2. User registration phase of Saleem et al.'s scheme.

B. Medical Gateway Registration Phase

MGW_j registers with MS before the authentication phase and receives the values required for authentication. MGW_j then computes the corresponding response using the PUF, and transmits the response to MS. The detailed description are illustrated in Fig 3.

Medical Server (MS)	Medical Gateway (MGW_j)
Selects ID_j, GID_j, cha, k_j $\xrightarrow{\{ID_j, cha, GID_j, k_j\}}$	
	Computes $res = PUF(cha)$
	$\xleftarrow{\{res\}}$
Stores ID_j, k_j, res in AES encrypted form	

Fig. 3. Medical gateway registration phase of Saleem et al.'s scheme.

C. Authentication Phase

This is an authentication phase Saleem et al.'s scheme. In the authentication phase, U_i and MGW_j, under the relay of MS, exchange the session key SK. During the authentication phase, all messages are transmitted over a public channel. Fig 4 shows the detailed step of authentication phase.

Fig. 4. Authentication Phase of Saleem et al.'s scheme.

IV. Cryptanalysis of Saleem et al.'s scheme

In this section, we analyze the authentication scheme proposed by Saleem et al. We discover that their scheme is vulnerable to insider and ESL attacks, fails to guarantee user anonymity and untraceability, and suffers from a correctness flaw.

A. Insider Attack

If an adversary $\mathcal{A}$ registers with MS as a legitimate user, $\mathcal{A}$ can perform authentication and establish a session key with MGW_j. Subsequently, $\mathcal{A}$ can compute session keys shared between MGW_j and other users. The detailed description is provided below.

Step 1: $\mathcal{A}$ performs authentication as a legitimate user and obtains $res \oplus ID_j$ by computing $D_3 \oplus (r_2||r_3)$. The $res \oplus ID_j$ is not updated in every session.

Step 2: $\mathcal{A}$ eavesdrops on D'_3 and D'_7 transmitted over the public channel during a session between MGW_j and another user. Then, $\mathcal{A}$ computes $(r'_2||r'_3) = D'_3 \oplus res \oplus ID_j$ and $(r'_5||r'_3) = D'_7 \oplus r'_2$. Finally, $\mathcal{A}$ can derive the session key $SK' = h(GID_j||ID_{ms}||r'_2||r'_5)$ shared between MGW_j and another user.

Therefore, Saleem et al.'s scheme does not prevent insider attacks.

B. User Anonymity and Untraceability

If an adversary $\mathcal{A}$ as insider has $res \oplus ID_j$ of specific MGW_j and a user authenticates twice with the MGW_j, $\mathcal{A}$ can obtain the user's real identity and trace continuous authentication of the user. The detailed step is as follows.

Step 1: $\mathcal{A}$ who has $res \oplus ID_j$ eavesdrops PID_i, D_1, D_3, D_8 from the user's first session and PID_i^* from the second session. Namely, PID_i^* denotes PID_i^{new} from the first session.

Step 2: $\mathcal{A}$ computes $(r_2||r_3) = D_3 \oplus res \oplus ID_j$, $r_1 = D_8 \oplus PID_i \oplus PID_i^*$, and $ID_i = D_1 \oplus (GID_j||r_1||r_2)$. Then, $\mathcal{A}$ obtains the user's real identity ID_i.

Step 3: Consequently, $\mathcal{A}$ eavesdrops D'_1, D'_8, PID'_i in each of the user's sessions and computes $(GID_j||r'_1||r'_2) = D'_1 \oplus ID_i$ and $PID_i^{new} = D_8 \oplus PID'_i \oplus r'_1$.

$\mathcal{A}$ can derive PID_i^{new} of the user using ID_i in every session. Hence, Saleem et al.'s scheme does not guarantee user anonymity and untraceability.

C. ESL Attack

Suppose that an adversary $\mathcal{A}$ obtains the session specific random numbers r_1, r_2, r_3, r_4, and r_5. In this case, $\mathcal{A}$ can compute the session key $SK = h(GIDj||IDms||r2||r5)$ using the random numbers and the public identities of MGW_j and MS. This demonstrates that the confidentiality of the session key relies heavily on the secrecy of session specific random values. Once these values are leaked, $\mathcal{A}$ can compute the session key without needing the user's or server's long-term secrets. Therefore, Saleem et al.'s scheme fails to resist ESL attack.

D. Correctness Issue

In Saleem et al.'s scheme, U_i computes $A_i = h(h(ID_i) + h(ID_i||PW_i||bio))$ for login. However, the user's biometric bio changes slightly each time due to noise. If U_i uses bio directly without the stable key generated by the fuzzy extractor, the output of the hash function will always differ. Then, the user will fail to log in consistently. As as result, Saleem et al.'s scheme has correctness issues in user login phase.

V. Countermeasure

The authentication scheme of Saleem et al. is exposed to insider and ESL attacks, has a correctness issue, and fails to guarantee user anonymity and untraceability. We provide countermeasures to overcome these security weaknesses. The detailed descriptions are as follows.

- **Countermeasure against insider attack and Lack of untraceability:** In their authentication phase, the overall

computation relies on XOR operations except for verification values. In the cases of insider attack and user untraceability, the vulnerabilities arise because a fixed, non-updated value such as $res \oplus ID_j$ is reused in multiple sessions. To mitigate these weaknesses, we recommend the use of change parameter in every session employing random numbers or timestamps with hash functions (e.g. $h(res||ID_j||T_1)$) rather than XOR alone.

- **Countermeasure against ESL attack:** In Saleem et al.'s scheme, the session key is derived only from session specific numbers. It makes the scheme susceptible to ESL attack. We note that the shared values k_i and k_j between U_i and MS, and between MGW_j and MS, are used only for verification. Incorporating shared key such as k_i, and k_j into the session key derivation would ensure that only the legitimate parties can compute the session key, maintaining security even if a session-specific number is exposed.
- **Countermeasure against correctness issue:** During the user's login process, U_i uses bio as hash function's input directly. It causes a correctness problem due to biometrics variation. In Saleem et al.'s scheme, U_i utilizes a fuzzy extractor. The fuzzy extractor is a technique that derives a stable key from noisy data such as biometrics. Therefore, the correctness problem can be solved by inserting a key x_i of the fuzzy extractor instead of bio.

VI. CONCLUSION

In this paper, we reviewed the mutual authentication scheme of Saleem et al. for mobile healthcare environments. Through informal analysis, we demonstrated that it fails to prevent several attacks including insider and ESL attack and does not support user anonymity and untraceability. Moreover, their scheme suffers from a correctness flaw in the user login phase. These weaknesses result from the use of non-updated parameters and reliance on XOR operations alone. To address them, we present countermeasures such as using more hash functions and session-specific numbers to improve the security level of the protocol. In the future, we plan to propose a concrete authentication protocol that establishes a session key between healthcare providers and patients. We will also evaluate security and efficiency through performance analysis and formal analysis, using "Burrows-Abadi-Needham (BAN)" logic, "Real-or-Random (RoR)" model, and "Automated verification of internet security protocols and applications (AVISPA)" simulation tool.

ACKNOWLEDGMENTS

REFERENCES

[1] B. M. Silva, J. J. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, "Mobile-health: A review of current state in 2015", *Journal of biomedical informatics,* vol. 56, pp. 265-272, Aug. 2015.

[2] J. A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Feb. 2014.

[3] J. J. P. C. Rodrigues et al., "Enabling Technologies for the Internet of Health Things," *IEEE Access*, vol. 6, pp. 13129-13141, 2018.

[4] H. Demirkan, "A Smart Healthcare Systems Framework," *IT Professional,* vol. 15, no. 5, pp. 38-45, Sept.-Oct. 2013.

[5] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *Journal of oral biology and craniofacial research*, vol. 12, no. 2, pp. 302-318, Mar/Apr. 2022.

[6] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," *Sustainability*, vol. 15, no. 4, pp. 3317, Feb. 2023.

[7] D. Kwon, S. Son, M. Kim, J. Lee, A. Kumar Das and Y. Park, "A Secure Self-Certified Broadcast Authentication Protocol for Intelligent Transportation Systems in UAV-Assisted Mobile Edge Computing Environments," *IEEE Transactions on Intelligent Transportation Systems,* vol. 25, no. 11, pp. 19004-19017, Nov. 2024.

[8] M. M. Baig, H. GholamHosseini, and M. J. Connolly, "Mobile healthcare applications: system design review, critical issues and challenges." *Australas Phys Eng Sci Med,* vol. 38, pp. 23–38, Dec. 2015.

[9] M. Wazid, J. Singh, C. Pandey, R. S. Sherratt, A. K. Das, D. Giri, and Y. Park, "Explainable deep Learning-Enabled malware attack detection for IoT-Enabled intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems,* vol. 26, no. 5, pp. 7231-7244, May. 2025.

[10] H. Taleb, A. Nasser, G. Andrieux, N. Charara, and E. Motta Cruz, "Wireless technologies, medical applications and future challenges in WBAN: A survey," *Wireless Networks*, vol. 27, no. 8, pp. 5271-5295, Sep. 2021.

[11] S. Prajapat, D. Gautam, P. Kumar, S. Jangirala, A. K. Das, Y. Park, and P. Lorenz, "Secure Lattice-Based Aggregate Signature Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology,* vol. 73, no. 9, pp. 12370-12384, Sept. 2024.

[12] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," *IEEE Wireless Communications,* vol. 22, no. 4, pp. 104-112, 2015.

[13] M. A. Saleem, X. Li, K. Mahmood, Z. Ghaffar, Y. Xie, and G. Wang, "Provably Secure Authenticated Key-Management Mechanism for e-Healthcare Environment," *IEEE Internet of Things J.,* Apr. 2025.

[14] D. Gautam, G. Thakur, P. Kumar, A. K. Das and Y. Park, "Blockchain Assisted Intra-Twin and Inter-Twin Authentication Scheme for Vehicular Digital Twin System," *IEEE Transactions on Intelligent Transportation Systems,* vol. 25, no. 10, pp. 15002-15015, Oct. 2024.