International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I8P239
Volume 70 Issue 8, 387-393, August 2022

Original Article

Can the User Authentication System for the Electronic Medical Record System Improve the Power to Secure in Medical Field? A Security Analysis

Seonjae Been [1], Younsung Choi[2], Haewon Byeon[3]

[1]*Department of Digital Anti-aging Healthcare (BK-21), Inje University, Republic of Korea.*
[2,3]*AI Convergence College, Inje University, South Korea*

[1]been.sj986@gmail.com

Received: 24 June 2022 Revised: 16 August 2022 Accepted: 24 August 2022 Published: 27 August 2022

Abstract *- The electronic medical record is the set of individual patient health information stored in a digital format. This format can be shared across medical networks. This system enables the efficient transfer of medical records between institutions, patients and staff. The EMR contains personal health information; therefore, network access to patient-related data must be controlled to ensure that unlawful parties do not misuse personal information. Han et al. proposed several biometric-based authentication methods. However, Madhusudan et al. revealed that the biometric-based authentication method proposed by Han et al. had various weaknesses and proposed an authentication scheme with improved security suitable for the EMR system. In this paper, through security analysis, we analyse the operation process of the scheme by Madhusudhan et al. and reveal problems, including $H(B_i)$ recognition errors, no perfect forward secrecy, insider attacks (user identification guessing attacks), insider attacks (forgery attacks) and denial-of-service attacks.*

Keywords *- Security Analysis, Authentication Scheme, EMR, Patient information, Medical Data.*

1. Introduction

The continuous development of technology has produced remarkable results for the development of humankind, such as artificial intelligence, IoT, virtual reality, blockchain technology, and robotics. The development of these technologies has contributed greatly to society. This development also includes the modern healthcare system. Technology has brought products and procedures to the medical field, such as wireless brain sensors, x-ray machines, heart monitors (HN), food scanners (SN), robotic surgery (SR) and other advances. In addition, simpler versions support medical care through TMIS and EMRs. (Telecare Medicine Information System, Electronic Medical Records).

The EMR is a piece of patient health information stored electronically in digital format that can be shared across a wider range of healthcare networks [1]. These records include various data, such as personal statistics, medications, allergies, demographics, immunisation status, electrocardiogram (ECG or EKG) and electroencephalography (EEG) reports, laboratory test (Lab test) results, medical history, vital signs and other information such as an image. Medical doctors (MD) use these records to diagnose the disease and provide further treatment [2]. The EMR can store data accurately and provide to ensure readability. And it also provides to ensures medical records transformation between patients, institutions and physicians. This system eliminates the need to track traditional paper medical records, capturing a patient's condition whenever needed. Combining different medical health record types across multiple systems helps clinicians identify the stratification of patients with chronic diseases. Remotely accessing medical data or merging health data residing at various sites into a central storage system can have a greater potential for loss of privacy in the data than if systems with traditional paper records did not take appropriate safeguards [3]. However, when applied with related technologies, the EMR can be advantageous over traditional paper medical records. EMR technology has reached a technological maturity stage and is being utilised as an essential component for managing health [4]. Policymakers and analysts have discovered that EMR systems have the potential to treat diseases and improve health, and they have called for more widespread use of EMR systems [5].

EMR records are shared or exchanged through enterprise-wide network information systems and various information networks [6]. Monitoring that controls access to various patient data on the network should ensure that personal data is not misused by unauthorised parties [7]. End-to-end authentication has become difficult because communication channels, such as wireless local area networks (LAN), wired local area networks (WLN) and wide area networks (WAN), are involved [8]. This authentication can be performed as appropriate by verifying the identity of the communicating party. A user's anonymity maintains (UAM) the confidentiality of the user identification, which plays a significant role in preventing eavesdroppers from discovering connections between communicating parties and ensuring user authentication [9]. As the healthcare field transmits highly sensitive personal information, ensuring user authentication in electronic healthcare services is essential. Therefore, user authentication is essential, and a secure authentication system is crucial.

The authentication method using a password is a one-step authentication method and can be said to be the simplest authentication method. However, since this authentication method is not secure, a smart card is used to enhance security. Because the smart card (SC) contains integrated circuits, so it can process, store, and transmit data [10]. However, if the power consumption (PCn) generated during the operation of the smart card is analysed, the data stored in the smart card can be analysed. Therefore, smart cards and biometric-based authentication (BbA) mechanisms are preferred. Biometrics comprise an individual's behavioural or psychological characteristics. Physical and behavioural human characteristics are very stable because they are challenging to falsify compared to cyphers or security codes [4]. BbA is accomplished in several ways: fingerprint, face recognition, iris recognition, speaker recognition technology, hand flexion, retinal flexion, and more [11]. These methods are used alone or with smart cards and cryptographic algorithms [12] or in combination with other algorithms, such as secure data transmission natural number algorithms, Elliptic Curve Cryptography (ECC) algorithms, biometrics, and hybrid group key management schemes to provide enhanced security for all applications [13-15]. Therefore, several biometric-based authentication methods reinvented by A were designed [16]. In this article, the security vulnerability of the technique by Han et al. is revealed, and a robust technique against these weaknesses is proposed.

Further, the calculation and execution times are compared. Madhusudhan [17] et al. proposed an authentication scheme with improved security to solve this problem. In this paper, through security analysis, we analyse the operation process of the scheme by Madhusudhan et al. and reveal such problems as $H(B_i)$ recognition errors, no perfect forward secrecy, insider attacks (user identification guessing attacks and forgery attacks) and denial-of-service (DoS) attacks.

This paper is organised as follows. Section 2 explains the terminology and mathematical background. Section 3 presents the analysis of the operation process of the security-enhanced authentication scheme proposed by Madhusudhan et al. (SPM). Section 4 describes the vulnerabilities found by analysing the security of the SPM. Finally, Section 5 concludes our paper.

2. Related Study

2.1. Summary of Symbol

Table 1 describes the terms used in the operation process. Table 1 shows the terms used in this paper.

Table 1. A symbol used in our paper

Symbol	Meaning
U_i	"User"
ID_i	"Identity of U_i"
B_i	"Biometrics of U_i"
PW_i	"Password of U_i"
SC_i	"Smart card of U_i"
S_i	"Server"
x	"Secret key of the server"
P	"Base point of the chosen elliptic curve, *E."*
$h(.)$	"Hash function"
$H(.)$	"Biohash function"
$\oplus$	"XOR operation"
$\|$	"Concatenation operator"
T_i	"Timestamp"

2.2. Mathematical Knowledge

2.2.1. Hash function

The hash function takes in a message of any length and outputs a hash of a fixed length known as a hash value $H(M)$. The hash value is a feature only present in the input message.

2.2.2. Biohashing

Biohashing uses your own tokenised random number to randomly map a biometric feature to a binary string (Biohash). In other words, it uses your random numbers to create a security template that has the form of an irreversible set of binary strings using biometric data [18].

2.2.3. Fuzzy Extraction

The fuzzy extractor (Fuext) can transform the user's biometric information into the form of a random string. Therefore, encryption technology for biometrics can be applied. This extractor comprises *Gen* ("generate") and *Rep* ("reproduce"), which are efficient randomisation functions [19].

3. Process Analysis

Madhusudhan et al. Scheme operation process analysis. The overall scheme process of Madhusudhan et al. is shown in Fig 1.

3.1. Registration phase (R phase)

When a new user (NU) wants to register with the telemedicine server (Telem Ser), the following steps:

a) The user U_i selects their own Identity, Password, and Biometrics (ID_i, PW_i, B_i). Then, the hashed password value $MPW = h(PW_i \| r) \oplus H(B_i)$ is calculated. The random number r is the random number selected from the user U_i. The user Sends a registration request message $\{ ID_i , MPW_i \}$ to Server S_i Using secure communication.

b) S_i calculates $K_1 = h(ID_i \| MPW_i)$ and $K_2 = h(h(ID_i \| x) \oplus h(ID_i) \oplus MPW_i$ Using x. The x is the server's master key. Then S_i generate a random number a to calculates $CID_i = h(ID_i) \oplus a$. It then stores $\{ a, CID_i \}$ in the server's database and issues the user's smart card (SmCa), including the values $\{K_1, K_2, CID_i, h(.), H(.)\}$.

c) Upon reception in the Smart card (SmCa) SC_i, the user U_i stores the random number r and now has $\{ r, K_1, K_2, CID_i, h(.), H(.)\}$ values.

3.2. Login phase (L phase)

When a user U_i has the will to log in to the server S_i, the smart card performs the next steps:

a) The user U_i installs their smart card into the smart card reader and inputs identity ID_i, password PW_i and biometric B_i. The smartcard calculates $MPW = h({PW_i}^l \| r) \oplus H(B_i)$, $K_1 = h({ID_i}^l \| MPW_i)$ and verifies if it is equal to K_1. If it is equal, step b) is executed, otherwise the entered identity ${ID_i}^l$ or password PW_i is not the same as the user's original identity (oriden) ${ID_i}^l$ or password PW_i and the process ends. Local password verification is performed at this stage.

b) The smart card calculation computes a random nonce r_i and calculates $M_1 = K_2 \oplus h({ID_i}^l) \oplus {MPW_i}^l$, $M_2 = M_1 \oplus r_1$ and $M_3 = h(h({ID_i}^l) \| M_1 \| M_2 \| T_1)$. It then forwards the login request message $\{T_1, M_2, M_3, CID_i\}$ to S_i.

3.3. Authentication phase (A phase)

The server executes the next phase S_i when it receives $\{T_1, M_2, M_3, CID_i\}$ from the user U_i. Fig 1 shows all the steps of the login and authentication (Loau) steps in the Madhusudhan et al. scheme:

a) The server S_i will check whether $|T_1\text{-}T_2| \leq \delta T$ holds, and if it does not hold, the timestamp received in the login message (logm) is outside the required threshold and aborts the session to resist replay attacks. If true, the server S_i takes into a the value associated with the CID_i got from the user's login message and calculated ${h(ID_i)}^l = CID_i \oplus a$, ${M_1}^l = h(h(ID_i)^l \| x)$ and $M_3 = h(h({ID_i}^l) \| M_1 \| M_2 \| T_1)$. Then check if ${M_3}^l = M_3$ is correct. If this holds, the server S_i computed random numbers b and r_2, and calculates ${r_1}^l = M_2 \oplus {M_1}^l$, ${CID_i}^{new} = h(ID_i) \oplus b$ and $M_4 = {M_1}^l \oplus r_2$. Then update $\{CID_i, a\}$ in the database with $\{{CID_i}^{new}, b\}$. Also calculate $SK = h(h({ID_i}^l) \| {r_1}^l \| r_2 \| {M_1}^l)$ and $M_5 = h(SK \| {M_1}^l \| M_4 \| T_3)$ where T_3 is the current timestamp. The server S_i then sends the user U_i an authentication message $\{M_4, M_5, {CID_i}^{new}, T_3\}$.

b) Upon receiving $\{M_4, M_5, {CID_i}^{new}, T_3\}$ from the server S_i, the user's smart card takes a timestamp T_4 and checks the freshness of T_3. Then we calculate ${r_2}^l = M_1 \oplus M_4$, $SK^l = h(h(ID_i) \| r_1 \| {r_2}^l \| M_1)$, ${M_5}^l = h(SK^l \| M_1 \| {M_4}^l \| T_3)$ and check whether ${M_5}^l = M_5$ holds. If they are not the same, the session is forced to end. To be maintained, the user U_i's smart card replaces $\{CID_i$ with ${CID_i}^{new}$ and uses the time stamp T_5 to calculate $M_6 = h(M_1 \| M_4 \| T_5)$. After then, the user sends the messages (Usm), including $\{M_6, T_5\}$ to the server S_i.

c) The server S_i validates the time stamp T_5 and checks that $h(M_1 \| M_4 \| T_5) = M_6$ is valid. If it holds, the server S_i authenticates the user U_i and accepts $SK = SK^l$ as the session key.

3.4. Password change phase (P phase)

Assuming a user U_i wants to modify their password (modpa) or update their biometrics, the following calculation is performed.

a) The user U_i inserts a smart card and enters ID_i, PW_i, B_i.

b) The smart card calculates $MPW_i = h({PW_i}^l \| r) \oplus H(B_i)$, ${K_1}^l = h({ID_i}^l \| {MPW_i}^l)$ and confirms whether ${K_1}^l$ is equal to K_1. If not, the session is aborted. If they are the same, the user U_i inputs the biometric information ${B_i}^{new}$ and user's new password ${PW_i}^{new}$.

c) The smart card SC_i counts ${MPW_i}^{new} = h({PW_i}^{new} \| r) \oplus H(B_i)^{new}$, ${K_1}^{new} = h(ID_i \| {MPW_i}^{new})$ and ${K_2}^{new} = K_2 \oplus MPW_i \oplus {MPW_i}^{new}$. Finally, replace respectively, K_1 and K_2 with ${K_1}^{new}$ and ${K_2}^{new}$.

4. Vulnerability Analysis

4.1. $H(B_i)$ recognition error

In Madhusudhan et al. scheme, a general hash function uses biometric information. If a general hash function is used, there is a problem that an error occurs even if biometric information is input slightly differently.

The user U_i enters biometric information in the login phase (l phase) to log in to the server S_i. B_i becomes the value of $H(B_i)$ using $H(.)$ for encryption. The login step proceeds only when the ${K_1}^l$ value is equal to K_1, ${K_1}^l$ is $h({ID_i}^l \parallel MPW_i)$, and MPW_i is $h({PW_i}^l \parallel r) \oplus H(B_i)$ to input MPW_i as $H(B_i)$. Since B_i Biometric information shows a little difference each time you enter a value. Since the combination of $H(.)$ comes out differently depending on the input value, even if B_i is input slightly differently, the value of $H(B_i)$ may be output differently from the existing value.

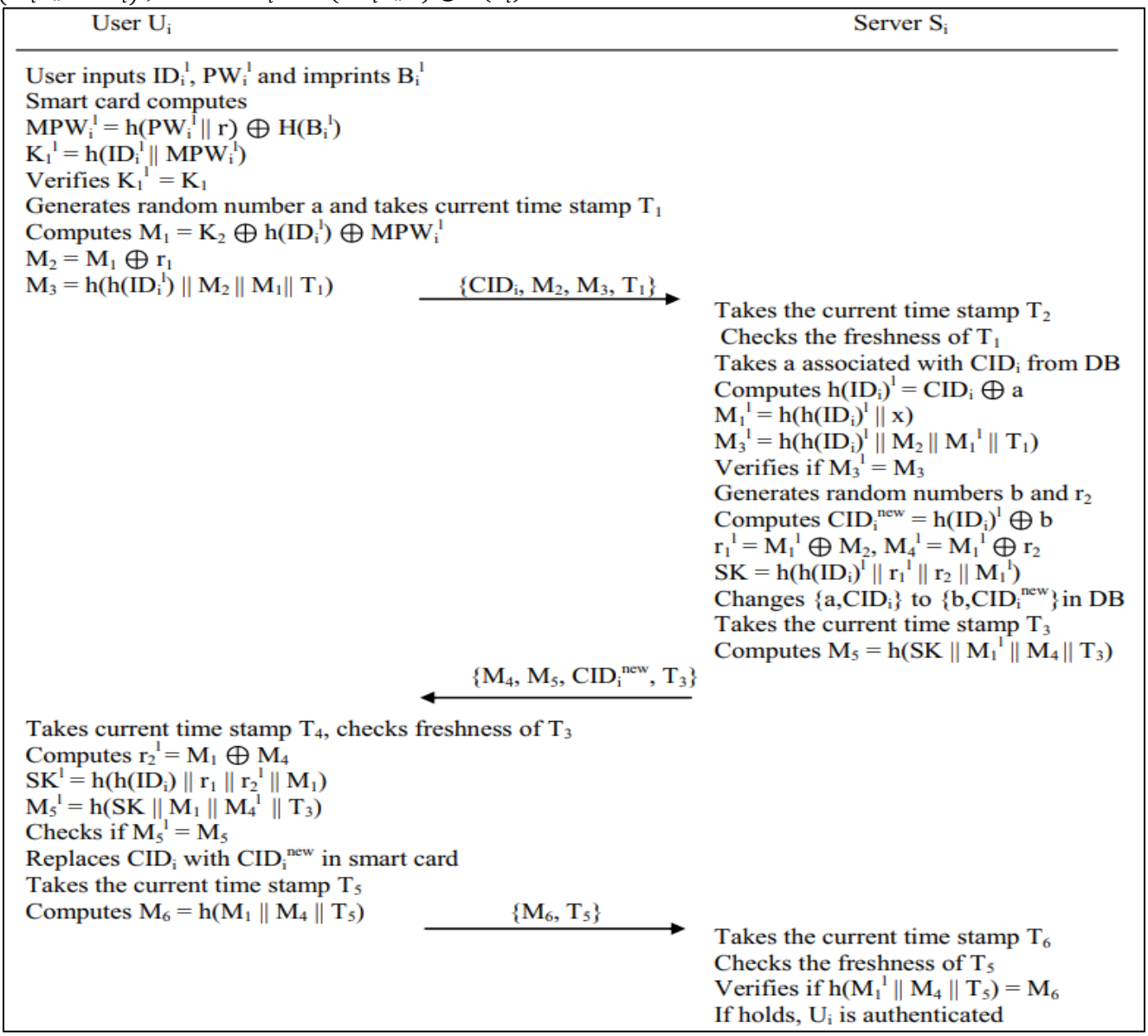

Fig. 1 A login and authentication phase (a phase) of the proposed scheme

There is a method of utilising fuzzy extraction technology to solve this security problem. In fuzzy extraction, Gen() function and Rep() function are used. Gen() function calculates R_i value and helper string P_i, which is the uniform string from information generating [20,21,22].

$$\text{Gen}(B_i) = (R_i, P_i)$$

The Rep() function allows calculating the same R_i value using the P_i value even if a B_i the value that is almost similar to the B_i is the value used in the Gen() function is input as reproduce.

$$R_i = \text{Rep}(B_i, P_i)$$

As such, by using fuzzy extraction technology, it is possible to solve the problem of a recognition error occurring as biometric information changes slightly over time, even for the same person.

4.2. No perfect forward secrecy (NPFS)

The fact that Perfect Forward Secrecy (PFS) is satisfied means that even if one of the important master keys (MK) of the scheme is exposed, the previous session key cannot be found [23,24]. However, in this scheme, if the value of x, one of the unchanging long-term keys (LTK), is exposed, not only the future session key but also the previously used session key can be found, which does not satisfy Perfect Forward Secrecy (PFS). And if the attacker acquires the user's smart card and knows the inside information, he can also find the user's previous session key.

The smart card contains r, K_1, K_2, CID_i, $h(.)$, $H(.)$. $K_1 = h(ID_i{}^l \| MPW_i)$, and $K_2 = h(h(ID_i \| x) \oplus h(ID_i) \oplus MPW_i$. $MPW_i = h(h(ID_i \| x) \oplus h(ID_i) \oplus K_2$. The process of finding the value of $h(ID_i)$ is shown in Fig 2. can be inferred by looking at the expression of K_2, and when the inferred expression is substituted into K_1 , $K_1 = h(ID_i{}^l \| h(h(ID_i \| x) \oplus h(ID_i) \oplus K_2)$ becomes. $h(ID_i)$ can be found through this process, and when x and $h(ID_i)$ are found, M_1 can be known.

If the attacker gets user's smart card,
the attacker can acquires $\{K^1, K^2, CID_i, r, h(\cdot), H(\cdot)\}$

$K^1 = h(ID_i \| MPW_i)$
$K^2 = h(h(ID_i) \| x) \oplus h(ID_i) \oplus MPW_i$
$MPW_i = h(h(ID_i) \| x) \oplus h(ID_i) \oplus K^2$
$K^1 = h(ID_i \| h(h(ID_i) \| x) \oplus h(ID_i) \oplus K^2$

→ The attacker can calculate $h(ID_i)$

Fig 2. A no perfect forward secrecy (NPFS)

If the attacker knows the value of M_1, he can find out the r_1 value by using $r_1{}^l = M_2 \oplus M_1{}^l$ from the M_2 obtained from the previous U_i -> S_i transmission message in the login phase. In addition, the r_2 value can be known by using $r_2 = M_1{}^l \oplus M_4$ from M_4 obtained from the previous S_i -> U_i transmission message in the login phase.

Therefore, since the attacker can find out the r_1, r_2 values used in the previous communication with x, $h(ID_i)$ And can create SK through the $SK^l = h(h(ID_i{}^l) \| r_1{}^l \| r_2 \| M_1{}^l)$ Expression in the authentication step, Madhusudhan et al. scheme does not satisfy perfect forward secrecy.

4.3. Insider attack (User ID guessing attack)

The number of cases of $h(ID_i)$ is small because the range that can create an ID is narrow because it must be used within a limited length, such as uppercase and lowercase letters, numbers, and special characters when creating an ID. So, insiders can guess the user's identity.

In the login phase, U_i sends a login request message $\{T_1, M_2, M_3, CID_i\}$ to S_i. Therefore, the insider can know the values of T_1, M_2, M_3, CID_i. Since the insider can also know the value of M_1 in the authentication phase, using the T_1 and M_2 values received from the login request message and the M_1 value in the authentication phase, $h(ID_i)$ can be guessed through $M_3{}^l = h(h(ID_i{}^l) \| M_1 \| M_2 \| T_1)$ in the authentication phase. Fig 3 shows the guessing process of $h(ID_i)$.

In Login phase, U_i sends $\{T_1, M_2, M_3, CID_i\}$ to S_i
An attacker can get M_1 in authentication phase

$M_3 = h(h(ID_i) \| M_2 \| M_1 \| T_1)$
The attacker knew M_3, M_2, T_1, M_1

→ **The attacker can guess** ID_i

Fig 3. Insider attack (User ID guessing attack)

4.4. Insider attack (Forgery Attack)

Insiders can know M_1 and $h(ID_i)$. The value of $r_1{}^l$ can be obtained through $r_1{}^l = M_1 \oplus M_2$, because M_2 is the value U_i receives from S_i at the login stage, and is the value obtained by XOR operation M_1 and the random nonce r_1. $r_1{}^l$ is obtained through this process, and S_i is sent to U_i through $M_4{}^l = M_1{}^l \oplus r^2$, so r^2 can be created using the known M_4 value and the known M_1. SK can be found by using the known values of M_1 and $h(ID_i)$ for $r_1{}^l$, r^2 and $SK = h(h(ID_i{}^l) \| r_1{}^l \| r_2 \| M_1{}^l)$. Using SK found here, it is possible to create a value of M_5 from $M_5 = h(SK \| M_1{}^l \| M_4 \| T_3)$. Also, using CID_i in the login request message received from U_iThe value of CID_i is changed to $CID_i{}^{new}$. An authentication message $\{M_4, M_5, CID_i{}^{new}, T_3\}$ can be sent from S_i to U_i.

Finally, to successfully log in, U_i must send $\{M_6, T_5\}$ to S_i, and M_6 is made of $h(M_1 \| M_4 \| T_5)$. You can log in by sending the created M_6 and the time stamp of the current time T_5 to S_i.

4.5. Denial of Service

The calculation formula from receiving the login request message to comparing the M_3 value requires 2 times stamp-related operations, 1 DB-related search operation, 1 XOR operation, 2 hash operations, and 1 comparison operation. Vulnerable to DOS attack. The calculation process is shown in Fig 4.

Denial of Service (DOS) reduces all allowed bandwidth by sending a large amount of information to a specific network at once or depletes the resources of the attack target system to prevent service [25, 26].

S_i checks whether ${M_3}^l = M_3$ is maintained in the authentication step. In this step, it is determined whether the user attempting to log in is a normal user by comparing the M_3 value. Therefore, the subsequent process can be performed only when the value of M_3 is satisfied.

When S_i receives the user's login message $\{T_1, M_2, M_3, CID_i\}$ from the U_i, the S_i extracts CID from the DB after comparing the time point with T_1 and the current timestamp T_2. When CID is extracted, the value related to CID obtained from the login message is taken in a and $h(ID_i)^l = CID_i \oplus a$, ${M_1}^l = h(h(ID_i)^l \| x)$ and ${M_3}^l = h\left(h\left({ID_i}^l\right) \| M_2 \| {M_1}^l \| T_1\right)$ are calculated. After all, these processes are completed, M_3 values are compared. If it is satisfied by comparing ${M_3}^l$ and M_3, the value of CID_i is changed to the value of ${CID_i}^{new}$. Therefore, it is possible to find out the CID_i value changed to the ${CID_i}^{new}$ value.

Therefore, the DOS attack uses the $CID_i the$ value found earlier, the CID_i found when proceeding from the login stage to the authentication stage, and T_1, which is the timestamp of the current time, and the values of M_2 and M_3. M_2 and M_3 are randomly inserted and attack the server.

In Authentication phase,

S_i check if $M_3^l = M_3$ hold and distinguish normal U_i

U_i sends $\{T_1, M_2, M_3, CID_i\}$ to S_i

Take the current T_2 checks the freshness of T_1 and takes a associated with CID_i from DB

$h(ID_i)^l = CID_i \oplus a$

$M_1^l = h(h(ID_i)^l \| x)$

$M_3^l = h(h(ID_i)^l \| M_2 \| M_1^l \| T_1)$

Verifies if $M_3^l = M_3$

→ **High computational cost on verification**

Fig 4. calculation process

5. Conclusion

In this paper, a security analysis was conducted after explaining the authentication scheme's operation process with improved security for the EMR proposed by Madhusudhan et al.. The SPM has security problems, such as $H(B_i)$ recognition errors, no perfect forward secrecy (FS), insider attacks (IA) (user identification guessing attacks and forgery attacks), and DoS attacks.

Acknowledgment

Our research was funded by Basic Science Research Program (BSRP) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (ME), grant number "2018R1D1A1B07041091, 2021S1A5A8062526", and "2022 Development of Open-Lab based on 4P in the Southeast Zone (SZ)".

References

[1] T. D. Gunter, and N. P. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions," *J Med Internet Res*, vol. 7, no. 1, pp. e383, 2005.

[2] M. Nikooghadam, and A. Zakerolhosseini, "Secure Communication of Medical Information using Mobile Agents," *J Med Sys*, vol. 36, no. 6, pp. 3839–3850, 2012.

[3] R. C. Barrows Jr and P. D. Clayton, "Privacy, Confidentiality, and Electronic Medical Records," *Journal of the American Medical Informatics Association*, vol. 3, no. 2, pp. 139-148, 1996.

[4] J. Goldsmith, D. Blumenthal, and W. Rishel, "Federal Health Information Policy: A Case of Arrested Development," *Health Affairs*, vol. 22, no. 4, pp. 44-55, 2003.

[5] C. W. Burt, and J. E. Sisk, "Which Physicians and Practices are using Electronic Medical Records?," *Health Affairs*, vol. 24, no. 5, pp. 1334-1343, 2005.

[6] S. B. Othman, A. Trad, and H. Youssef, "Security Architecture for at-Home Medical Care using Wireless Sensor Network," *IEEE*, pp. 304-309, 2014

[7] M. Li, W. Lou, and K, Ren, "Data Security]and Privacy in Wireless Body Area Networks," *IEEE Wirel. Commun.*, vol. 17, no. 1, pp. 51-58, 2010.

[8] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Cryptanalysis and Improvement of 'A Secure Authentication Scheme for Telecare Medical Information System' with Nonce Verification.," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 841-853, 2016.

[9] C. S. Park, "Authentication Protocol Providing user Anonymity and Untraceability in Wireless Mobile Communication Systems.," *Computer Networks*, vol. 44, no. 2, pp. 267-273, 2004.

[10] W. Rankl, and W. Effing, "*Smart Card Handbook*," John Wiley & Sons., 2004.

[11] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric Authentication: A Review.," *International Journal of u-and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13-28, 2009.

[12] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES And AES) for Information Security.," *Int. J. Comput. Appl.*, vol. 67, no. 19, 2013.

[13] R. Mahaveerakannan, and C. S. G. Dhas, "Customised RSA Public Key Cryptosystem using Digital Signature of Secure Data Transfer Natural Number Algorithm.," *IJCTA*, vol. 9, no. 5, pp. 543-548, 2016.

[14] K. Lauter, "The advantages of Elliptic Curve Cryptography For Wireless Security.," *IEEE Wirel. Commun.*, vol. 11, no. 1, pp. 62-67, 2004.

[15] R. Mahaveerakannan, and C. Suresh Gnana Dhas, "A Hybrid Group Key Management Scheme for Uav–Mbn Network Environment Increasing Efficiency of Key Distribution in Joining Operation.," *International Conference on Intelligent Information Technologies.*, pp. 93-107, 2017.

[16] L. Han, X. Tan, S. Wang, and X. Liang, "An Efficient and Secure Three-Factor Based Authenticated Key Exchange Scheme using Elliptic Curve Cryptosystems.," *Peer Peer Netw. Appl.*, vol. 11, no. 1, pp. 63-73, 2018.

[17] C. S. Nayak, "An Improved User Authentication Scheme for Electronic Medical Record Systems.," *Multimed. Tools Appl.*, vol. 79, no. 29, pp. 22007-22026, 2020.

[18] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, "Security Analysis and Improvement of Bio-Hashing Based Three-Factor Authentication Scheme for Telecare Medical Information Systems.," *J. Ambient Intell. Humaniz. Comput*, vol. 9, no. 4, pp. 1061-1073, 2018.

[19] Y. choi, "Smart Card Based Password Authentication Scheme using Fuzzy Extraction Technology.," *Journal of Korea Society of Digital Industry and Information Management*, vol. 14, no. 4, pp. 125-134, 2018.

[20] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How To Generate Strong Keys from Biometrics and Other Noisy Data.," International Conference on the Theory and Applications of Cryptographic Techniques.," pp. 523-540, 2004.

[21] X. Boye, Reusable cryptographic fuzzy extractors, "Proceedings of the 11th ACM conference on Computer and Communications Security," pp. 82-91, 2004.

[22] W. Duch, R. Adamczak, and K. Grabczewski, "A New Methodology of Extraction, Optimisation and Application of Crisp and Fuzzy Logical Rule," *IEEE Transactions on Neural Networks*, vol. 12, no. 1, pp. 277-306, 2001.

[23] Y. choi, J. Nam, D. Lee, J. Kim, J. Jung and D. Won, "Security Enhanced Anonymous Multiserver Authenticated Key Agreement Scheme Using Smart Cards And Biometrics.," *The Scientific World Journal*, 2014.

[24] M. Nikooghadam, and H. Amintoosi, "Perfect Forward Secrecy Via an ECC-Based Authentication Scheme for SIP in Voip.," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 3086-3104, 2020.

[25] W. S. Chun, and D. W. Park, "A Study on N-IDS Detection and Packet Analysis Regarding a DoS Attack.," *Journal of the Korea Society of Computer and Information*, vol. 13, no. 6, pp. 217-224, 2008.

[26] A. D. Wood, and J. A. Stankovic, "Denial of Service in Sensor Networks.," *Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[27] Dr. Azeez Ajani Waheed, Mrs. Kikelomo Okesola, Mrs. Oluwaseyi Afe, Mr. Babafemi Samuel "An Integrated and Secured Web Based Electronic Health Record" International Journal of Recent Engineering Science 8.4(2021):19-26.

[28] Salim Istyaq, Afrah Nazir, Mohammad Sarosh Umar "*Hybrid Graphical User Authentication Scheme Using Grid Code"* International Journal of Engineering Trends and Technology 69.5(2021):166-176.

[29] Mezui Eya'a Guy Lysmos, Dr.Mostafa Hanoune, *"Hybrid Data Compression System In Smart E-Health Gateway For Medical Monitoring Applications"* SSRG International Journal of Computer Science and Engineering 7.1 (2020): 1-6. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V7I1P101