Cyber Security and Applications 1 (2023) 100013

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Cryptanalysis of Secure ECC-Based Three Factor Mutual Authentication Protocol for Telecare Medical Information System

C. Madan Kumar[a], Ruhul Amin[b,*], M. Brindha[a]

[a] Department of Computer Science & Engineering, National Institute of Technology, Tiruchirappalli 620015, India
[b] Department of Computer Science & Engineering, National Institute of Technology, Jamshedpur, Jharkhand 831014 India

ARTICLE INFO

Keywords:
Telecare medical information system
Authentication
Elliptic curve cryptography
Biohashing

ABSTRACT

Telecare Medical Information System (TMIS) is gaining importance in the present COVID-19 crisis. TMIS as a technology, offers patients a range of remote medical services, incorporated into Wireless Body Area Network (WBAN). The patient's medical report is confidentially transmitted over an open channel in TMIS environments. An attacker may attempt to compromise the security, such as forgery, replay, and impersonation attacks. To ensure secure communication, various authentication solutions have been introduced for TMIS. Biometrics and Elliptic Curve Cryptography-based mutual authentication protocol was recommended by Sahoo et al. (2020) and is proved to have some loopholes in the protocol. We discovered, however, Sahoo et al. method is unable to prevent privileged insider attacks and insider attacks along with patient anonymity. Jongseok Ryu et al. recommended a ECC based three-factor mutual authentication protocol and ensures patient's confidentiality for TMIS with proof of informal analysis. They have also performed formal security studies utilizing the Automated Validation of Internet Security Protocols and Applications (AVISPA), the Burrows–Abadi–Needham (BAN) logic and Real-Or-Random (ROR) model. However, we have reviewed the Jongseok Ryu et al.'s proposal. Based on his attacker model, we have examined that this scheme is unsafe against Message Substitution Attacks, Man-in-the-Middle attacks, Session Key Disclosure attacks, Privileged Insider attacks, and Stolen verifier attacks. we suggest a technique to be safe from the above security threats.

1. Introduction

People have developed an interest in utilizing remote services to limit social interaction with others in the recent COVID-19 issue. They avoid going to hospitals and medical centers for fear of spreading the virus to patients who may have the disease. Most of the population found it challenging to go to hospitals and medical centers because of their sensitive health or other circumstances. As a result, there is a growing need for utilizing medical resources online, such as diagnosing patient health online, prescribing medicines, and monitoring patients' health using wearable devices. Wireless Body Area Network (WBAN) is employed for providing medical benefits with the quick progress of internet and wireless communication technology. One of the technologies utilized in WBAN is the Telecare Medical Information System (TMIS), which may deliver various medical services to patients in remote locations through telecare servers [1,2]. TMIS is receiving greater attention in the COVID-19 situation than earlier in-person healthcare services. Patients use wearable sensor devices in the TMIS environment to record their medical data, like heart rate, body temperature and blood pressure. Then, their medical report was sent to the registered mobile devices. Patients can then send the medical data to telecare medical servers anytime. After receiving patient medical data, the telecare servers provide appropriate healthcare services with doctor's suggestions available in remote access, such as medical monitoring, therapy, prescriptions, etc. Patients can use intelligent healthcare services, saving time and money. These advantages make TMIS more suitable for providing competent medical services than instead of the physical presence of patients in the recent COVID-19 circumstances. Despite having many benefits, as mentioned, TMIS has several security-related issues. The telecare server in TMIS is responsible for protecting patient privacy and medical data, including identities, passwords, and medical records available electronically. Only authorized patients should be given access to safeguard the privacy and confidentiality of the patient data. Additionally, private patients' information is sent to the telecare medical server over a open channel, giving a chance for an attacker to carry out various attacks like man-in-the-middle (MITM) attacks and impersonation attacks. Therefore, key agreement techniques and secure mutual authentication are crucial challenges in TMIS contexts. To address TMIS security issues, numerous studies have recently been proposed [3,4]. An IoT-enabled device with mutual verification protocol for TMIS was designed by

* Corresponding author.
E-mail addresses: amin_ruhul@live.com (R. Amin), brindham@nitt.edu (M. Brindha).

https://doi.org/10.1016/j.csa.2023.100013
Received 26 July 2022; Received in revised form 25 September 2022; Accepted 25 January 2023
Available online 5 February 2023

Sahoo et al. [3]. Sahoo et al.'s technique uses biometric data, Elliptic Curve Cryptography, and symmetric key cryptosystem to secure the patient's confidential data. They asserted that their proposed protocol could survive various security attacks such as offline password guessing attacks, replay attacks, and smartcard Stolen attacks. We scrutinized that their proposed protocol is compromised with privileged insider attacks and insider attacks. In line, we investigated that their scheme is defenseless for patient anonymity and a password updating process. This research recommends a robust mutual authentication protocol with three-factor authentication for TMIS that uses a patient's mobile communication device.

1.1. Research contribution

In this article, we have reviewed Jongseok Ryu's authentication scheme for Telecare Medical Information System. We then demonstrated that Ryu's proposal is vulnerable to Message substitution attacks, Man-in-the-middle attacks, Session Key Disclosure attacks, and privileged insider attacks described in Section 5 by performing the cryptanalysis on Ryu's authentication scheme. We also proposed suggestions for improving the protocol, which prevents the attacks mentioned above.

2. Related works

In the recent trend, numerous authentication methods were proposed for TMIS environments [2,5–9]. Using a smartcard for two-factor-based authentication and TMIS was proposed by Khan and Kumari [10] in 2013. They claimed their system is safe from offline password prediction attacks, replay attacks, and stolen verifier attacks. Their plan is defenseless to an offline password guessing attack. To enhance Khan and Kumari's system, Giri et al. [11] recommended a user authentication scheme appertaining to RSA in 2014. Giri et al. asserted that their proposal defends numerous threats like guessing offline password attacks, insider attacks, and replay attacks by performing informal security. Giri et al.'s technique is suffering from privileged insider attacks and guessing offline passwords found by Amin and Biswas [12] in 2015. Later, they offered an enhanced RSA-based authentication method and AVISPA to have high security. However, Sutrala et al. [13] found that Amin and Biswas's proposal failed to control offline password guessing attacks, impersonation attacks and replay attacks. Later, they suggested an RSA-based verification scheme and key agreement scheme.

Authenticated key agreement approach in TMIS, utilizing ECC, was suggested by Zhang and Zhu [14] in 2015 and offers greater security having a minor key size compared to Asymmetric key cryptography like RSA. Zhang and Zhu claimed their safety against offline and MITM password guessing assault. According to Liu et al. [15], Zhang and Zhu's protocol cannot resist guessing offline password attacks, including attacks using smartcards thefts. An ECC-based authentication technique was also presented in 2018 by Ostad-Sharif et al. [16]. Their system contains security weaknesses like key compromise impersonation and password guessing attacks, although being more effective than RSA [17]. These techniques [10–12,18–21] depend on the following factors like password and smartcard, by which it is challenging to perform attacks using stolen smartcards or offline password guessing attacks. Researchers recommended a three-factor authentication technique to address the issues in the TMIS environment with two-factor authentication [3,22,23]. Lu et al. [22] in 2015, recommended an authentication protocol with a biometric technique for the TMIS architecture. They claimed their proposal is safe against multiple security assaults, like replay attacks and offline password guessing attacks. Their proposal, however, is prone to impersonation attacks and offline password guessing attacks [24]. In 2016, Ravanbakhsh and Nazari [25] proposed a session key agreement technique with an enhanced mutual authentication for TMIS. Unfortunately, Ostad-Sharif et al. [26] shows that Ravanbakhsh and Nazari's method cannot guarantee forward secrecy and cannot defend against known session-specific temporary information attacks. Then, in 2018, Qi and Chen [27] recommended mutual authentication technique adopting biometrics features and Elliptic Curve Cryptography for TMIS. They proved that their proposal offers mutual authentication by employing BAN logic. However, there are security weaknesses in the Qi and Chen approach, like key compromise impersonation attacks along with offline password guessing attacks [28]. Consequently, Lu et al. [22], Ravanbakhsh and Nazari [25], Qi and Chen [27] continue to be unsuitable for TMIS situations. In 2019, Zeng et al. [29] exhibited an anonymous user authentication (E-AUA) proposal for both users and servers in a multiserver environment. In 2020, Shoban Mandal et al. [30] scrutinized that Zeng et al.'s proposal is suffering from lost/stolen smart gateway, offline Password guessing assault involving a privileged insider attack and has proposed Certificateless-Signcryption-Based Three-Factor User Access Control Scheme, resistant to assaults mentioned above. In 2019, Shuai et al.'s protocol [31] presented a protected three-factor authentication protocol for online patient monitoring. In 2020 Jiaqing Mo et al. [32] scrutinized that Shuai et al.'s proposal is prone to offline dictionary guessing attacks and privileged insider attacks by performing the cryptanalysis. In addition, they also pointed out a flaw in their design, part of their proposal results password update phase and proposed countermeasures for the enhancement of Two verification Schemes for Healthcare Systems. Using Wireless Medical Sensor Networks, we can prevent all possible attacks. Fotouhi et al. [33] in 2020, proposed a secured scheme having perfect forward security, untraceability, and resilience against numerous attacks, is secure against a variety of known attacks required for WBANs. The suggested technique is resistant to known session-specific temporary information attacks as well as key compromise impersonation attempts. Taleb et al. [34] in 2021, presented a analysis between leading wireless technologies with proposed wireless technologies oriented for medical applications. Jiliang Li et al. [35] in 2021, to avail complete public channels in IoMT, introduced the provably secure and lightweight MAAKA (PSL-MAAKA) protocol. The hash operation and XOR operation are the main operations in the verification stage and key agreement. This article uses the random oracle model to demonstrate the security of the protocol that is being given. In 2020, Xiong Li et al. [35] have proposed a strategy that offers user privacy and guards against sensor node impersonation attacks. Later, Muhammad Asad Saleem et al. [36] claimed that their scheme fails to prevent sensor node impersonation attacks and fails to provide user anonymity. Muhammad proposed a suitable solution for the problem mentioned above. In 2021, authors [37,38] proposed a robust anonymous verification and key agreement proposal with privacy-preserving for smart cities. In 2022, Tanveer et al. [5], proposed REAS-TMIS claiming that this protocol is resistant to all possible attacks. Madan et al. [39] has scrutinized the Tanveer et al.'s protocol and found that it is suffering from session key disclosure attacks, privileged insider attacks, and medical server impersonation attacks. Madan et al. has recommended a mechanism to overcome the above mentioned attacks. In 2022, Many Authors, including Prateek et al. [40–45] recommended V2I authentication in vehicular ad-hoc networks, suggested implementing the Privacy-Preserving verification Protocol for Quantum Computing. Using message authentication codes, several message authentication proposals are also created in VANETs. The quantum cryptosystem [46,47], which combines quantum ciphering and conventional encryption, utilizing laws of physics and quantum mechanics for safe transmission of data between the involved entities. A quantum key exchange or distribution technique [48,49] does not rely on the computationally difficult behaviour of some mathematical problem. A subset of the enormously popular developing concept of IoT is called the Internet of Vehicles (IoV). In order to transform a vehicle into a smart vehicle, an extended vehicular adhoc network (VANET) is used, by giving them a on board unit (OBU), enabling them to communicate with other vehicles, Humans (customers or pedestrians), technology (internet, cloud, parking lots, traffic signals, etc.). Through messages or beacons, the vehicles can directly or indirectly communicate with each other over wireless open channels. Open channels during communication allow for a

Table 1
Summary of the existing work in user authentication schemes.

Scheme	Year	Cryptographic Features	Limitations
Zhang et al. [52]	2017	Exclusive-OR, chaotic map and SHA	difficult to prevent PGU and SIM attacks.
Qui et al. [53]	2018	ECC, Exclusive-OR, and SHA	difficult to prevent URIM attacks. Unable to provide URA feature.
Chaudhry et al. [54]	2018	ECC, Exclusive-OR, and SHA	difficult to prevent EPLE attacks and impersonation and can not provide anonymity feature.
Renuka et al. [9]	2019	ECC, Exclusive-OR, and SHA	cannot prevent PIN and provide URA feature.
Madhusudhan et al. [8]	2019	Exclusive-OR, chaotic map and SHA	cannot prevent replay, MATM, PIN, and SIM. Does not provide MA and URA feature.
Son et al. [2]	2020	BP, Exclusive-OR, and SHA	cannot prevent replay, MATM, PIN, and SIM. Does not provide MA and URA feature.
Nayak et al. [7]	2020	Exclusive-OR, and SHA	difficult to prevent D-SYN and cannot provide URA feature.
Chaudhry et al. [55]	2021	ECC, Exclusive-OR, and SHA	cannot prevent impersonation attacks and EPLE attacks and cannot provide anonymity feature.
Ryu et al. [6]	2022	ECC, Biohashing	cannot restrain impersonation, forgery and MITM attack.
Tanveer et al. [5]	2022	SHA and AEAD scheme	cannot restrain impersonation, smartcard stolen attack, insider attack

variety of attacks, including replay, man-in-the-middle, impersonation, fabrication, etc. To overcome these attacks, Bagga et al. [50] developed a novel remote access management system to address security concerns in smart transportation. Later, keeping in view the needs of smart devices in terms of storage cost, Yan et al. [51] designed a update protocol to optimize the storage cost to constant. Sahoo et al. [3] developed a three-factor authentication scheme for the TMIS environment in 2020 to solve security issues comparable to existing techniques. Their technique proved resistant to insider attacks, offline password guessing, and attacks using stolen smart cards. We scrutinized Sahoo et al.'s solution and found it defenseless against privileged insider attacks and insider attacks. Additionally, we discovered a weakness in the password update stage and cannot guarantee patient privacy. So, utilizing biometrics and ECC, we suggest a robust mutual authentication system for TMIS security. In Table 1, we exhibit the analysis of existing works to highlight the features and Limitations.

3. Paper organization

The paper is organized using the following sections: Section 1 presents the requirement for Telecare Medical Information System. The Related works are discussed in Section 2. The paper organization is defined in Section 3. The review of Jongseok Ryu et al. protocol is presented in Section 4. Security limitations of Jongseok Ryu et al. protocol are discussed in Section 5. Suggestions to overcome these limitations by improving the protocol are given in Section 6. Concluding comments and the scope of this paper are presented in Section 7.

4. Brief review of Jongseok Ryu et al. scheme

We exhibit a review of Jongseok Ryu et al.'s [6] proposal. This protocol executes different phases like the initialization phase, patient registration phase, telecare server registration phase, login phase, authentication phase, and password update phase. The notations used in this article are summarized in Table 2.

4.1. Initialization section

In the initialization section, RC chooses an elliptic curve $E_p(r, s)$, a plane curve over a finite field F_p. Following that, a base point P is considered on $E_p(r, s)$ and also a private key k_{rc} is selected by RC. The following $E_p(r, s)$, P, $h(\bullet)$, $h_b(\bullet)$ are the parameters which are then published by RC.

4.2. Registration section

To exchange the services in between the patient U_i and the telecare server TS_j, both the units need to register with RC, which results in being part of the TMIS environment.

Table 2
List of notations in this paper.

Terms	Expansion
U_i	User
TS_j	Telecare Medical Server
SC	Smart card
RCI	Identity of RC
SID_j	TS_j's Identity
$PSID_i$	TS_j's Pseudo Identity
RC	Registration Center
ID_i	Identity of U_i
PID_i	Pseudo Identity of U_i
PW_i	Password of U_i
BI_i	Biometric information of U_i
MD_i	Mobile device of U_i
$n_1, n_2, R_j, RN_u, RN_{sj}$	Random Numbers
x, y, k_{rc}	RC's Private key
T_u, T_r, T_1, T_2	Timestamps
SK	RC's Session key
k_{sj}	TS_j's Private key
pk_{sj}	TS_j's Public key
mk	Master key of RC
$h_b(.)$	Biohash function
$h(.)$	Hash operation
E_k/D_k	Symmetric Cipher/decipher
$\oplus$	XOR operations
$\|$	concatenation operations

4.2.1. Patient registration

To utilize the medical facilities from TS_j, all the users U_i need to register in RC safely. The details are presented as follows: User (U_i) creates an identity (ID_i), a password (PW_i), the biometrics BI_i and creates RN_u a random no. Later, User U_i calculates $HID_i = h(ID_i \| RN_u)$, $HPW_i = h(PW_i \| h_b(BI_i))$, and $GPW_i = (HPW_i \oplus RN_u)$ and transfers the (HID_i, GPW_i) message to Registration Center through a secured communication path. Registration Center calculates $UR_i = h(HID_i \| k_{rc})$ and $B_i = UR_i \oplus GPW_i$. Afterwards, Registration Center safely keeps HID_i in the RC server and transfers B_i to User U_i. User U_i calculates $RPW_i = h(ID_i \| PW_i \| h_b(BI_i))$, $A_1 = RN_u \oplus RPW_i$, $A_2 = h(HID_i \| HPW_i \| RPW_i \| RN_u)$, and $A_3 = B_i \oplus RN_u = UR_i \oplus HPW_i$. Later, these computed entities (A_1, A_2, A_3) are stored by U_i into the memory of mobile device MD_i.

4.2.2. Telecare medical server registration

To provide medical facilities to the users U_i, TS_j should get registered in RC. As part of registration, TS_j chooses SID_j, an identity and RN_{sj}, a random number. Later, TS_j computes the pseudo-identity $PSID_j = SID_j \oplus RN_{sj}$ and transfers $PSID_j$, RN_{sj} to Registration Center via a safe communication channel. Registration Center calculates $SID_j = PSID_j \oplus RN_{sj}$ and keeps SID_j to RC database. Later, Registration Center extracts HID_i from its database and calculates $k_{sj} = h(SID_j \| k_{rc})$, $pk_{sj} = k_{sj} \bullet P$, $TID_i = h(HID_i \| pk_{sj})$, $UR_i = h(HID_i \| k_{rc})$, and $V_{ij} = h(PSID_j \| UR_i)$. Thereafter, RC makes $PSID_j, pk_{sj}$ public to all and transfers the parameters (k_{sj}, TID_i, V_{ij}) to TS_j. TS_j is de-

fined k_{sj} as a private key. Later, TS_j computes $SV_{ij} = V_{ij} \oplus h(SID_j \| k_{sj})$ and stores the parameters (TID_i, SV_{ij}) in the database.

4.3. Login phase

To access the application and utilize the medical facilities from the telecare medical server (TS_j), the users (U_i) need to accomplish the following steps: User U_i takes his Mobile device MD_i and enters ID_i, PW_i and BI_i. The mobile device MD_i performs computations, to compute $RPW_i = h(ID_i \| PW_i \| h_b(BI_i))$, $RN_u = A1 \oplus RPW_i$, $HID_i = h(ID_i \| RN_u)$, $HPW_i = h(PW_i \| h_b(BI_i))$, and $A_2^* = h(HID_i \| HPW_i \| RPW_i \| RN_u)$. MD_i checks whether $A_2^*? = A_2$. If there is a matching, move to the next step. If there is no matching, MD_i discards the login phase. MD_i chooses a random number n_1 along with a timestamp T_1. Later on, MD_i performs computations to $computeS_1 = n_1 \bullet P$, $S_2 = n_1 \bullet pk_{sj}$, $UR_i = A3 \oplus HPW_i$, $PID_i = h(HID_i \| pk_{sj}) \oplus h(PSID_j \| S_2), UID_i = h(h(HID_i \| pk_{sj}) \| h(PSID_j \| UR_i) \| T_1)$, and $M_i = h(UID_i \| S_2 \| h(PSID_j \| UR_i) \| T_1)$. Later, MD_i transfers (PID_i, M_i, S_1, T_1) to TS_j via an open communication channel.

4.4. Authentication phase

The Authentication between U_i and TS_j is performed by TS_j, utilizing the following procedure. TS_j checks the condition whether $\Delta T \geq |T_1^* - T_1|$. If the time is valid, TS_j computes $S_2 = k_{sj} \bullet S_1$ and $TID_i = h(HID_i \| pk_{sj}) = PID_i \oplus h(PSID_j \| S_2)$. Thereafter, TS_j retrieves SV_{ij} in its database corresponding to TID_i and computes $V_{ij} = SV_{ij} \oplus h(SIDj \| k_{sj})$, $UID_i = h(TID_i \| V_{ij} \| T_1)$, and $M_1^* = h(UID_i \| S_2 \| V_{ij} \| T_1)$. Next, TS_j checks the condition whether $M_i^*? = M_i$. If it has a match, TS_j assumes a random no. (n_2) and a timestamp T_2. At last, TS_j calculates $S_3 = n_2 \bullet P$, $S_4 = n_2 \bullet S_1$, $SK = h(UID_i \| S_2 \| S_4)$, $M_j = h(UID_i \| SK \| T_2)$ and transfers (M_j, S_3, T_2) to User U_i via an insecure communication route. Later getting the message (M_j, S_3, T_2) from TS_j, User U_i validates the timestamp T_2 with the condition $\Delta T_1 \geq |T_2^* - T_2|$. Then, User U_i computes $S_4 = n1 \bullet S_3$, $SK = h(UID_i \| S_2 \| S_4)$, $M_j^* = h(UID_i \| SK \| T_2)$, and verifies the condition $M_j^*? = M_j$. If a match is found, it means between User Ui and TSj, a mutual authentication and session key agreement has been created.

If there is a match, the mutual authentication and session key agreement have been initiated between User U_i and TS_j.

5. Security limitations of Jongseok Ryu et al

5.1. Adversary model

To perform security protocol analysis, we apply the "Dolev-Yao (DY) model" [56] in this research work. According to the DY model, an attacker can use an insecure channel to intercept, change, and delete the transmitted message. Below is a definition of an Attacker's capabilities.

- An Attacker may use forgery, impersonation, MITM Attack, etc. [57].
- Using power analysis, an adversary can access a legitimate patient's information stored on his mobile device [58,59].
- A legitimate patient or privileged individual could be an opponent at the registration desk, as an Attacker.

We take into account the "Canetti–Krawczyk (CK) model" [60], having a stronger hypothesis compared to the DY model. Using the CK approach, an attacker can compromise sensitive information, including the secret session key, master key, and private key credentials.

5.2. Message substitution attack

Under the CK Model, the Attacker can get the private key K_{rc} of RC. User sends the message (PID_i, M_i, S_1, T_1) to TS_j through insecure channel. we assume that Attacker gets the message (PID_i, M_i, S_1, T_1) and do the following computations in the minimum time accepted by the receiver. Attacker performs the computations by initially selecting the nonce $(n_1^{'})$ and then calculates $S_1^{'} = n_1^{'} \bullet p$, $S_2^{'} = n_1^{'} \bullet pk_{sj}$, $UR_i = h(HID_i \| K_{rc})$, where K_{rc} is under CK-Model and HID_i is under DY-Model. The value UR_i will be same as patient UR_i, but $S_1^{'}$, $S_2^{'}$ will change. $PID_i^{'} = h(HID_i \| pk_{sj}) \oplus h(PSID_j \| S_2^{'})$, where HID_i is under DY-Model, pk_{sj} and $PSID_j$ is the public information. $UID_i = h(h(HID_i \| pk_{sj}) \| h(PSID_j \| UR_i) \| T_1)$, $M_i^{'} = h(UID_i \| S_2^{'} \| h(PSID_j \| UR_i) \| T_1)$. Eventually, Attacker discards the user message and transmits the $(PID_i^{'}, M_i^{'}, S_1^{'}, T_1)$ to TS_j. TS_j calculates $S_2^* = k_{sj} \bullet S_1^{'}$, $TID_j = PID_i^{'} \oplus h(PSID_j \| S_2^{'})$. TS_j retrieves SV_{ij} corresponding to TID_i and then computes $V_{ij} = SV_{ij} \oplus h(SID_j \| k_{sj})$, $UID_i = h(TID_i \| V_{ij} \| T_1)$, $M_1^* = h(UID_i \| S_2^* \| V_{ij} \| T_1)$ and verifies $M_1^{*}? = M_1^{'}$. Later TS_j selects random number (N_2) and timestamp(T_2) and then it calculates $S_3 = N_2 \bullet P$, $S_4 = N_2 \bullet S_1^{'}$, $S_k = h(UID_i \| S_2^* \| S_4)$, $M_j = h(UID_i \| SK \| T_2)$ and later forwards (M_j, S_3, T_2). When Attacker receives (M_j, S_3, T_2) from open channel, it further calculates $S_4^{'} = N_1^{'} \bullet S_3$, $S_K^{'} = h(UID_i \| S_2^{'} \| S_4^{'})$ and $M_j^* = h(UID_i \| S_K^{'} \| T_2)$. Finally verifies $M_j^{*}? = M_j$.

5.3. Man-in-the-middle attack

As the patient uses an insecure channel to transmit the message (PID_i, M_i, S_1, T_1) to TS_j, we assume that the Attacker received the message (PID_i, M_i, S_1, T_1), and the Attacker performs the following computations in the shortest amount of time that the recipient will accept. The computations are carried out by the Attacker by initially choosing the nonce. $S_1^{'} = n_1^{'} \bullet p$, also computes $S_2^{'} = n_1^{'} \bullet pk_{sj}$, $UR_i = h(HID_i \| (K_{rc})$, where K_{rc} is from CK-Model and HID_i is from the DY-Model. The patient's UR_i value will remain the same, but S_1 and S_2 will change. $PID_i^{'} = h(HID_i \| pk_{sj}) \oplus h(PSID_j \| S_2^{'})$, where HID_i is under the DY-Model, pk_{sj}, and $PSID_j$ is the publicly available information.

5.4. Session key disclosure attack

The telecare server performs further computations to compute S_3, S_4, SK, and M_j, only when there is a proper authentication established between patient and telecare medical server and then the telecare server sends (M_j, S_3, T_2) to User through a public channel. But the Attacker tries to get M_j, S_3, T_2 from the insecure channel and attempts to compute $S_4^{'} = N_1^{'} \bullet S_3$, $S_K^{'} = h(UID_i \| S_2^{'} \| S_4^{'})$ and $M_j^* = h(UID_i \| S_K^{'} \| T_2)$ and finally verifies $M_j^{*}? = M_j$.

5.5. Privileged insider attack

As the patient uses an insecure channel to transmit the message (PID_i, M_i, S_1, T_1) to TS_j, we assume that the Attacker received the message (PID_i, M_i, S_1, T_1), and the Attacker performs the following computations in the shortest amount of time that the recipient will accept. The computations are carried out by the Attacker by initially choosing the nonce. $S_1^{'} = n_1^{'} \bullet p$, also computes $S2^{'} = n_1^{'} \bullet pk_{sj}$, $UR_i = h(HID_i \| (K_{rc})$, where K_{rc} is from CK-Model and HID_i is from the DY-Model. The patient's UR_i value will remain the same, but S_1 and S_2 will change. $PID_i^{'} = h(HID_i \| pk_{sj}) \oplus h(PSID_j \| S_2^{'})$, where HID_i is under the DY-Model, pk_{sj}, and $PSID_j$ is the publicly available information.

6. Proposal for enhancement

In the Adversary Model" Canetti–Krawczyk (CK) model [60], there is a chance for the adversary to pull out sensitive information, including the secret session key, private key, master key credentials. From the attacker model, it is clearly understood that the intruder will try to abstract the credentials to compromise the confidentiality, integrity and authenticity. If the attacker abstracts any clue related to credentials, the attacker can easily get the user credentials and create vulnerabilities by

accessing the Remote server. To prevent the attacker from abstracting the credentials, we employ the ECC based cryptosystem. In this cryptosystem, ECC based point multiplication is used. From Sender A_1, the private key of sender (Pr_A) is point multiplied with the public key of the receiver (Pu_B), which results in generation of two coordinates (A_x, A_y) with the help of a generator function. The same set of operations occur on the other side of the receiver, resulting in (B_x, B_y). If the verification results on both sides as $(A_1 = B_1)$ and if the result has a matching, it means that attacker is unable to guess the credentials and failed to perform attacks. If there is a mismatch, it means that attacker has modified the data.

To witness this solution, we can follow the below steps:

Step 1: We consider the encryption from sender A_1 with a private key of A as $A_1 = (Pr_A \bullet Pu_B)$ and this can be evaluated as $A_1 = Pr_A \bullet (Pr_B \bullet G)$, which generates two coordinates (A_x, A_y).

Step 2: We consider the encryption from receiver B_1 with a private key of B as $B_1 = (Pr_B \bullet Pu_A)$ and this can be written as $B_1 = Pr_B \bullet (Pr_A \bullet G)$, which generates two coordinates (B_x, B_y).

Step 3: When the computations are evaluated correctly on both the sender(A_1) and receiver (B_1), then the verification should result in $(A_1) = B_1)$. And if there is a match, then it indicates that the attacker is unable to guess the credentials required to perform the attacks.

Note: By implementing the above-mentioned solution in the current protocol we can assume that $A = (Pr_A \bullet Pu_B)$, which generates two points on the curve as (A_x, A_y) and we get $S_1 = n_1 \bullet p$ and then based on this value we get $M_1 = h(UID_i \parallel S_2^* \parallel V_{ij} \parallel A_x \parallel T_1)$. In M_1, If the attacker is unable to guess the exact value of A_x, then there is no possibility for the attacker to compute the exact coordinates to perform an attack, and the same thing is applicable on the receiver side as well.

7. Concluding remarks

In the current paper, we initially reviewed Jongseok Ryu et al.'s recently published Three Factor Mutual Authentication Protocol for TMIS based on ECC. Later, we have shown that their proposal is defenseless to session key disclosure attack, MITM attack, Message Substitution attack, stolen verifier attack and privileged insider attack which results in insecurity to the application. In this paper, we have projected the loopholes by performing the cryptanalysis on the Jongseok Ryu et al. proposal, and we have also addressed the suggestions for the improvement of the protocol. We are proposing an authentication protocol to prevent the above mentioned security threats in the near future.

Declaration of Competing Interest

Authors declare that they have no conflict of interest.

References

[1] C.-L. Hsu, T.-V. Le, M.-C. Hsieh, K.-Y. Tsai, C.-F. Lu, T.-W. Lin, Three-factor UC-SSO scheme with fast authentication and privacy protection for telecare medicine information systems, IEEE Access 8 (2020) 196553–196566.

[2] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191.

[3] S.S. Sahoo, S. Mohanty, B. Majhi, A secure three factor based authentication scheme for health care systems using IoT enabled devices, J. Ambient Intell. Humaniz. Comput. 12 (1) (2021) 1419–1434.

[4] S. Shamshad, M.F. Ayub, K. Mahmood, S. Kumari, S.A. Chaudhry, C.-M. Chen, An enhanced scheme for mutual authentication for healthcare services, Digit. Commun. Netw. 8 (2) (2022) 150–161.

[5] M. Tanveer, A. Alkhayyat, S.A. Chaudhry, Y.B. Zikria, S.W. Kim, et al., REAS-TMIS: resource-efficient authentication scheme for telecare medical information system, IEEE Access 10 (2022) 23008–23021.

[6] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, Y. Park, Secure ECC-based three-factor mutual authentication protocol for telecare medical information system, IEEE Access 10 (2022) 11511–11526.

[7] C.S. Nayak, et al., An improved user authentication scheme for electronic medical record systems, Multimed. Tools Appl. 79 (29) (2020) 22007–22026.

[8] R. Madhusudhan, C.S. Nayak, A robust authentication scheme for telecare medical information systems, Multimed. Tools Appl. 78 (11) (2019) 15255–15273.

[9] K. Renuka, S. Kumari, X. Li, Design of a secure three-factor authentication scheme for smart healthcare, J. Med. Syst. 43 (5) (2019) 1–12.

[10] M.K. Khan, S. Kumari, An authentication scheme for secure access to healthcare services, J. Med. Syst. 37 (4) (2013) 1–12.

[11] D. Giri, T. Maitra, R. Amin, P.D. Srivastava, An efficient and robust RSA-based remote user authentication for telecare medical information systems, J. Med. Syst. 39 (1) (2015) 1–9.

[12] R. Amin, G.P. Biswas, An improved RSA based user authentication and session key agreement protocol usable in TMIS, J. Med. Syst. 39 (8) (2015) 1–14.

[13] A.K. Sutrala, A.K. Das, V. Odelu, M. Wazid, S. Kumari, Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems, Comput. Methods Progr. Biomed. 135 (2016) 167–185.

[14] L. Zhang, S. Zhu, Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems, J. Med. Syst. 39 (5) (2015) 1–11.

[15] W. Liu, Q. Xie, S. Wang, B. Hu, An improved authenticated key agreement protocol for telecare medicine information system, SpringerPlus 5 (1) (2016) 1–16.

[16] A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications, J. Med. Syst. 43 (1) (2019) 1–22.

[17] S. Kumari, P. Chaudhary, C.-M. Chen, M.K. Khan, et al., Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications, IEEE Access 7 (2019) 39717–39720.

[18] M. Burrows, M. Abadi, R.M. Needham, A logic of authentication, Proc. R. Soc. Lond. A 426 (1871) (1989) 233–271.

[19] M. Abdalla, P.-A. Fouque, D. Pointcheval, Password-based authenticated key exchange in the three-party setting, in: International Workshop on Public key Cryptography, Springer, 2005, pp. 65–84.

[20] J. Lee, G. Kim, A.K. Das, Y. Park, Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks, IEEE Trans. Netw. Sci. Eng. 8 (3) (2021) 2412–2425.

[21] J. Srinivas, A.K. Das, M. Wazid, A.V. Vasilakos, Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system, IEEE Internet Things J. 8 (9) (2020) 7727–7744.

[22] Y. Lu, L. Li, H. Peng, Y. Yang, An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem, J. Med. Syst. 39 (3) (2015) 1–8.

[23] R. Amin, S.K.H. Islam, P. Gope, K.-K.R. Choo, N. Tapas, Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system, IEEE J. Biomed. Health Inform. 23 (4) (2018) 1749–1759.

[24] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, J. Ma, Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems, J. Ambient Intell. Humaniz. Comput. 9 (4) (2018) 1061–1073.

[25] N. Ravanbakhsh, M. Nazari, An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems, Multimed. Tools Appl. 77 (1) (2018) 55–88.

[26] A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC, Int. J. Commun. Syst. 32 (5) (2019) e3913.

[27] M. Qi, J. Chen, New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography, Multimed. Tools Appl. 77 (18) (2018) 23335–23351.

[28] S.S. Sahoo, S. Mohanty, B. Majhi, Improved biometric-based mutual authentication and key agreement scheme using ECC, Wirel. Pers. Commun. 111 (2) (2020) 991–1017.

[29] X. Zeng, G. Xu, X. Zheng, Y. Xiang, W. Zhou, E-AUA: an efficient anonymous user authentication protocol for mobile IoT, IEEE Internet Things J. 6 (2) (2018) 1506–1519.

[30] S. Mandal, B. Bera, A.K. Sutrala, A.K. Das, K.-K.R. Choo, Y. Park, Certificateless-signcryption-based three-factor user access control scheme for IoT environment, IEEE Internet Things J. 7 (4) (2020) 3184–3197.

[31] M. Shuai, B. Liu, N. Yu, L. Xiong, Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks, Secur. Commun. Netw. 2019 (2019) 1–15.

[32] J. Mo, Z. Hu, Y. Lin, Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks, Secur. Commun. Netw. 2020 (2020) 1–11.

[33] M. Fotouhi, M. Bayat, A.K. Das, H.A.N. Far, S.M. Pournaghi, M.-A. Doostari, A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT, Comput. Netw. 177 (2020) 107333.

[34] H. Taleb, A. Nasser, G. Andrieux, N. Charara, E. Motta Cruz, Wireless technologies, medical applications and future challenges in WBAN: a survey, Wirel. Netw. 27 (8) (2021) 5271–5295.

[35] J. Li, Z. Su, D. Guo, K.-K.R. Choo, Y. Ji, PSL-MAAKA: provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things, IEEE Internet Things J. 8 (17) (2021) 13183–13195.

[36] M.A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar, K. Mahmood, Security analysis on 'a secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems', IEEE Syst. J. 15 (4) (2021) 5557–5559.

[37] X. Xia, S. Ji, P. Vijayakumar, J. Shen, J.J. Rodrigues, An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities, Int. J. Distrib. Sens. Netw. 17 (6) (2021). 15501477211026804

[38] P. Vijayakumar, M.S. Obaidat, M. Azees, S.K.H. Islam, N. Kumar, Efficient and secure

anonymous authentication with location privacy for IoT-based WBANs, IEEE Trans. Ind. Inf. 16 (4) (2019) 2603–2611.
[39] C.M. Kumar, R. Amin, M. Brindha, Cryptanalysis and improvement of REAS-TMIS: resource-efficient authentication scheme for telecare medical information system, Secur. Privacye 6 (1) (2023) e268 Security and Privacy, Wiley.
[40] K. Prateek, F. Altaf, R. Amin, S. Maity, A privacy preserving authentication protocol using quantum computing for V2I authentication in vehicular ad hoc networks, Secur. Commun. Netw. 2022 (2022) 1–17.
[41] X. Li, T. Liu, M.S. Obaidat, F. Wu, P. Vijayakumar, N. Kumar, A lightweight privacy-preserving authentication protocol for VANETs, IEEE Syst. J. 14 (3) (2020) 3547–3557.
[42] P. Yu, W. Ni, G. Yu, H. Zhang, R.P. Liu, Q. Wen, Efficient anonymous data authentication for vehicular ad hoc networks, Secur. Commun. Netw. 2021 (2021) 1–14.
[43] T.-Y. Wu, Z. Lee, L. Yang, C.-M. Chen, A provably secure authentication and key exchange protocol in vehicular ad hoc networks, Secur. Commun. Netw. 2021 (2021) 1–17.
[44] S. Olariu, A survey of vehicular cloud research: trends, applications and challenges, IEEE Trans. Intell. Transp. Syst. 21 (6) (2019) 2648–2663.
[45] S. Kona, S.V.K.R. Morthala, R. Konathala, P.K. Pinninti, H.K. Mavuru, A. Maria, An efficient key agreement and anonymous mutual authentication protocols for secure communication in VANETs, in: 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC), IEEE, 2022, pp. 146–151.
[46] O. Galindo, V. Kreinovich, O. Kosheleva, Current quantum cryptography algorithm is optimal: a proof, in: 2018 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, 2018, pp. 295–300.
[47] C. Ottaviani, M.J. Woolley, M. Erementchouk, J.F. Federici, P. Mazumder, S. Pirandola, C. Weedbrook, Terahertz quantum cryptography, IEEE J. Sel. Areas Commun. 38 (3) (2020) 483–495.
[48] Y. Li, P. Zhang, R. Huang, Lightweight quantum encryption for secure transmission of power data in smart grid, IEEE Access 7 (2019) 36285–36293.
[49] D. Jin, P. Verma, S. Kartalopoulos, Key distribution using dual quantum channels, in: 2008 The Fourth International Conference on Information Assurance and Security, IEEE, 2008, pp. 327–332.
[50] P. Bagga, A.K. Das, J.J. Rodrigues, Bilinear pairing-based access control and key agreement scheme for smart transportation, Cyber Secur. Appl. 1 (2023) 100001.
[51] W. Yan, S. Ji, A secure and efficient DSSE scheme with constant storage costs in smart devices, Cyber Secur. Appl. 1 (2022) 100006.
[52] L. Zhang, S. Zhu, S. Tang, Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme, IEEE J. Biomed. Health Inform. 21 (2) (2016) 465–475.
[53] S. Qiu, G. Xu, H. Ahmad, L. Wang, A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems, IEEE Access 6 (2017) 7452–7463.
[54] S.A. Chaudhry, H. Naqvi, M.K. Khan, An enhanced lightweight anonymous biometric based authentication scheme for TMIS, Multimed. Tools Appl. 77 (5) (2018) 5503–5524.
[55] S.A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A.K. Bashir, Y.B. Zikria, GCAC-S-IoD: a certificate based generic access control scheme for internet of drones, Comput. Netw. 191 (2021) 107999.
[56] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29 (2) (1983) 198–208.
[57] D. Kwon, Y. Park, Y. Park, Provably secure three-factor-based mutual authentication scheme with PUF for wireless medical sensor networks, Sensors 21 (18) (2021) 6039.
[58] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, Y. Park, A secure and lightweight authentication protocol for IoT-based smart homes, Sensors 21 (4) (2021) 1488.
[59] S. Yu, N. Jho, Y. Park, Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes, IEEE Access 9 (2021) 126186–126197.
[60] R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 337–351.

C Madan Kumar received the B.Tech. degree in Computer Science and Engineering from Dr. Paul Raj Engineering College (JNT University), Hyderabad, India, in the year 2004, M.Tech. degree in Software Engineering from Vaagdevi College of Engineering (JNTUniversity, Hyderabad) India, in the year 2012 and also pursuing his Ph.D. degree from NIT Tiruchirappalli. He is working as Assistant Professor in the Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal, Telangana, India. His areas of interest include Multimedia Security, Cryptography and Network Security, Cryptanalytic attacks, Authentication Protocols, WSN Security, IoT Security and Image Security.

Ruhul Amin received doctoral (Ph.D.) degree in Computer Science and Engineering from the Indian Institute of Technology(ISM) Dhanbad, Jharkhand, India, in 2017. Dr. Amin received B.Tech and M.Tech both in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2009 and 2013, respectively. Presently, he is working as an Assistant Professor in the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. He has authored many technical research papers published in leading international conferences and peer reviewed international journals from the IEEE, Elsevier, Springer, John Wiley, etc. Some of his research findings are published in top cited journals such as IEEE Transactions on cloud computing, IEEE Transaction on Consumer Electronics, IEEE Internet of Things, IEEE System Journal, Ad-Hoc Networks, Computer Networks, Future Generation Computer Science, Journal of Network and Computer Application of Elsevier. He is also serving as Associate Editor of 'Security and Privacy Journal' published by John Wiley. He has been included in the subject-wise ranking of top 2 percent scientists from India (all fields) in the area of Networking & Telecommunications. His research interest includes Cryptography and Network Security, Authentication protocol, WSN Security, IoT Security and blockchain technology.

Dr. M. Brindha was born in Nagercoil, Tamil Nadu, India, in 1983. She received her B.E. degree from Dr. SivanthiAditanar College of Engineeing, Tiruchendur, India in the year of 2004; and her M. E. Degree from Government College of Engineering, Tirunelveli, India in the year of 2006. She received her Ph.D. degree from National Institute of Technology, Tiruchirappalli, in 2016. From February 2009 onwards she is working as an Assistant Professor in the Department of Computer Science and Engineering, National Institute of Technology Tiruchirappalli, Tamilnadu, India. Her areas of interest include Multimedia security, Cryptanalytic attacks, Multimedia compression.