Received: 1 February 2019 | Accepted: 1 March 2019

DOI: 10.1002/spy2.67

ORIGINAL ARTICLE

WILEY

Security analysis on "mutual authentication scheme for multimedia medical information systems"

Marimuthu Karuppiah[1] | **Mohammad S. Obaidat**[2,3,4,5] | **SK Hafizul Islam**[6] | **Pandi Vijayakumar**[7]

[1] School of Computing Science and Engineering, Vellore Institute of Technology, Vellore, India
[2] ECE Department, Nazarbayev University, Astana, Kazakhstan
[3] KAIST, University of Jordan, Amman, Jordan
[4] University of Science and Technology, Beijing, China
[5] Amity University, Noida, India
[6] Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, Kalyani, India
[7] Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, India

Correspondence
Mohammad S. Obaidat, Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, Webel IT Park Campus, West Bengal 741235, India.
Email: msobaidat@gmail.com
SK Hafizul Islam, Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, Kalyani, West Bengal 741235, India.
Email: hafi786@gmail.com

In this paper, the security of a mutual authentication scheme is analyzed. We discern three different attacks in various scenarios. Moreover, we also identify some inherent design flaws of the scheme. As the scheme is suffering from many threats, therefore we argue that the scheme does not have strong characteristics against attacks for practical applications.

KEYWORDS

medical information system, multimedia, replay attack, user anonymity, user impersonation attack

1 | INTRODUCTION

Multimedia medical information system (MMIS) is changing the face of remote healthcare by delivering medical services at the user's doorstep. Affordable services, efficient personnel utilization, and high availability are few of the key motivation factors for developing MMIS. In a typical MMIS scenario, which is depicted in Figure 1, a registered user sends his/her medical data, in the form of an electronic medical record (EMR), over the Internet to the medical server. The EMR's are then accessed by the concerned medical professional, who then performs diagnosis based on the user's symptoms. It should be noted that the various entities of the MMIS system may be geographically dispersed. The doctor views the EMR sent by the patient and sanctions the necessary tests. The laboratory is then allowed access to the EMR and uploads the results of the test performed. The doctor then prescribes the medical care to the patient. The manager is responsible for the performance, integrity, and security of the medical server. MMIS also opens the door for identifying trends among the various medical records using data analytics thus, providing swifter and more precise care.

Mohammad S. Obaidat is Fellow of IEEE and Fellow of SCS.

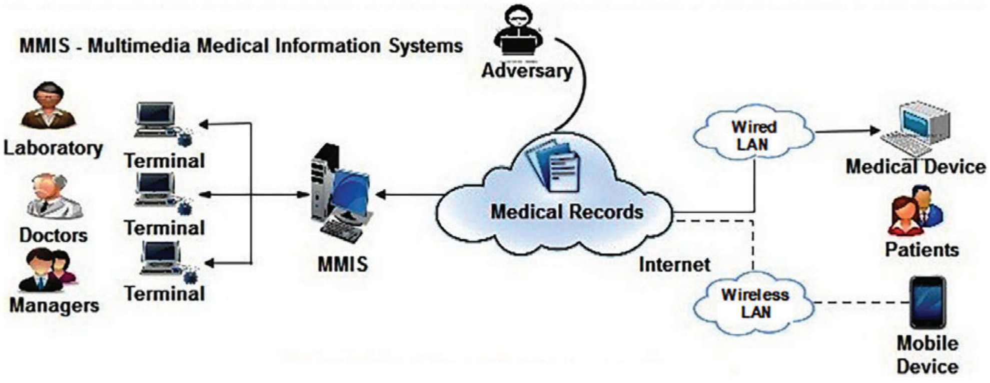

FIGURE 1 Overview of a Multimedia medical information system (MMIS)

However, the communication is taking place between the various entities of the MMIS over the public channels, where any adversary can monitor the channel. Furthermore, the medical server itself maintains the patient's medical records. This raises several security concerns such as data privacy, data security, message integrity, user anonymity, unauthorized access, etc. Password authentication schemes are considered the de-facto approach to resolve the aforementioned concerns. Many researcher's employ various cryptographic algorithms to design secure authentication protocols. Examples of such cryptographic algorithms are noninvertible one-way hash function,[1–3] chaotic maps,[4–6] elliptic curve cryptosystem (ECC),[1,7–10] RSA,[11] discrete logarithmic problem (DLP)[3] and other operations such as XOR and concatenation. Additionally, methodologies such as usage of smartcard,[1,2,12,13] two-factor[7–9] or three-factor (involving biometrics)[1,4,5,13] authentication, etc. are used to further strengthen the protocol.

1.1 | Related works

In 2010, Wu et al[3] devised an authentication scheme for medical information system based on DLP. They considered a precomputation phase, which handled the computationally expensive operations, thus greatly increasing the performance. However, in 2011, He et al[14] cryptanalyzed that the scheme by Wu et al[3] is defenseless against the impersonation attack and insider attack, and then designed a new scheme. Wei et al[15] revealed that both the schemes by Debiao et al[14] and Wei et al[15] are vulnerable to off-line password guessing attack, when the information stored in the smartcard is disclosed, and, thus fail to achieve two-factor authentication. Wei et al[15] then proposed a new authentication scheme for medical information systems. Later on, Wu and Xu[16] designed an authentication scheme, which is an improvement of Jiang et al's scheme.[17] Mishra and Mukhopadhyay[18] in 2013 showed that the scheme by Wu and Xu[16] is susceptible to off-line password guessing attacks and incapable to offer the property of user anonymity.

Jiang et al[6] showed that the scheme by Hao et al[19] can be forged against the smartcard-stolen attack. To overcome this problem, they devised a chaotic-map based authentication scheme. Amin et al[20] in 2015 cryptanalyzed that the scheme by Lu et al[21] is insecure against user anonymity, new smartcard issue attack, patient and medical server impersonation attacks. They have then designed an enhanced scheme using smartcard and ECC. Das[22] in the same year analyzed the schemes by Tan[23] and Arshad and Nikooghadam,[24] and found out that they both have several security loopholes. Das[22] then proposed a new three-factor protocol with higher computational cost than previous schemes. Mishra[25] in 2015 pointed out security flaws in the schemes by Lee[26] and Xu et al.[27] Wazid et al[28] scrutinized the recently proposed three-factor user authentication scheme of Amin and Biswas[1] and observed that their scheme is insecure against privileged-insider, offline password guessing, strong replay, and user impersonation attacks. Wazid et al[28] then proposed a new scheme that provided user unlinkability and anonymity properties.

1.2 | Contribution and motivation

We have studied the mutual authentication schemes proposed in References [1–28] Unfortunately, these schemes are often found to be vulnerable to attacks such as replay attack, password guessing attack, user impersonation attack, privileged insider attack, etc. Moreover, they have been often found to be unable to provide essential security features like forward secrecy, backward secrecy, user anonymity, known session key, mutual authentication, among others.

Recently, David[29] proposed another authentication scheme for multimedia information systems (MIS) based on bilinear pairings. The author further employs BAN logic[13] to validate that the proposed protocol provides the required security features of a MMIS. Here, we cryptanalyzed that David's scheme[29] is susceptible to replay, privileged insider, and known session-specific temporary information attack. Moreover, the protocol does not offer the property of user anonymity and fails to achieve proper mutual authentication. The scheme also has several inherent design weaknesses.

TABLE 1 Notations

Nomenclature	Definition
S	Server
C	Client
S_p	Security parameter
q	Prime order
Se_k	Master Key
PU_k	Public Key
r_k	Random number
C_{ID}	Identity of C
PR_k	Private key
M_{key}	Session key
P	Generator of G_1
G_1, G_2	Cyclic groups
e	Bilinear map

1.3 | Roadmap

The remaining part of the paper is arranged in the following way. In Section 2, we examine the mathematical concepts and assumptions of a mutual authentication system. In Sections 3 and 4, we provide a brief overview of David's protocol,[29] and discuss its design flaws. In Section 5, we analyze the David's protocol[29] and identify its weaknesses. Finally, Section 6 concludes the paper.

2 | PRELIMINARIES

Assume that G_1 is an additive cyclic group of order q (a large prime number) of elliptic curve points and P is its generator. Also assume that G_2 is a multiplicative cyclic group with same order q. Therefore, the bilinear mapping is with the subsequent properties.

- *Bilinearity:* $e(c \cdot P, d \cdot Q) = e(P, Q)^{cd}$, where $P, Q \in G_1$ and $c, d \in Z_q^*$.
- *Non-degeneracy:* $e(P, P) \neq 1_{G_1}$, where 1_{G_1} is the identity element of G_1.
- *Computability:* An efficient and polynomial-time algorithm must exist, which can calculate $e(P, Q)$ for all $P, Q \in G_1$.
- *Computational Diffe Hellman problem (CDHP):* Given $(P, c \cdot P, d \cdot P)$ for any $c, d \in Z_q^*$, computation of $c \cdot d \cdot P$ is hard.
- *Collision attack assumption:* Given $\{n \in Z_q^*, y \in Z_q^*, Z \in G_1, y \cdot Z \in G_1\}$, $\{f_1, f_2, \ldots, f_n\} \in Z_q^*$, and $\left\{\frac{1}{y+f_1} \cdot Z, \frac{1}{y+f_2} \cdot Z, \cdots, \frac{1}{y+f_n} \cdot Z\right\} \in G_1$, computation of $\frac{1}{y+f}$ is hard,[30] where $f \notin \{f_1, f_2, \ldots, f_n\}$.

3 | REVIEW OF DAVID'S SCHEME

In this section, we discuss briefly David's scheme for MIS.[29] The scheme has three phases: (a) client setup, (b) key generation, and (c) mutual authentication. The notations used in David's scheme are given in Table 1.

- *Client setup:* S initially selects the security parameter S_p. S does:

1. an additive cyclic group G_1 of prime order q and its generator Z,
2. a multiplicative cyclic group G_2 of prime order q,
3. a bilinear mapping $e : G_1 \times G_2 \rightarrow G_2$.
4. choose $G = e(Z, Z) \in G_2$.
5. choose the master key Se_k randomly from Z_q^* and computing the public key as $PU_k = Se_k \cdot Z$.
6. choose hash functions H_1: $\{0,1\}^* \times G_1 \rightarrow Z_q^*$, H_2: $G_1 \times \{0,1\}^* \times Z_q^* \times G_1 \rightarrow Z_q^*$, H_3: $\{0,1\}^* \times Z_q^* \times G_1 \times Z_q^* \times G_1 \rightarrow Z_q^*$, $H_4 : Z_q^* \times \{0,1\}^* \times Z_q^* \times G_1 \times G_1 \rightarrow Z_q^*$.

Hence, S accepts $\{G_1, G_2, e, Z, PU_k, g, H_1, H_2, H_3, H_4\}$ as public parameters.

- *Key generation:* To compute the partial-private-key, S and C execute as follows:

1. S selects a random number $r_k \in Z_q^*$, and performs $U_r = r_k \cdot Z$ and $H_r = H_1(C_{ID}, U_r)$, where C_{ID} is the identity of C.
2. S computes the private key of U_r as $PR_k = r_k + Se_k \cdot H_r \bmod q$.
3. S delivers the U_r via offline approach and PR_k via online approach to the C.[31]

- *Mutual authentication:* The purpose of this phase is to establish a session key M_{key} between C and S. The procedure is described in detail as follows:

1. C chooses a number r_c randomly from Z_q^*, and determines $M = r_c \cdot Z$ and $U_1 = r_c \cdot PU_k$. C then sends $msg_1 = \{C_{ID}, M\}$ to S over a public channel.
2. S receives msg_1, and performs the computation of $U_2 = Se_k \cdot M$. The server S then chooses a number α randomly from Z_q^* and calculates $A_u = H_2(PU_k, C_{ID}, \alpha, U_2)$ and $h = H_3(C_{ID}, \alpha, M, A_u, PU_k)$. Finally, S transmits $msg_2 = \{\alpha, A_u\}$ to C over a public channel.
3. After receiving msg_2, C checks whether $A_u = ?H_2(PU_k, C_{ID}, \alpha, U_1)$. If the condition holds, a session key $M_{key} = H_4(PU_k, C_{ID}, \alpha, M, U_1)$ is computed. Moreover, C also derives $V_r = \frac{1}{h+PR_k} \cdot Z$ and transmits $msg_3 = \{U_r, V_r\}$ to S over a public channel.
4. S receives msg_3 and invokes the computation of $H_r = H_1(C_{ID}, PR_k)$ to verify whether $e(V_r, h \cdot Z + PR_k + H_r \cdot PU_k)$ equates to g. If it does, a session key $M_{key} = H_4(PU_k, C_{ID}, \alpha, M, U_2)$ is computed.

The proof of the verification process is depicted as follows. Since $U_2 = Se_k \cdot M = Se_k \cdot r_c \cdot Z = r_c \cdot Se_k \cdot Z = r_c \cdot PU_k = U_2$. Moreover,

$$
\begin{aligned}
& e(V_r, h \cdot Z + PR_k + H_r \cdot PU_k) = e\left(\left(\frac{1}{h + PR_k}\right) \cdot Z, h \cdot Z + PR_k + H_r \cdot PU_k\right) \\
& = e\left(\left(\frac{1}{h + PR_k}\right) \cdot Z, h \cdot Z + r_k \cdot Z + H_r \cdot Se_k \cdot Z\right) \\
& = e\left(\left(\frac{1}{h + PR_k}\right) \cdot Z, (h + r_k + H_r \cdot Se_k) \cdot Z\right) \\
& = e\left(\left(\frac{1}{h + PR_k}\right) \cdot Z, (h + PR_k) \cdot Z\right) \\
& = g
\end{aligned}
$$

4 | INHERENT DESIGN FLAWS

The scheme presented in Reference [29] strives to augment the security features of MIS via bilinear pairings. However, we find that the scheme is inefficient in providing the required features, mainly due to the following design flaws:

- *Ambiguity of H_r:* Note that H_r is computed as $H_1(C_{ID}, U_r)$ in Step 1 of key generation phase whereas, it is computed as $H_1(C_{ID}, PR_k)$ in Step 4 of mutual authentication phase.

Remark 1. If this is not attributed to a printing oversight, then the key generator verification, $e(V_r, h \cdot Z + PR_k + H_r \cdot PU_k) = g$ fails as follows: Let $H_{r_1} = H_1(C_{ID}, U_r)$ and $H_{r_2} = H_1(C_{ID}, PR_k)$ then, $PR_k = r_k + Se_k \cdot H_{r_1} \bmod q$ and,

$$
\begin{aligned}
& e\left(\left(\frac{1}{h + PR_k}\right) \cdot Z, (h \cdot Z + r_k \cdot Z + H_{r_2} \cdot PU_k\right) \\
& = e\left(\left(\frac{1}{h + r_k + Se_k \cdot H_{r_1} \bmod q}\right) \cdot Z, (h + r_k + H_{r_2} \cdot Se_k) \cdot Z\right) \\
& \neq g
\end{aligned}
$$

This results in a Denial-of-Service (DoS) attack.

- *PR_k substituted by U_r:* Note that PR_k is substituted by $U_r = r_k \cdot Z$ in the key generator verification process.

Remark 2. Let us presume that $H_r = H_1(C_{ID}, U_r)$ and that PR_k being substituted by U_r is a printing error, then the key generator verification fails as follows:

$$\begin{aligned} & e\left(\left(\frac{1}{h+PR_k}\right)\cdot Z, h\cdot Z + PR_k + H_{r_2}\cdot PU_k\right) \\ & = e\left(\left(\frac{1}{h+PR_k}\right)\cdot Z, h\cdot Z + r_k + Se_k\cdot H_r \bmod q + H_{r_2}\cdot Se_k\cdot Z\right) \\ & \neq g. \end{aligned}$$

Thus the verification fails and results in a DoS attack.

- *Omission of mod q operation:* Note that mod q is absent from the term $H_r \cdot Se_k$ during the key generator verification process.

Remark 3. Let us assume that U_r is the apparent term in the generator verification process as alluded to in

Remark 4. Then the verification process follows as:

$$\begin{aligned} & e\left(\left(\frac{1}{h+PR_k}\right)\cdot Z, (h + r_k + H_r\cdot Se_k)\cdot Z\right) \\ & = e\left(\left(\frac{1}{h + r_k + H_r\cdot Se_k \bmod q}\right)\cdot Z, (h + r_k + H_r\cdot Se_k)\cdot Z\right). \end{aligned}$$

Now, if we presume that $H_r \cdot Se_k > q$ then, $H_r \cdot Se_k \bmod q = H_r \cdot Se_k$ and thus the verification holds. Otherwise, the verification fails, resulting in a DoS attack.

5 | CRYPTANALYSIS OF DAVID'S SCHEME

In this section, we will analyze David's scheme for MIS. We analyzed the scheme in Reference [29] based on the following assumptions[32]:

Assumption 1. The attacker has full knowledge about the hash functions and can compute digest of it for a given input.

Assumption 2. The attacker can eavesdrop on all communication between C and S.

5.1 | Replay attack

In David's scheme,

1. The message $msg_1 = \{C_{ID}, M\}$ is sent as plaintext between C and S over a public channel.
2. S has no means to check whether the integer r_c, used to compute $M = r_c \cdot Z$ is actually fresh or not as there is no use of timestamps.

We assume that the attacker is $\mathscr{A}$, intercepts and stores the messages transmitted between C and S for a particular session such as $msg_1 = \{C_{ID}, M\}$. C_a then replays the message $msg_1 = \{C_{ID}, M\}$ to S. As the S has no way to know whether msg_1 is replayed by $\mathscr{A}$ in accordance with Assumption 2, it authenticates $\mathscr{A}$ as a legal client and send $msg_2 = \{\alpha, A_u\}$. Thus, David's scheme is vulnerable to partial-replay attack.

Remark 5. Furthermore, we assume that message msg_1 of the previous session is stored at S. After getting a new authentication request message from C, S verifies the current authentication request message against the previously stored authentication request messages. If they are the same, S terminates the current session to avoid replay attack. Assume that an attacker $\mathscr{A}$ traps the authentication request message for some sessions $S_1, S_2, \dots, S_m$ with $S_1 < S_2 < \cdots < S_m$, where $S_i < S_j$ means S_i is an earlier session than S_j. Suppose $\mathscr{A}$ obtains an authentication request message from any old sessions $\{S_1, S_2, \dots S_{m-1}\}$ and replays to S in the current session, say S_{m+1}. Thus, S rejects the login request of $\mathscr{A}$. To resist this kind of replay attack in David's scheme, the sever S would have to keep all the old messages of previous session for all the clients and then check it against the login request received in the current session. This is not at all an efficient approach to detect the replay attack as the server would be busy searching and comparing the messages.

5.2 | User anonymity

The client identity C_{ID} is transmitted as plaintext in the mutual authentication request message $msg_1 = \{C_{ID}, M\}$. Therefore, an adversary $\mathscr{A}$ can identify a particular C_{ID} (By using statistical analysis of message msg_1 in different sessions) and misuse it to track a particular users login history. Hence, David's scheme fails to provide the property of user anonymity.

5.3 | Privileged-insider attack

The variables C_{ID}, Ur, PR_k are stored in the database of the Home Subscriber Server (HSS). Suppose that the HSS admin is malicious. He can then misuse the stored variables to authenticate as a legal user as briefly described below.

- He chooses a r^* randomly from Z_q^* and computes $M^* = r^* \cdot Z$ and $U_1^* = r^* \cdot P_{Uk}$. He then sends $msg_1^* = \{C_{ID}, M^*\}$.
- As S does not detect any abnormality, it performs its computations and sends $msg_2^* = \{\alpha^*, A_u^*\}$ to the adversary $\mathscr{A}$.
- $\mathscr{A}$ then computes $h^* = H_3(C_{ID}, \alpha^*, M^*, A_u^*, PU_k)$ and derives $V_r^* = \left(\frac{1}{h^*+PR_k}\right) \cdot Z$. $\mathscr{A}$ then also computes $M_{key}^* = H_4(P_{Uk}, C_{ID}, \alpha^*, M^*, U_1^*)$ and sends $msg_3^* = \{U_r, V_r^*\}$ to S.
- Upon receiving msg_3, S verifies whether $e(V_r, h \cdot Z + PR_k + H_r \cdot PU_k) = g$. As there is no irregularity, S then computes $M_{key} = H_4(PU_k, C_{ID}, \alpha, M, U_2)$. Thus, the malicious admin is validated as a legal user by server. Hence, David's scheme is vulnerable to privileged insider attack.

5.4 | Known session-specific temporary information attack

The security of the session key computed in David's scheme depends on the secrecy of random number r_c as discussed by Canetti and Krawczyk.[33] Let us assume the realistic scenario that r_c is leaked for a specific session. An adversary $\mathscr{A}$ can then derive $U_1 = r_c \cdot Z$. Moreover, $\mathscr{A}$ can also deduce $M_{key} = H4(PU_k, C_{ID}, \alpha, M, U_1)$ by trapping $msg_1 = \{C_{ID}, M\}$ and $msg_2 = \{\alpha, A_u\}$. Thus, the security of the session key is compromised. Hence, David's scheme cannot avoid the known session-specific temporary information attack.

5.5 | Fails to achieve proper mutual authentication

Mutual authentication schemes generally allow the client and server to securely communicate with each other by establishing a common session key. David's scheme claimed that it provides the mutual authentication property. However, David's scheme is vulnerable to some popular attacks such as replay attack and privileged insider attack, as discussed in Sections 5.1 and 5.3. Thus, these two attacks break the mutual authentication of David's scheme. Hence David's scheme is unsuccessful to provide proper mutual authentication property.

6 | CONCLUSION

In this paper, we cryptanalyzes David's scheme and showed that it is vulnerable to different attacks. In addition, the scheme also suffers from several design faults. Therefore, we claim that David's scheme is not suitable for real-time applications.

ORCID

SK Hafizul Islam https://orcid.org/0000-0002-2703-0213

REFERENCES

1. Amin R, Biswas G. A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity. *J Med Syst*. 2015;39(8):1-19.
2. Chen H-M, Lo J-W, Yeh C-K. An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. *J Med Syst*. 2012;36(6):3907-3915.
3. Wu Z-Y, Lee Y-C, Lai F, Lee H-C, Chung Y. A secure authentication scheme for telecare medicine information systems. *J Med Syst*. 2012;36(3):1529-1535.
4. Moon J, Choi Y, Kim J, Won D. An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. *J Med Syst*. 2016;40(3):1-11.
5. 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*. 2017;21(2):465–475. doi: 10.1109/JBHI.2016.2517146.
6. Jiang Q, Ma J, Lu X, Tian Y. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *J Med Syst*. 2014;38(2):1-8.

7. Arshad H, Teymoori V, Nikooghadam M, Abbassi H. On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *J Med Syst*. 2015;39(8):1-10.
8. Pu Q, Wang J, Zhao R. Strong authentication scheme for telecare medicine information systems. *J Med Syst*. 2012;36(4):2609-2619.
9. Jian G. Feng R. *Cryptanalysis and Improvement of an Improved Two Factor Authentication Scheme for Telecare Medicine Information Systems*. arXiv: 1607.01471.
10. Kalra S, Sood SK. Secure authentication scheme for IOT and cloud servers. *Pervasive Mob Comput*. 2015;24:210-223.
11. Amin R, Biswas G. An improved RSA based user authentication and session key agreement protocol usable in TMIS. *J Med Syst*. 2015;39(8):1-14.
12. Liu W, Xie Q, Wang S, Hu B. An improved authenticated key agreement protocol for telecare medicine information system. *SpringerPlus*. 2016;5(1):1.
13. Guo D, Wen Q, Li W, Zhang H, Jin Z. An improved biometrics-based authentication scheme for telecare medical information systems. *J Med Syst*. 2015;39(3):1-10.
14. Debiao H, Jianhua C, Rui Z. A more secure authentication scheme for telecare medicine information systems. *J Med Syst*. 2012;36(3):1989-1995.
15. Wei J, Hu X, Liu W. An improved authentication scheme for telecare medicine information systems. *J Med Syst*. 2012;36(6):3597-3604.
16. Wu F, Xu L. Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *J Med Syst*. 2013;37(4):9958.
17. Jiang Q, Ma J, Ma Z, Li G. A privacy enhanced authentication scheme for telecare medical information systems. *J Med Syst*. 2013;37(1):1-8.
18. Mishra D, Mukhopadhyay S. *Cryptanalysis of Wu and Xu's Authentication Scheme for Telecare Medicine Information Systems*. arXiv: 1309.5255.
19. Hao X, Wang J, Yang Q, Yan X, Li P. A chaotic map-based authentication scheme for telecare medicine information systems. *J Med Syst*. 2013;37(2):9919.
20. Amin R, Islam SH, Biswas G, Khan MK, Obaidat MS. Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. *J Med Syst*. 2015;39(11):1-20.
21. Lu Y, Li L, Peng H, Yang Y. An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *J Med Syst*. 2015;39(3):1-8.
22. Das AK. A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems. *J Med Syst*. 2015;39(3):1-20.
23. Tan Z. A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J Med Syst*. 2014;38(3):1-9.
24. Arshad H, Nikooghadam M. Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *J Med Syst*. 2014;38(12):1-12.
25. Mishra D. Understanding security failures of two authentication and key agreement schemes for telecare medicine information systems. *J Med Syst*. 2015;39(3):19.
26. Lee T-F. An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *J Med Syst*. 2013;37(6):1-9.
27. Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *J Med Syst*. 2014;38(1):1-7.
28. Wazid M, Das AK, Kumari S, Li X, Wu F. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Secur Commun Netw*. 2016;9(13):1983–2001.
29. David DB. Mutual authentication scheme for multimedia medical information systems. *Multimed Tools Appl*. 2017;76(8):10741–10759.
30. Mitsunari S, Sakai R, Kasahara M. A new traitor tracing. *IEICE Trans Fundam Electron Commun Comput Sci*. 2002;85(2):481-484.
31. Debiao H, Jianhua C, Jin H. An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security. *Inform Fusion*. 2012;13(3):223-230.
32. Islam SH, Khan MK. Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks. *Int J Commun Syst*. 2016;29:2442-2456.
33. Canetti R, Krawczyk H. *Analysis of key-exchange protocols and their use for building secure channels*. *International Conference on the Theory and Applications of Cryptographic Techniques*. Innsbruck (Tyrol), Austria: Springer; 2001:453-474.

How to cite this article: Karuppiah M, Obaidat MS, Islam SKH, Vijayakumar P. Security analysis on "mutual authentication scheme for multimedia medical information systems". *Security and Privacy* 2019;e67. https://doi.org/10.1002/spy2.67