9th International Conference on Computer and Knowledge Engineering (ICCKE 2019), October 24-25 2019, Ferdowsi University of Mashhad

A Novel Provably-Secure ECC-based Authentication and Key Management Protocol for Telecare Medical Information Systems

Haleh Amintoosi
Computer Engineering Department
Faculty of Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
amintoosi@um.ac.ir

Mahdi Nikooghadam
Computer Engineering Department
Faculty of Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
mahdi.nikooghadam@mail.um.ac.ir

***Abstract*—Telecare medical information systems are becoming more and more popular due to the provision of delivering health services including remote access to health profile for doctors, staff and patients. Since these systems are installed entirely on Internet, they are faced with different security and privacy threats. So, an important challenge is the establishment of a secure key agreement and authentication procedure between the medical servers and patients. Recently, an ECC-based authentication and key agreement scheme for telecare medical systems in smart city has been proposed by Khatoon et.al. In this paper, at first, we descriptively analyse Khatoon et al.'s protocol and demonstrate that it is vulnerable against to known-session-specific temporary information attack and cannot satisfy perfect forward secrecy. Next, we propose a provably secure and efficient authentication and key agreement protocol using Elliptic Curve Cryptography (ECC). The security of the proposed scheme is informally analysed and it is proved that it can satisfy perfect forward secrecy and resist known attacks such as user/server impersonation attack. The protocol is also simulated and its security is formally analyzed using Scyther tool. The results show its robustness against different types of attacks.**

***Index Terms*—Authentication, Key Agreement, Healthcare, TMIS, Cryptanalysis**

I. INTRODUCTION

With latest propels in information technology, we are confronting a development in the improvement of medicinal services related applications, for example, telecare medical information systems (TMISs) that have been set up to give online health-related services to patients. In these systems, the data belonging to the patients (e.g., blood pressure) are saved into medicinal databases. To utilize health-related services, the patient needs to sign up with the TMIS restorative server. The initial step in service provisioning for the patients, thus, is to confirm the authenticity of the patient by the server. Once verified, medicinal services staff as well as specialists are reached out to give him the necessary health-related advice.

Although there are lots of benefits within the utilization of TMIS, an important remaining challenge is the establishment of a confidential and secure communication channel between the patient and the medical server. Without such secure channel, the attacker is able to insert falsified data into the database or gain unapproved access to private health data of patients, leading to injury or false diagnosis. Therefore, many researches has recently been done in order to propose secure authentication and communication protocols for TMISs [1], [3]–[10].

Recently, an Elliptic Curve Cryptography (ECC)-based mutual authentication and key agreement protocol for TMIS has been proposed by Khatoon et al. [1], where authors have discussed that their proposed scheme is able to resist against various attacks and guarantee the provision of anonymity and un-linkability. In this article, we first demonstrate that Khatoon et al. [1]'s scheme is prone to known-session-specific temporary information attack and cannot provide perfect forward secrecy. We then propose a secure and efficient ECC-based key management and authentication scheme for TMISs. Our contribution is as follows:

- We carry out cryptanalysis of Khatoon et al.'s scheme [1] and show it is vulnerable against known-session-specific temporary information attack and cannot guarantee perfect forward secrecy.
- We propose a secure authentication and key agreement protocol based on Elliptic Curve Cryptography which is able to provide mutual authentication and user anonymity. We also demonstrate that the proposed protocol is robust against various attacks including user/server impersonation attack, replay attack, and known-session-specific temporary information attack, and provides perfect forward secrecy.
- We formally analyse the security of our protocol using Scyther tool [2] and show the correctness of the approach. We also analyse the performance of the proposed scheme and show that our scheme is able to satisfy various security features.

978-1-7281-5075-8/19/$31.00

Registration Phase

---

patient U_i

Computes $C_i = PW^i \oplus H_B(B_i)$

$$\xrightarrow[\text{(Secure Channel)}]{C_i, ID_i}$$

TMIS server S

S checks the ID_i in its database
if new, S records N=0
otherwise S records N=N+1
Computes $V_i = h(ID_i||C_i)$ and $W_i = C_i \oplus h(ID_i||s)$
Customizes SC_i with $(V_i, W_i, P_{pup}, h, H, H_B)$
sends it securely to U_i

Login and Authentication Phase

Patient U_i

U_i insert his smart card SC_i in card reader
Input ID_i, PW_i and imprints B_i
the SC_i computes $h(ID_i||PW_i \oplus H_B(B_i))$
Checks $h(ID_i||PW_i \oplus H_B(B_i)) = V_i$
if invalid, SC_i aborts the session
Otherwise,
selects $r_i \in Z_p$ and fresh T_i
Computes $Q_i = H(ID_i), Q_s = H(ID_s)$
$R_i = r_i.Q_i, K_i = e(P_{pub}, r_i.Q_s)$
$Auth_i = E_{k_i}(ID_i||T_i||r_i)$

$$\xrightarrow{R_i, T_i, Auth_i}$$

TMIS server S

Upon receiving LR_i, S checks
$\Delta T < T_s - T_i$ if valid it proceed
And calculate $K_s = e(s, R_i.P)$
decrypts $Auth_i$ to obtain $(ID_i||T_i||r_i)$
Computes $Q_i = H(ID_i)$
checks $R_i = r_i.Q_i$. If valid
Then S generates a random number r_s
Computes $Q_s = H(ID_s), R_s = r_s.Q_i, L_s = r_s.R_i$
$Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_s)$
$SK_s = h(T_i||R_i||T_s||R_s||L_s)$

$$\xleftarrow{R_s, T_s, Auth_s}$$

verifies $\Delta T < T_s - T_i$
if valid
Computes $L_i = r_i.R_s$
verifies $Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_i)$
And computes $SK_i = h(T_i||R_i||T_s||R_s||L_s)$

Fig. 1. Registration and Authentication phase of Khatoon et al.'s scheme [1]

TABLE I
NOTATIONS USED IN THE ARTICLE

symbol	description
q	a large prime
e	a bilinear map e: $G_1 \times G_1 \rightarrow G_2$
P	The generator of G_1
ID_i, PW_i, B_i	Patient's identity, password and biometric information
S	TMIS server
s	Master private key $s \in Z_q^*$ of S
P_{pub}	Public key $P_{pub} = sP$ of S
h	A hash function $h : \{0,1\}^* \rightarrow Z_q$
H	A hash function $H_1 : \{0,1\}^* \rightarrow G_1$
T_{k_i}	Encryption with symmetric key k_i
T_s, T_i, T_1, T_2, T_3	Time stamp of U_i and S
a_i, c_i, d_i, m_i	Random numbers
SC	Smart Card
SK	Session Key

II. RELATED WORK

Rapid growth in wireless communications as well as mobile devices has paved the way for the emergence of telecare medical information system (TMIS), which enables patients to have remote access to medical treatments from the specialists. However, preserving the patients' privacy and providing a secure communication channel is a major challenge. To address this challenge, Li et al. [3] proposed a cloud-based privacy-aware authentication scheme based for TMIS and claimed that their protocol is resistant against all known security threats. However, Kumar et al. [4] showed that Li et al.'s work is prone to impersonation attack and does not provide user anonymity and unlinkability. Further, they presented an enhanced protocol to address the above-mentioned challenges. Also, in 2018, Ravanbakhsh and Nazari [5] presented a remote key agreement and authentication scheme for healthcare systems. But Ostad-Sharif et al. [6] showed that their work is prone to known session-specific temporary information attack and cannot guarantee perfect forward secrecy. To address these drawbacks, they proposed an ECC-based authentication and key management scheme for TMIS. Chaudhry et al. [7] also showed in 2018 that the work presented by Mir and Nikooghadam [8] is prone to smart card stolen attack and to address this shortcoming, they proposed a robust and computationally efficient authentication scheme for healthcare systems that is able to protect against user anonymity violation attack and smart card stolen attack.

III. OVERVIEW AND CRYPTANALYSIS OF KHATOON ET AL.'S SCHEME

In this section, a review and analysis on Khatoon et al.'s scheme [1] is presented and we demonstrate that this protocol is vulnerable against known-session-specific temporary information attack and does not provide perfect forward secrecy.

A. Overview of Khatoon et al.'s Scheme

Table I shows Khatoon et al. scheme's notations. Figure 1 also demonstrates Khatoon et al. authentication protocol. In order to access the medical server services, the patient first needs to sign up to the server. To do so, in the registration phase, the required log in information is sent from the server to the patient. Upon completing the registration process, a key is shared between the server and the patient via the authentication phase. The patient and the server are then able to use the shared key in their subsequent secure communications.

B. Cryptanalysis of Khatoon et al.'s Scheme

In this section, at first, we prove that Khatoon et al. [1]'s scheme is prone to the known-session-specific temporary information attack. Next, we demonstrate that it does not guarantee perfect forward secrecy.

1) Vulnerability to Known-session-specific Temporary Information Attack: As discussed in [6], known-session-specific temporary information attack refers to the situation where by knowing the session random numbers, the adversary succeeds in obtaining the session key. In what follows, we show that Khatoon et al.'s scheme is prone to known-session-specific temporary information attack.

- As expressed in Khatoon et al.'s scheme authentication step in Figure 1, R_i is obtainable by the attacker due to being exchanged on public channel. Also, r_s is a random parameter which is supposed to be available to the attacker in known-session-specific temporary information attack. Hence, the adversary can calculate L_s as $L_s = r_s.R_i$.
- As shown in Figure 1, the session key SK is computed as $SK_i = h(T_i||R_i||T_s||R_s||L_s)$. Parameters R_i, T_i, R_s, T_s are available to the adversary due to being exchanged on public channel. As expressed above, the adversary can compute L_s. Having all the parameters included in SK, the session key SK is now computable by the adversary. This clearly shows that Khatoon et al.'s scheme is vulnerable against known-session-specific temporary information attack.

2) Lack of Perfect Forward Secrecy: The protocol is said to provide perfect forward secrecy if the adversary cannot compute the session key SK even if he knows the longterms such as the server's public/private keys. In the following, we demonstrate that Khatoon et al.'s scheme is not able to provide perfect forward secrecy.

- Suppose that the adversary knows the public and private keys of the medical server. Now, he can compute K_s as $K_s = e(s, R_i.P)$, due to the fact that R_i is available on public channel.
- As $K_s = K_i$, he is now able to decrypt $Auth_i$ and get r_i as $Auth_i = E_{k_i}(ID_i||T_i||r_i)$.
- Since r_i and R_i are accessible via public channel, the adversary calculates $L_i = r_i.R_s$.
- At the same time, $L_i = r_i.R_s = r_i.r_s.Q_i = r_s.r_i.Q_i = r_s.R_i = L_s$. So, the adversary already has L_s at hand too.
- L_s has been computed in the above step and T_i, R_i, T_s and R_s are accessible on public channel. So, the adver-

sary can now compute the session key SK as $SK_i = h(T_i||R_i||T_s||R_s||L_s)$. This implies the weakness of Khatoon et al.'s scheme in providing perfect forward secrecy.

IV. THE PROPOSED SCHEME

In this section, we present the details of the proposed ECC-based protocol, which has two steps: registration, and authentication and key agreement. The notations used in our proposed method are the same as the one shown in Table I.

- Registration: The patient selects an identity and password ID_i and PW_i and random number a_i. He then computes $HID_i = h(ID_i||a_i)$ and $A_i = h(ID_i||PW_i||a_i) \oplus ID_i$ and sends A_i, HID_i to the TMIS server through a secure communication channel. Upon receiving the parameters, the server computes $R_i = E_s(A_i||HID_i)$ and $Q_i = A_i \oplus R_i$ and then, stores $Q_i, E(.)/D(.)$ in smart card SC and sends the smart card back to the patient via a secure channel. The patient computes $D_i = h(A_i||HID_i)$ and adds D_i, a_i to smart card. The smart card now contains $\{Q_i, a_i, D_i, E(.)/D(.)\}$.
- Authentication and key agreement: The patient inserts his smart card SC into the card reader and inputs his identity ID_i^* and password PW_i^*. He then computes $HID_i^* = h(ID_i^*||a_i)$, $A_i^* = h(ID_i^*||PW_i^*||a_i) \oplus ID_i^*$ and $D_i^* = h(A_i^*||HID_i^*)$ and checks whether D_i^* equals D_i. If so, it is verified that the card belongs to the user. Otherwise, the session is terminated. He then selects random numbers c_i, d_i, time stamp T_1 and computes $C_i = c_i.p$ and $key{1_i} = c_i.P_{pub} = c_i.s.p$. He then encrypts $\{A_i, D_i, Q_i, T_1\}$ with $key{1_i}$ to obtain E_i as $E_i = E_{key{1_i}}(A_i, D_i, Q_i, T_1)$. The message $\{C_i, E_i, T_1, d_i.p\}$ is then sent to the server. Once received at the TMIS server, the server selects time stamp T_2 and checks the freshness of the message by verifying whether $|T_2 - T_1| < \Delta T$. If not so, the session is terminated. Otherwise, it computes $key{1_i'} = C_i.s = c_i.p.s$ and decrypts E_i with $key{1_i'}$ as $D_{key{1_i'}}(E_i) = (A_i^*, D_i^*, Q_i^*, T_1^*)$ and obtains A_i^*, D_i^*, Q_i^*, and T_1^*. The server then checks whether $T_1^*? = T_1$. If so, it recomputes $R_i^* = A_i^* \oplus Q_i^*$ and then decrypts R_i^* with the server's private key s to obtain A_i^* and HID_i^* as $D_s(R_i^*) = (A_i^*, HID_i^*)$. It then calculates $D_i^{**} = h(A_i^*||HID_i^*)$ and compares D_i^{**} with D_i^*. If equal, it selects random number m_i and computes the session key SK as $SK = h(m_i.d_i.p||HID_i||D_i)$ and $z_i = h(SK||HID_i||D_i)$. The message $\{m_i.p, z_i, T_2\}$ is then sent back to the patient. Upon receiving the message, the patient computed the session key $SK = h(d_i.m_i.p||HID_i||D_i)$. He then computes $z_i^* = h(SK||HID_i||D_i)$ and if z_i^* equals to z_i received within the message, the server is authenticated.

V. SECURITY ANALYSIS

In this section, we first present an informal security analysis of the proposed protocol and demonstrate that the proposed scheme is secure against the most common security attacks. Then, we formally prove the security and correctness of the proposed scheme using the Scyther tool.

A. *Informal Security Analysis*

Perfect Forward Secrecy Perfect forward secrecy refers to the property of a key agreement scheme that guarantees the compromise of the server's private key will not lead to the compromise of session keys. In the proposed protocol, the session key SK is computed as $SK = h(m_i.d_i.p||HID_i||D_i)$, in which, m_i and d_i are random numbers. If the server's session key s is compromised, the adversary is able decrypt R_i and obtain HID_i and A_i since $R_i = E_s(A_i||HID_i)$ and since $Di = h(A_i||HID_i)$, he is able to compute D_i as well. As shown in the protocol, $d_i.p$ is exchanged on public channel, so, accessible to the adversary. However, as stated in Elliptic Curve Diffie-Hellman Problem (ECDHP), if $a_i.p$ and $b_i.p$ are accessible, it is not possible to obtain $a_i.b_i.p = b_i.a_i.p$. So, having access to $d_i.p$, the adversary is not able to compute $m_i.d_i.p$ which is included in SK. So, our proposed protocol is able to provide perfect forward secrecy.

Known-session-specific Temporary Information Attack If session random numbers a_i, c_i, d_i, m_i are unexpectedly disclosed to the attacker, he should not be able to retrieve session key SK. As shown above, $SK = h(m_i.d_i.p||HID_i||D_i)$ contains HID_i and D_i which are only achievable by decrypting R_i with the server's secret key s, not accessible by the attacker. So, even if the random numbers m_i and d_i are disclosed, the attacker is only able to compute $m_i.d_i.p$ and not able to obtain HID_i and D_i. So, he is not able to obtain the session key SK. In other words, the proposed protocol is secure against known-session-specific temporary information attack.

User Impersonation Attack In order to authenticate the patient, the server decrypts R_i^* to obtain A_i^* and HID_i^*. Next, it computes D_i^{**} as $D_i^{**} = h(A_i^*||HID_i^*)$. It then compares D_i^{**} with D_i^* obtained from decrypting E_i received from the patient. If equal, the patient is authenticated. In the proposed protocol, the attacker is not in the possess of the server's secret key, so he is not able to decrypt R_i^* to obtain D_i^{**}, thus, not able to impersonate the patient. So, the proposed scheme is robust against user impersonation attack.

Server Impersonation Attack In order to authenticate the server, the patient computes $z_i^* = h(SK||HID_i||D_i)$ and compares it with the one sent from the server. To impersonate the server, the attacker tends to send his own z_i and sends it to the patient. But since z_i^* is dependant on HID_i and D_i which are calculated on the patient's side and are not exchanged anywhere, the attacker will not be successful ro pass the comparison of $z_i^*? = z_i$. In other words, he is not able to impersonate the server. So, the proposed protocol is secure against server impersonation attack.

Replay Attack The replay attack happens when the attacker replays an old message $\{C_i, E_i, T_1, d_i.p\}$ to the server. In our scheme, the server is able to figure out that this message is old. At first, the server verifies $|T_2 - T_1| \leq \Delta T$, and if this condition is not true, it means that the message is old and the

Registration Phase

Patient U_i **TMIS server S**

Chooses ID_i, PW_i
Selects random number a_i
$HID_i = h(ID_i||a_i)$
$A_i = h(ID_i||PW_i||a_i) \oplus ID_i$

$$\xrightarrow[\text{(Secure Channel)}]{\{A_i, HID_i\}}$$

$R_i = E_s(A_i||HID_i)$
$Q_i = A_i \oplus R_i$
Stores $[Q_i, E(.)/D(.)$] in Smart Card SC.

$$\xleftarrow[\text{(Secure Channel)}]{SC}$$

$D_i = h(A_i||HID_i)$
adds $\{D_i, a_i\}$ to SC
SC=$[Q_i, a_i, D_i, E(.)/D(.)]$

Login and Authentication Phase

Patient U_i **TMIS server S**

Inserts his/her smart card SC and enters ID_i^*, PW_i^*
$HID_i^* = h(ID_i^*||a_i)$
$A_i^* = h(ID_i^*||PW_i^*||a_i) \oplus ID_i^*$
$D_i^* = h(A_i^*||HID_i^*)$
$D_i^* =^? D_i$
Selects random numbers $c_i, d_i \in Z^*$
Selects Time Stamp T_1
Computes $C_i = c_i.p$
Computes $key_{1_i} = c_i.P_{pub} = c_i.s.p$
$E_i = E_{key_{1_i}}(A_i, D_i, Q_i, T_1)$

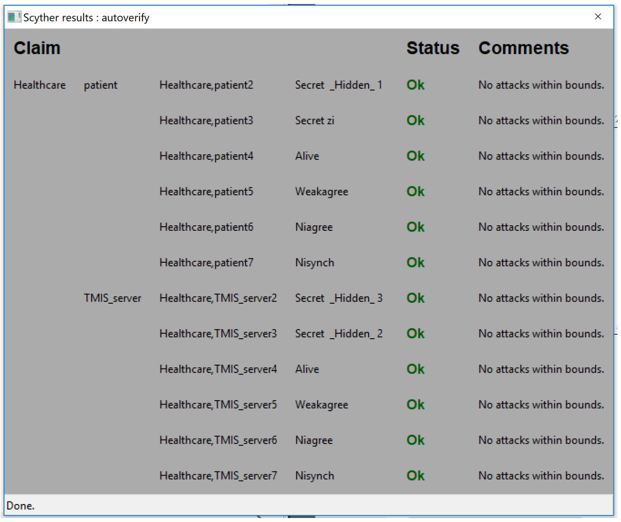
$$\xrightarrow{\{C_i, E_i, T_1, d_i.p\}}$$

Selects Time Stamp T_2
Checks $|T_2 - T_1| < \Delta T$
Computes $key_1{}'_i = C_i.s = c_i.p.s$
Decrypts $D_{key_1{}'_i}(E_i) = (A_i^*, D_i^*, Q_i^*, T_1^*)$
Checks $T_1^*? = T_1$
$R_i^* = A_i^* \oplus Q_i^*$
Decrypts $D_s(R_i^*) = (A_i^*, HID_i^*)$
$D_i^{**} = h(A_i^*||HID_i^*)$
Checks $D_i^{**}? = D_i^*$
Selects random number $m_i \in Z^*$
Computes $SK = h(m_i.d_i.p||HID_i||D_i)$
Computes $z_i = h(SK||HID_i||D_i)$

$$\xleftarrow{\{m_i.p, z_i, T_2\}}$$

Selects Time Stamp T_3
Checks $|T_3 - T_2| < \Delta T$
Computes $SK = h(d_i.m_i.p||HID_i||D_i)$
Computes $z_i^* = h(SK||HID_i||D_i)$
Checks $z_i^*? = z_i$

Fig. 2. Registration and Authentication Phase of the Proposed Scheme



Claim				Status	Comments
Healthcare	patient	Healthcare,patient2	Secret _Hidden_ 1	Ok	No attacks within bounds.
		Healthcare,patient3	Secret zi	Ok	No attacks within bounds.
		Healthcare,patient4	Alive	Ok	No attacks within bounds.
		Healthcare,patient5	Weakagree	Ok	No attacks within bounds.
		Healthcare,patient6	Niagree	Ok	No attacks within bounds.
		Healthcare,patient7	Nisynch	Ok	No attacks within bounds.
	TMIS_server	Healthcare,TMIS_server2	Secret _Hidden_ 3	Ok	No attacks within bounds.
		Healthcare,TMIS_server3	Secret _Hidden_ 2	Ok	No attacks within bounds.
		Healthcare,TMIS_server4	Alive	Ok	No attacks within bounds.
		Healthcare,TMIS_server5	Weakagree	Ok	No attacks within bounds.
		Healthcare,TMIS_server6	Niagree	Ok	No attacks within bounds.
		Healthcare,TMIS_server7	Nisynch	Ok	No attacks within bounds.

Fig. 3. Security Analysis of the Proposed Scheme using Scyther

session terminates. Even if the attacker changes T_1 with current time T_1^{**} and sends $\{C_i, E_i, T_1^{**}, d_i.p\}$ to the server, the server is able to distinguish that the message is old. The server decrypts E_i with key_{1_i} as $D_{key_{1_i}}(E_i) = (A_i^*, D_i^*, Q_i^*, T_1^*)$ and compares T_1^* (obtained from decryption) with T_1^{**}. if not equal, the server identifies that the timestamp has been changed. The same stands for T_2 in $\{m_i.p, z_i, T_2\}$, where the server checks the freshness of the message by selecting T_3 and verifying whether $|T_3 - T_2| < \Delta T$. So, our proposed scheme is resistant against replay attacks.

B. Formal Security Analysis by Scyther Tool

Scyther has been designed and extended as a tool with the aim of formally analyzing the security protocols and identifying their security requirements and vulnerabilities [2]. Scyther is based on the development model algorithm that provides the representation of traces, analyzes the protocol automatically and examines its behavior against most of the potential attacks. Figure 3 depicts the analysis result of the proposed protocol via Scyther for 15 iterations. The term *Claim* is used to specify security requirements *Alive*, *Nisynch*, *weakagree* and *secret*. The aim of using *Alive* is ensuring that some events have been executed by an intended communication party R. *Nisynch* means that all received messages are indeed sent by the sender and have been received by the receiver. $claim(R; secret; rt)$ means that R claims that rt must be unknown to an adversary. Finally, *weakagree* ensures that the protocol is secure against impersonation attack. As shown in Figure 3, the proposed protocol is able to satisfy all the above-mentioned security requirements. Scyther code has also been shown at the end of article.

VI. CONCLUSION AND FUTURE WORK

Lots of attention has recently been paid on the provision of a privacy-preserving and secure communication channel among various parties in telecare medical information systems. In this paper, we analysed Khatoon et al.'s authentication and key agreement scheme, and proved that it is vulnerable against known-session-specific temporary information attack and cannot guarantee perfect forward secrecy. We also proposed a secure and efficient mutual authentication and key agreement scheme for TMIS and proved that it is able to resist known attacks including user/server impersonation attack and known-session-specific temporary information attack. We also analysed and proved the security of the proposed scheme via the Scyther tool.

REFERENCES

[1] S. Khatoon, S. M. M. Rahman, M. Alrubaian and A. Alamri, Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment, in IEEE Access, vol. 7, pp. 47962-47971, (2019)

[2] Cremers, C., Scyther,Semantics and Verification of Security Protocols. Ph.D. dissertation, Eindhoven University of Technology, (2006)

[3] Chun-Ta Li, Dong-Her Shih, Chun-Cheng Wang, Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems, Computer Methods and Programs in Biomedicine, vol. 157, pp. 191-203, (2018)

[4] Vinod Kumar, Musheer Ahmad, Adesh Kumari, A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS, Telematics and Informatics, vol. 38, pp. Pages 100-117, (2019)

[5] Ravanbakhsh N, Nazari M. An efficient improvement remote user mutual authentication and session key agreement scheme for E-healthcare systems. Multimed Tools Appl. vol. 77, no. 1, pp. 55-88, (2018)

[6] Ostad-Sharif, A, Abbasinezhad-Mood, D, Nikooghadam, M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst. 32:e3913. https://doi.org/10.1002/dac.3913, (2019)

[7] Chaudhry, S.A., Naqvi, H. , Khan, M.K., An enhanced lightweight anonymous biometric based authentication scheme for TMIS, Multimed Tools Appl vol. 77, no. 5, : 5503-5524. (2019)

[8] Omid Mir, Morteza Nikooghadam, A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services, Wireless Personal Communications, vol. 83, Issue 4, pp. 2439–2461, (2015)

[9] M. Safkhani and A. Vasilakos, A New Secure Authentication Protocol for Telecare Medicine Information System and Smart Campus, IEEE Access, vol. 7, pp. 23514-23526, (2019)

[10] Jiang, Q., Chen, Z., Li, B. et al. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems, J Ambient Intell Human Comput, vol. 9, no. 4, pp: 1061-1073, (2018)