International Journal of Mathematics and
Computer Science, **15**(2020), no. 4, 1015–1027

An Efficient Two Factor User Authentication and Key Exchange Protocol for Telecare Medical Information System

Fairouz Sherali, Sarhan Falah

Education College for Girls
University of Kufa
Najaf Governorate, Iraq

email: fairoozm.jaafar@uokufa.edu.iq, falahh.sarhan@uokufa.edu.iq

(Received July 16, 2020, Accepted August 27, 2020)

Abstract

Telecare medical information system (TMIS) is substantially desirable to patients by allowing them to remotely access medical services. Authentication schemes for TMIS try to ensure secure and authorized access. Recently, some smart card-based password authentication schemes have been proposed, but privacy is not duly addressed. In this paper, we propose a key agreement technique for a medical server environment to overcome the limitations of the existing schemes. In the proposed scheme, we suggest bringing together the advance of both the crypto and Information Retrieval (IR) community to enhance the health-care process between patients and doctors by supporting an efficient communicating platform on the internet which overcomes some drawbacks in traditional health-care services. However, to keep patient medical data confidential against untrusted patients, we apply cryptographic methods by disclosing the data decryption key only to authorized patients and doctors to retrieve medical files containing certain keywords. We show that the proposed scheme is secure in the random oracle model (ROM) under the Bilinear Diffie-Hellman Problem BDHP.

Keywords and phrases: Telecare medicine information system (TMIS); Information Retrieval; Authentication; Bilinear Diffie-Hellman Problem.
AMS (MOS) Subject Classifications:
ISSN 1814-0432, 2020, http://ijmcs.future-in-tech.net

1 Introduction

At this time, people are accessing different services and applications through the Internet. For instance, they use different electronic devices like computers and mobile phones to get access to a remote server from anywhere and anytime through a public channel. Nowadays, low cost mobile devices and internet services make electronic health care and telemedicine services available directly to the user (patient). With electronic health care, users are able to get different healthcare services without visiting the healthcare center physically, but through the Internet. The traditional clinical medical service system can often be replaced by electronic health care, distance nursing, and home watching facility[1]

Telecare medical information system (TMIS)[2] has become an available choice for users or patients to get remote healthcare services conveniently. As we are moving from paper-based patients records to electronic patients records, the telecare medical information system provides easy access to electronic records for remote patients. Despite the advantages of TMIS, several issues should be addressed before users or patients can adopt it. First, the TMIS is vulnerable to different attacks because these systems are constructed on public networks. Secondly, private information and medical history of patients are supposed to be maintained carefully by TMIS and be kept secret in messages transferred among all entities to prevent users' privacy from being revealed. Thus, a secure technique is required to protect the communication process in TMIS and reduce the adversary threat. The remote authentication protocol is a promising way to protect patients and TMIS from attackers in different information systems. We propose a new two-factor user authentication scheme for medical storage services to resolve the above issues.

In this paper, we show that many of the two-factor authentication schemes are not secure against an off-line dictionary attack and fail to provide the revocation of lost/stolen disguised smart card. To overcome these drawbacks, we suggest an improved scheme to achieve an efficient authentication phase using a secure searchable keyword as a password-based authentication. In this scheme, we propose to bring together the advance of both the crypto and IR community [3, 4, 5] to construct a novel authentication scheme to overcome the security drawbacks. Also, we apply cryptographic methods by disclosing the data decryption key only to authorized patients and doctors to retrieve medical files containing certain keywords. Furthermore, we show that the proposed scheme is secure in the random oracle model (ROM).

In 1981, Lamport [6] presented a password-based authentication technique in which the TMIS server saved all the passwords into a password table. Later, this topic has become popular among researchers [7, 8]. These techniques are susceptible to stolen-verifier attacks. Dictionary attacks may guess a password list with low entropy. In other words, password-based authentication fails to withstand the password-guessing attacks. To overcome these problems, traditional password authentications have been combined with the smart cards to form a two-factor-based authentication scheme. Two-factor authentication requires a legal user to have both valid factors: password and card. The authentication procedure would fail if either of the two factors was invalid. With the support of the two-factor authentication, users and TMIS servers can be authenticated by each other. A session key will be shared between users and TMIS servers for securing communication after the authentication phase. The session key can preserve the privacy of the user's personal information during communication operation over public networks [9]. Recently, researchers presented various authentication schemes to provide efficient health services for remote users and patients in TMIS. Wu et al. [10] proposed an efficient authentication scheme for TMIS, which used passwords and smart cards to construct a two-factor-based remote authentication scheme for TMIS. The scheme is better than the previously presented schemes for low computing devices by adding the precomputing stage. Chen et al. [11] proposed a dynamic ID-based authentication scheme which protects user anonymity and is less costly. Jiang et al.[12] proposed an authentication scheme that achieved patient anonymity. Also, Lin[13] observed that user identity is disclosed under the dictionary attack and the password can be inferred with the stolen smart card in the Chen et al. scheme. He suggested an enhanced scheme which efficiently withstands the dictionary attack and protects anonymity. Xu et al.[14] proposed a two-factor authentication key agreement scheme using ECC. As a new direction, biometric keys can maintain the uniqueness feature because they can neither be forged nor estimated easily. Therefore, biometric keys have been widely used in authentication protocols [15].

2 Preliminaries

In this section, we present some necessary concepts needed in this work.

2.1 Complexity assumptions

Here, we review the definition of the Bilinear Diffie-Hellman (BDH) problem associated with the bilinear pairings [16].

Definition 2.1. *(BDH Problem) Let* G_x, G_y *be two groups of prime order* r, v *be a generator of* G_x, $\hat{e} : G_x \times G_x \to G_y$ *be an admissible bilinear map and AR be an attacker algorithm. The BDH problem in* $(G_x, G_y, \hat{e})$ *is as follows: Given* (v, v^a, v^b, v^c) *for some* $a, b, c \in Z_n$*, compute* $\hat{e}(v, v)^{abc} \in G_y$*. An algorithm AR has advantage in solving BDH in* G_y *if* $Pr[AR(v, v^a, v^b, v^c) = \hat{e}(v, v)^{abc}] \geq \epsilon$*.*

2.2 Random oracles

In our scheme, we use asymmetric encryption and three cryptographic hash functions $h_1 : \{0,1\}^* \to G_x$ and $h_2 : G_y \to \{0,1\}^{logr}$, where h_1 and h_2 are random oracles[17], and select one hash function h_3 to secure the ID of patient. The cryptographic one-way hash function is irreversible and it demands less execution time for encryption/decryption algorithms. Therefore, our proposed scheme is efficient.

3 Problem formulation

Our scheme involves three different entities: patients, doctors, and medical servers. We suppose that these entities are semi-honest and do not collude with each other to skip the security measures.

- Patient P: this entity has a collection of medical files $MF = \{mf_1, mf_2, ..., mf_n\}$, which are encrypted using a standard symmetric algorithm like AES. To allow the searching capability over the encrypted medical files for effective data utilization, the patient, in an off-line stage before uploading, will first encrypt keyword set Kw extracted from *MF*. Patient uploads both the *Kw* and the encrypted medical files to the medical server.

- Doctor D: this entity is an authorized user to access the medical files of the patient. With l query keywords, the authorized doctor can create a trapdoor Td through search control mechanisms to retrieve the encrypted record from

the server. Then, the doctor can decrypt the medical files with the shared secret key.
- Medical Server *MS*: the server stores the encrypted keywords and the encrypted medical files for the patient. Upon receiving the trapdoor *Td* from the Doctor, the server searches over the keyword set and retrieves the corresponding set of the encrypted medical files.

4 Outline of the proposed scheme

Initially, the patients P and the medical servers *MS* are enrolled with the medical service registration center. Patient authentication is verified by the smart card *SMC* and only the authentic patients can log into the system. *MS* also checks the authenticity of the patient with respect to the received login message. The medical server sends a reply-message to the patient after verification of authentication. Then, the patient checks the authenticity of the *MS* based on the received message. On the other hand, to retrieve only the medical records containing keyword Kw, the doctor computes the trapdoor *Td* and sends it to the *MS*. The scheme includes four phases, namely, Registration phase, Login phase, Authentication phase and Doctor phase.

I. Registration phase
Step 1. Patient P chooses a keyword of his choice, P encrypts kw using the key generation algorithm and keyword encryption algorithm as follows:
-The medical server provider *MSP* and patient P run key generation algorithm, the algorithm takes the large security parameters $\mu_1, \mu_2 \in Z_+$ to generate a prime number r, selects a random generator V of G_1, selects a random $\alpha, \gamma, \beta \in Z_r$ as private keys for P, *MS* and D respectively, computes the corresponding public keys $P_{Pub} = V^{\alpha}, MS_{Pub} = V^{\gamma}$ and $D_{Pub} = V^{\beta}$ for P, *MS*, and D respectively.
- As mentioned before we use a public key encryption algorithm to encrypt keywords, the patient runs the keyword encryption algorithm using a public key P_{Pub} to encrypt $kw, C_{kw} = h_2(\hat{e}(D_{Pub}, h_1(Kw)^{\alpha}))$.
- P sends the registration request with encrypted keyword C_{wk}, the identity of patient *IDp* and encrypted medical record *MF* to *MSP* via secure channel.
Step 2. Upon receiving the *P's* request, *MSP* verifies whether *IDp* is previously registered or not. If *IDp* is already registered, *MSP* asks for a new identity. Otherwise, *MSP* computes $K = h_3((ID_P^{\gamma}))$.

Then *MSP* personalizes smart card *SMC* by embedding the parameters $\{C_{wk}, K, MS_{Pub}, h_3(.)\}$ and returns *SMC* to P via a secure channel. *SMC* stores *IDp* in registered patients' database.
Step 3. P computes $K = h_3((ID_P^{\alpha})), X_1 = h_3(K||Kw)$ and $Z = X_1||C_{wk}$ then stores C_{wk}, α and X_1 into the smart card

II. Login phase: a registered patient with a valid smart card generates the login message and submits the login message to the server as follows:
Step 1. patient P inserts the smart card *SMC* into the card reader and inputs Kw and *IDp*.
Step 2. *SMC* computes $KK = h_3((ID_P))^P$. $X_2 = h_3(KK||Kw)$ and C_{Kw}, *SMC* verifies $Z = X_2||C_{Kw}$. If the verification does not hold, *SMC* terminates the session. Otherwise, *SMC* selects a random prime number n_P, and computes $K_1 = h_3(ID_P||KK||C_{Kw}||T_P)^{MS_{Pub}}$ where T_P is the current timestamp. Finally, *SMC* submits K_1 and T_P as a message to *MS*.

III. Authentication phase: patient and server mutually authenticate each other and establish a session key as follows:
Step 1. Upon receiving T_1 at time $\acute{T}_P$, *MSP* checks whether the condition $\acute{T}_P - T_P$ holds. If the condition holds, *MSP* verifies $K_1^{S_{Priv}} mod\ r = h_3(ID||KK||n_P||C_{kw}||T_P)$, If the verification holds, *MSP* considers P as an authorized patient. Then *MSP* computes $T_{Ps} = T_P \oplus T_s$ and the session key $S_{key} = h(T_{Ps}||n_P||C_{kw})$. Finally, *MS* responds with T_{Ps} and S_{key}.
Step 2. Upon receiving T_{Ps} and S_{key} at time $\acute{T}_s$, *SMC* verifies $\acute{T}_s - T_s \leq \triangle T$. If the verification holds, *MS* computes the session key $\acute{S}_{key} = h_3(T_{Ps}||n_P||C_{kw})$. Then *MS* verifies $\acute{S}_{key} = S_{key}$. If the verification holds, P considers S_{key} as the session key and *MS* as an authorized server

IV. Doctor Phase: this phase includes two algorithms, Trapdoor algorithm and keyword check algorithm. In the first algorithm, D takes a private key β and a keyword Td to compute trapdoor Td as $Td{=}h_2(\hat{e}(P_{Pub}, h_1(Td)^{\beta}))$. Then, D submits the trapdoor to the medical server. The keyword check algorithm is executed by the *MSP*, it takes an encrypted keyword C_{kw}, and a trapdoor *Td* as inputs, and outputs 1 or 0. The algorithm outputs 1 if *Kw*=*Td*, and 0 otherwise. If the output is 1, *MSP* considers that D as an authorized doctor.

5 Security and performance analysis of the proposed schemes

5.1 Informal security analysis

Here, we have discussed the security strength of the proposed scheme against possible attacks. The security features of other existing schemes are compared with the proposed scheme.

I. User Anonymity: the patient ID_P is protected under the security of secret key of *MS* and P. To know the ID_P from the data stored in the smart card, an attacker should know the keyword K_w and the secret key α and γ of the patient and the server respectively, only a registered *MS* knows the secret key of the server. Therefore, only the authentic server may compute the patient's identity. The timestamp Tp is different for each session. This ensures different login messages for each session. Thus, an attacker cannot relate between any two-login messages. Anonymity and Unlinkability make communication completely private.

II. Man-in-The-Middle-Attack: in this attack, an attacker pretends as a medical server to the patient P and as a patient to the medical server MS. He needs to be authenticated by both P and *MS*. However, the attacker cannot be authenticated by the medical server without the validity of P's keyword α and the attacker cannot be authenticated by the patient without *MS*'s secret key γ. This shows that the scheme resists man-in-the-middle attack.

III. Off-Line Dictionary Attack: an attacker may target the *SMC* to guess the keyword. The keyword is associated with the following values $Z = X_1||C_{wk}$ where $X_1 = h_3((ID_P))^{\alpha}||Kw$ and $C_{wk} = h_2(\hat{e}(D_{Pub}, h_1(Kw)^{\alpha}))$. However, the attacker needs to know *IDp*, Kw, and the secret key α. Again, it is hard to know the secret key α and the patient *IDp* to obtain the keyword *Kw* by the attacker.

IV. Replay Attacks: the scheme uses the current timestamp in every session to prevent the replay attacks. An attacker tries to intercept message $\langle K_1, T_P \rangle$ of the login. If the attacker replays a previous message by resubmitting to the medical server or the patient, the medical server or the patient will detect the attack immediately when the freshness of the timestamps will be verified. If the attacker wants to construct a valid message, he needs to know the secret key α, the random number n_P and *IDp*. However, attacker cannot get them. Hence the proposed scheme has abilities to withstand replay attack.

V. Impersonation Attack: once attacker *At* intends to launch a patient or server impersonation attack, he/she must compute the valid value of $\acute{K}_1 = h_3(ID_P||\acute{K}K||C_{kw}||T_P)^{MS_{Pub}}$. An attacker couldn't compute $\acute{K}K$ for many reasons: (1) attacker could not compute $\acute{K}K$, because he did not know the secret keys α and γ of the patient and medical server respectively. (2) Neither the keyword nor *IDp* is known by the attacker. Thus, an attacker cannot compute $\acute{K}_1$. Therefore, the improved protocol can resist impersonation attacks.

VI. Stolen Smart Card Attacks: we suppose that a smart card is stolen by an attacker and he can extract all stored information $(C_{wk}, K, MS_{Pub}, X_1)$ from the stolen smart card and try to generate a valid login message using these parameters. Where $X_1 = h_3(K||Kw)$ and $C_{kw} = h_2(\hat{e}(D_{Pub}, h_1(Kw)^{\alpha}))$. The adversary may try to compute the secret embedded parameters from the extracted information of *SMC*. However, it is difficult to disclose any information from hash values. Therefore, the proposed scheme avoids smart card stolen attack.

VII. Mutual Authentication: the medical server authenticates the patient by extracting KK. The computation of KK needs $h_3((ID_P))^{\alpha}$ which requires the patient's secret key. On the other hand, the medical server is verified by the Patient with $h_3(T_{ps}||n_p||C_{kw})$. Because an attacker doesn't have the secret key of MS, he cannot calculate the session key $\acute{S}_{key}$ correctly. Therefore, the mutual authentication between the medical server and the patient is achieved in this scheme.

VIII. Privileged-Insider Attacks: a user sends $C_{kw} = h_2(\hat{e}(D_{Pub}, h_1(Kw)^{\alpha}))$ to the *MS* in the registration phase. An insider patient of the trusted *MS* may behave like an attacker *At* and the registration message of the patient can be recorded by *At* during the registration of the patient P. Furthermore, we assume that *At* can access all secret information of *SMC*. In this scheme, no Kw related parameters are stored in *MS*'s database. Hence, extracting the Kw from C_{kw} without exact knowledge of the key α is a very hard problem. For that reason, a privileged insider cannot pretend the patient P to log into the *MS* because the *At* does not know Kw. As a result, the proposed scheme resists insider attacks.

5.2 Security proof

In this section, we show that the proposed protocol is secure in the formal security model. We prove its security in the random oracle model ROM under the fact that the BDH problem is computationally infeasible to be solved.

To analyze the security of the proposed method, we provide the following theorem, which shows that the proposed method is semantically secure under the BDH assumption:

Theorem 5.1. *Let h_1 and h_2 be random oracles from $\{0,1\}^*$ to G_x and from G_y to $\{0,1\}^n$, respectively. Suppose At is an attacker that has the advantage ε against the proposed protocol. Suppose At makes $qh_2 > 0$ hash function queries to h_2. Then, there is an algorithm C that solves the Bilinear Diffie-Hellman Problem with the advantage at least $\acute{\varepsilon} = \frac{2\varepsilon}{qh_2}$.*

Proof. C is given $\sigma \in \{0,1\}^{logq}, \theta_0 = V, \theta_1 = V^\alpha, \theta_2 = V^\beta, \theta_3 = V^\gamma$ where α, β, γ are random numbers in Z_q. The goal is to output $G = \acute{e}(V,V)^{\alpha\beta\gamma} \in G_y$. Let V be the solution to the BDHP. C finds G by interacting with the adversary as follows:
KeyGen: C sends (θ_0, θ_1) as the public key to At
h_1**-queries:** C maintains a list of tuples called h_1-list, in which each entry is a tuple of the form $\langle \sigma_j, \delta_j \rangle$. The list is initially empty. When At queries h_1 at a point of σ_i, C checks if $\sigma_i = \sigma_j$ where σ_j already appears on h_1-list. If so, C answers At with $h_1(\sigma_i) = \delta_j$. Otherwise, C picks a random element $\lambda \in Z_q$, computes $\delta_j = \theta_2 * V^\lambda = V^\beta * V^\lambda$, adds the tuple $\langle \sigma_i, \delta_i \rangle$ to h_1- list, and answers At with $h_1(\sigma_i) = \delta_i$.
h_2**-queries:** C maintains a list of tuples called h_2-list, in which each entry is a tuple $\langle \epsilon_j, \tau_j \rangle$. The list is initially empty. When At queries h_2 at a point of ϵ_i, C checks if $\epsilon_i = \epsilon_j$ where ϵ_j already appears on h_2-list. If so, C answers At with $h_2(\epsilon_i) = \tau_j$. Otherwise, C picks a random string $\tau_i \in \{0,1\}^n$, adds the tuple $\langle \epsilon_i, \tau_i \rangle$ to h_2-list, and answers At with $h_i(\epsilon_i) = \tau_i$.
Challenge: At outputs two keywords σ_0 and σ_1 on which it wishes to be challenged. C randomly picks $b \in \{0,1\}$ and gives θ_1 to At.
Since C is given $\theta_0, \theta_1, \theta_2$, and θ_3 as part of the BDH challenge, C creates the secure keyword by executing the keyword encryption algorithm and sends the challenge to At,
$\sigma_b = h_2(\acute{e}(h_1(\sigma), \theta_1)^\gamma)$
$= h_2(\acute{e}(h_1(\sigma), V^\alpha)^\gamma)$
$= h_2(\acute{e}(V^\beta * V^\lambda, V^\alpha)^\gamma)$
$= h_2(\acute{e}(V^{\beta+\lambda}, V^\alpha)^\gamma)$
$= h_2(\acute{e}(V,V)^{\alpha\gamma(\beta+\lambda)})$

Hence, θ_1 is a valid keyword for σ_b as required.

Guess: At outputs its guess $\acute{b} \in \{0, 1\}$ for b. C picks a random pair $\langle \epsilon_i, \tau_i \rangle$ from h_2-list and outputs ϵ_ii as the solution to the given instance of BDHP. Now, we complete the proof of the above theorem, we show that C correctly outputs M with the probability at least $2\varepsilon/q$. Let v be the event that At issues a query for z. If $-v$, we know that the decryption of the ciphertext is independent of Ats view. Let $pr[b = \acute{b}]$ be the probability that At outputs the correct result, therefore, in the real attack $pr[b = \acute{b}| - v] = \frac{1}{2}$ Since At has the advantage $\varepsilon, pr[b = \acute{b}| - v] - \frac{1}{2}| \geq \varepsilon$. Based on the following formula, we know $pr[v] \geq 2\varepsilon$:
$Pr[b = \acute{b}] = Pr[b = \acute{b}| - v]Pr[-v] + Pr[b = \acute{b}|v]Pr[v] \leq \frac{1}{2}Pr[-v] + Pr[v] = \frac{1}{2} + \frac{1}{2}Pr[v]$,
$Pr[b = \acute{b}] \geq Pr[b = \acute{b}| - v]Pr[-v] = \frac{1}{2}Pr[-v] = \frac{1}{2} - \frac{1}{2}Pr[v]$.

Therefore, we have $Pr[v] \geq 2\varepsilon$ in the real attack. That is to say, At will issue a query for τ with the probability at least 2ε. C will choose the correct pair with the probability at least $\frac{1}{qh_2}$ and thus, Cproduces the correct answer with the probability at least $\acute{\varepsilon} = \frac{2\varepsilon}{qh_2}$ as required. □

6 Performance comparisons

Here, we compare our method with the related recent existing schemes. The performance of the proposed scheme is compared with the [18, 19, 20, 21, 23, 22, 24, 25, 26] concerning their securities. In this scheme, the keyword is protected using the secret key and random oracle hash function under the Bilinear Diffie-Hellman Problem BDHP. A secret key is embedded in a smart card; it is required to extract the Kw from *SMC*. The comparison is presented in Table 1. In this table, we consider different attacks and compare our scheme with the related mentioned schemes. According to informal security analysis, it has been observed that the proposed scheme withstands all the different known attacks.

7 Conclusion

In this paper, we have first revisited a series of two-factor authentication schemes and shown that they are not secure against the off-line dictionary attack. To cope with the aforementioned defects, we have proposed a novel and

Table 1: Comparison with respect to security features.

	[18]	[19]	[20]	[21]	[23]	[22]	[24]	[25]	[26]	Our
User anonymity	×	√	√	×	×	√	√	×	√	√
Off-line dictionary attack	√	√	√	√	√	√	√	√	√	√
Replay attacks	×	×	√	√	√	√	√	√	√	√
Impersonation on attack	×	√	√	√	×	√	√	×	√	√
Stolen smart card attacks	×	√	√	√	√	√	√	√	√	√
Mutual authentication	×	√	√	×	√	√	√	×	√	√
Privileged insider attacks	√	√	√	×	√	√	×	×	×	√

secure authentication scheme using a searchable encrypted keyword, which possesses high security properties to protect the valid patient against attacks and helps the doctor to retrieve medical files containing such encrypted keywords. The protocol is proved secure in the random oracle model. The proposed method is efficient and practical compared with other existing schemes. Comprehensive security analysis shows that the robustness of the proposed method is more secure than other related schemes.

References

[1] S. H. Li, C. Y. Wang, W. H. Lu, Y. Y. Lin, D. C. Yen, ”Design and implementation of a telecare information platform,” J. Med. Syst., **36,** no. 3, (2012), 1629–1650.

[2] E. Kyriacou et al., ”Multi-purpose HealthCare Telemedicine Systems with mobile communication link support,” 2003. Accessed: Apr. 14, 2020. [Online]. Available: http://www.biomedical-engineering-online.com/content/2/1/7.

[3] F. S. Ali, H. N. Saad, F. H. Sarhan, B. Naaeem, ”Enhance manet usability for encrypted data retrieval from cloud computing,” Indones. J. Electr. Eng. Comput. Sci., **18,** no. 1, (2019), 64–74.

[4] F. S. Ali, S. F. Lu, ”Public Key Encryption with Conjunctive Field Free Keyword Search Scheme Indexing terms, **15,** no. 14, (2016), 7423–7434.

[5] F. S. Ali, S. Lu, ”Searchable encryption with conjunctive field free keyword search scheme,” Proc. 2016 Int. Conf. Netw. Inf. Syst. Comput., ICNISC 2016, (2017), 260–264.

[6] L. Lamport, ”Password Authentication with Insecure Communication,” Commun. ACM, **24,** no. 11, (1981), 770–772.

[7] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li, A. Alelaiwi, ”Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy,” Nonlinear Dyn., **83,** no. 4, (2016), 2085–2101.

[8] D. Wang, P. Wang, ”Two Birds with One Stone: Two-Factor Authentication with Security beyond Conventional Bound,” IEEE Trans. Dependable Secur. Comput., **15,** no. 4, (2018), 708–722.

[9] Y. Zhao, S. Li, L. Jiang, ”Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment,” 2018.

[10] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, Y. Chung, ”A Secure Authentication Scheme for Telecare Medicine Information Systems,” J. Med. Syst., **36,** no. 3, (2012), 1529–1535.

[11] H. M. Chen, J. W. Lo, C. K. Yeh, ”An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems,” in Journal of Medical Systems, **36,** no. 6, (2012), 3907–3915.

[12] Q. Jiang, J. Ma, Z. Ma, G. Li, ”A privacy enhanced authentication scheme for telecare medical information systems,” J. Med. Syst., **37,** no. 1, (2013), 1–8.

[13] H. Y. Lin, ”On the security of a dynamic ID-based authentication scheme for telecare medical information systems,” J. Med. Syst., **37,** no. 2, (2013), 1–5.

[14] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, L. He, ”A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems,” J. Med. Syst., **38,** no. 1, (2014), 9994.

[15] G. Panchal, D. Samanta, S. Barman, ”Biometric-based cryptography for digital content protection without any key storage,” Multimed. Tools Appl., **78,** no. 19,(2019), 26979-27000.

[16] D. Boneh, M. Franklin, ”Identity-based encryption from the weil pairing,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), **2139,** LNCS, no. 3, (2001), 213–229.

[17] M. Bellare, P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing EEcient Protocols," ACM, 1993.

[18] M. C. Chuang, M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," Expert Syst. Appl., **41,** (2014), 1411–1418.

[19] D. Mishra, A. K. Das, S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards, Expert Syst. Appl., **41,** no. 18, (2014), 8129–8143.

[20] R. Amin, G. P. Biswas, A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TIMS, J. Med. Syst., **39,** no. 3, (2015), 33.

[21] H. Lin, F. Wen, C. Du, "An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics," Wirel. Pers. Commun., **84,** no. 4, (2015), 2351–2362.

[22] A. Irshad, S. A. Chaudhry, S. Kumari, M. Usman, K. Mahmood, M. S. Faisal, "An improved lightweight multiserver authentication scheme," Int. J. Commun. Syst., **30,** no. 17, (2017), e3351.

[23] Y. Lu, L. Li, X. Yang, Y. Yang, "Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards," PLoS One, **10,** no. 5, (2015), e0126323.

[24] R. Ali, A. K. Pal, "Three-Factor-Based Confidentiality-Preserving Remote User Authentication Scheme in Multi-server Environment," Arab. J. Sci. Eng., **42,** no. 8, (2017), 3655–3672.

[25] C. Wang, X. Zhang, Z. Zheng, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme," PLoS One, **11,** no. 2, (2016), e0149173.

[26] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues, Y. Park, "Provably Secure Multi-Server Authentication Protocol Using Fuzzy Commitment," IEEE Access, **6,** (2018), 38578–38594.