Three Factor Authenticated Key Agreement Scheme for Telecare Medicine Information System Using Chebyshev Chaotic Maps

T. Janani and Dr. P. Gokulakrishnan

1PG Student, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul.
2Assistant Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul.

Received 28 January 2017; Accepted 22 May 2017; Available online 28 May 2017

ABSTRACT
Telecare Medicine Information System (TMIS) is an effective technology in which patients can remain at their home and get suggestions for medical treatment through the internet. One of the challenges faced by this system is security of medical data. Hence mutual authentication and session key establishment on a medical server between doctor and a patient are required for enhancing security of TMIS. Password authentication schemes have been widely used as a security scheme in TMIS. Most of the Password authentication schemes are associated with chaotic map. However, they are vulnerable to various attacks such as offline password guessing attack, man-in-the-middle attack, stolen smart card attack etc. The Objective of this work is to provide medical data security, privacy and user access authentication. It shows that, the biometrics based password authentication scheme using extended chaotic maps had been used, which secured TMIS from vulnerable attacks such as outsider attack, impersonation attack and replay attack in the existing system. Though it provides user anonymity, forward secrecy and session key security, it does not consider about privacy protection. The proposed system introduces three factor (password, smart card and biometrics) authenticated key agreement scheme using chebyshev chaotic map to provide privacy protection. The proposed system enhances the security of TMIS against vulnerable attacks such as man-in-middle attack, replay attack and provides various features such as user anonymity, perfect forward secrecy, efficient login and password updating.

KEYWORDS: Telecare Medical Information System, Mutual Authentication, Key Establishment, Biometrics-based Password Authentication, Extended Chaotic Maps, Chebyshev Chaotic Map.

INTRODUCTION
Network security is defined as the authorization of access to data in the network based on the different policies for preventing and monitoring the authorized access, misuse, modification or any other denial-of-attacks and is controlled by the network administrator. Users are selected or assigned their ID and password or other authentication information which allows them for accessing the information and programs within their authority. Network security is mostly used in different applications like transactions and communications among different businesses, government agencies and individuals.
The easiest way for protecting the network resource is by assigning the unique name and corresponding password. In addition, the security management is also varies for different applications. For example, small office or home requires fundamental security whereas large businesses requires the high-maintenance and advanced software and hardware for preventing the malicious attacks from hacking and spamming.

User authentication is defined as the verification of an individual-to-machine transfer of credentials for confirming the user’s authentication. The network security is initiated with the user authentication which involves the username and password and it is termed as one-factor authentication. If the user utilizes the security token or dongle, ATM card, or mobile phone along with the user name and password, then it is called as two-factor authentication. If the user utilizes the biometrics such as fingerprint, retinal scan and etc, then it is termed as three-factor authentication.

Once the authentication is completed then the firewall enforces the access policies to the user such that what services are allowed to be accessed by the network users. However it may be failed for checking the harmful content like computer worms or Trojans which are transmitted over the network. Such malware actions are detected by using the anti-virus software or an Intrusion Prevention System (IPS). Communication between two hosts is encrypted by using different encryption methods for maintaining the privacy. Nowadays, different biometrics-based encryption methods are also developed for improving the security and protecting the network from different malicious attacks. However, there are several challenges are occurred in terms of computational time complexity, security and etc. Therefore, in this paper, the modified biometric-based password authentication technique is proposed based on the chebyshev chaotic map scheme.

Literature Survey:

Lam et al [1] presented the major architecture and functional characteristics of the authentication system. In addition, the security features are investigated which are provided by the smart cards are developed for ensuring the confidentiality and integrity of the medical data stored in the patient cards. The advantages of the Health-Insurance smart card are also discussed. However, this system is not analyzed for large-scale database.

Xie et al [2] proposed the anonymous Three-Party Password Authenticated Key Exchange (3PAKE) protocol. In the proposed approach, the pi calculus is applied for providing the security based on the formal verification tool named ProVerif and achieving the mutual authentication and session key security. The proposed method is used for resisting the off-line password guessing attack. It detects the attack if an adversary launches the on-line password guessing attack. However, there are still security risks are happened.

Wu et al [3] proposed the novel authentication method which is utilized for incorporating the pre-computing idea to the communication process for eliminating the exponential computation time complexity. However, this method is vulnerable to the insider and impersonation attacks. He et al [4] proposed the authentication method for mobile devices which are used in TMIS. The proposed system is utilized for improving the security but vulnerable to the off-line password guessing attacks.

Wei et al [5] proposed the improved authentication method for Telecare medicine information system. In addition, the two-factor authentication such as smartcard based password authentication method is also developed. However, the proposed method is insecure for the off-line password guessing attack. Tseng et al [6] presented the protocol for defending the replay attacks, forgery attacks and stolen-verifier attacks effectively. However, this protocol is not used for providing the user anonymity.

Niu et al [7] proposed the protocol for improving the security and preserving the user anonymity. Moreover, the key agreement protocol is proposed for sharing the secret key for specified parties and also helping the communication parties in order to establish the shared secret session key. However, this method is vulnerable to the man-in-the-middle attacks. Guo et al [8] proposed the novel chaotic maps-based password authenticated key agreement protocol along with the smartcards. The proposed method has comprehensive
characteristics for improving the security requirements. However, the user anonymity is not ensured by this method.

Hao et al [9] proposed the chaotic map-based authentication method for Telecare medicine information systems. Here, the medical servers are utilized for maintaining the electronic medical records (EMR) of the registered users and providing the different services. However, this scheme is not effective for establishing the session key. Jiang et al. [10] proposed the robust authentication and key agreement method in order to provide the improved efficiency. In the proposed method, the two-factor authentication method is designed based on the privacy protection assumptions. However, this method is not used for resisting the service misuse attack for non-registered users.

**Password Authentication Using Three Factor Authenticate Key:**

In this section, the proposed system is explained in detail. The proposed system is used for enhancing the security against the vulnerable attacks by using the three-factor authenticated key agreement method which utilizes the chebyshev chaotic map-based cryptography along with less computational time complexity. The transmitted medical data through the open channel is protected and realized during the remote diagnosing process. In the proposed system, there are five phases are included such as initial phase, modified registration phase, login phase, authentication phase and password and biometrics update phase. The proposed system is used for resisting the guessing password attacks by using the Chaotic Map Discrete Logarithm problem (CMDLP) and Chaotic Map Computational Diffie-Hellman problem (CMCDHP) and enhancing the privacy protection. The proposed mechanism has different advantages such as it provides the resist against replay attack, man-in-the-middle attack and it has less time complexity.

**A. Basic TMIS Setup:**

The Telecare Medical Information System (TMIS) is developed based on the server client model where the server acts as the hospital environment and the clients are acts as patients. Patients may be saved the large amount of time by utilizing the TMIS and easily accessing the doctors. For example, the hypertension patients or diabetes mellitus patients are directly exchanging their medical data on daily basis through the TMIS and the doctors are collected the patient’s medical data without requirement of patients visiting the hospital or the clinic.

**B. Privacy Preserving of Biometric Data:**

In this module, privacy preservation of user’s fingerprint is implemented. We consider minutiae points (ridge ending and bifurcations) as the biometric features. The features are stored as (x, y) form, where (x, y) denotes coordinate value. For all fingerprint images, the number of minutiae points for a person lies within 50. However, in case, if there are more than 50 minutiae points (i.e., N ≥ 50), then first 50 minutiae points according to their quality value would be selected and the rest be discarded. The fingerprint template is transformed into non-invertible forms, called cancellable templates, to provide revocability as well as privacy to the fingerprint data.

**C. Registration Phase:**

(i) U inputs his/her biometrics feature BIO, and selects an identity ID and a password PW. Then, U computes $\text{PWD} = h_1(\text{PW} \parallel H(\text{BIO}))$, and sends {ID, PWD} to S over a secure channel.

(ii) S computes $K = h_3(ID \parallel \text{PWD})$ and $\text{IM} = K \oplus h_4(k_s)$, where $k_s$ is S’s secret key. S then issues a smart card containing $(\text{IM}_s, h_1(\cdot), h_2(\cdot), H(\cdot))$ to U.

(iii) U selects a secret key $k_u$ and computes $f = h_3(ID \parallel k_u) \oplus \text{PWD}$. Then, User U stores $f$ on to the smart card; so, it is noted that the smart card of User U contains the information $(\text{IM}_s, f, h_1(\cdot), h_2(\cdot), H(\cdot))$.

**D. Login and Authentication Phase:**

(i) User inserts the smart card into a card reader and enters his/her identity ID, password PW, and secret key $k_u$ and also imprints his/her biometrics BIO at the sensor. U then checks whether $h_3(ID \parallel k_u) \oplus h_1(\text{PW} \parallel H(\text{BIO})) = f$; if it holds, U computes $K = h_1(ID \parallel h_1(\text{PW} \parallel H(\text{BIO})))$; generates a random number $u$, and computes $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$ and $R_3 = h_1(ID \parallel T_u(K))$. Lastly, U sends the message $\{R_1, R_2, R_3\}$ to S.

(ii) After receiving the login request message from U, S uses the secret key $k_s$ to derive K by computing $K' = IM_1 \oplus h_4(k_s)$. Then computes $ID = R_1 \oplus K$ and $T_u(K) = ID \oplus R_2$, and checks $h_3(ID \parallel T_u(K)) = R_3$; if it is correct, S then generates a random number $v$ and computes $IM_2 = T_u(K) \oplus ID$ and $sk = h_2(T_u(K), T_v(K), T_{uw}(K))$ and $Auth_u = h_1(K \parallel T_v(K) \parallel sk)$. Lastly, S sends the message $\{Auth_u, IM_2\}$ to U.
(iii) Upon receiving the login response message from S, U derives $T_s(K)$ by computing $IM_2 \oplus ID$, and computes $sk = h_2(T_s(K), T_v(K), T_{uv}(K))$ to verify whether $h_1(sk \parallel T_v(K) \parallel s) = Auth_u$ is equal to the received Auths. If it is holds, U successfully authenticates S and computes $Auth_u = h_1(sk \parallel T_v(K) \parallel K)$, and then sends the message $\{Auth_u\}$ to S.

(iv) Upon receiving the message from U, S validates whether $h_1(sk \parallel T_v(K) \parallel K) = Auth_u$. If it is true, S successfully authenticates U; otherwise, S aborts the request. Lastly, U and S have the common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

E. Update Phase:
If User U wants to change his/her password, U inserts his/her smart card into the card reader and keys in ID, PW, $k_o$, and BIO. Then, the smart card checks whether $h_1(ID||k_o) \oplus h_1(PW||H(BIO)) = f$; if it holds, U submits a new password $PW_{new}$ as well as a new secret key $k_o(new)$. The smart card then computes $f_{new}$, followed by the replacement off with $f_{new}$.

F. Modified Registration Phase:
(i) U inputs his/her modified biometrics characteristic PP-BIO, and selects an identity ID and a password PW. Then, U computes $PWD = h_1(PW \parallel H(PP - BIO))$ and sends $\{ID, PWD\}$ to S over a secure channel.

(ii) S computes $K = h_1(ID \parallel PWD)$ and $IM_1 = K \oplus h_1(k_s)$ where $k_s$ is S’s secret key. Then issues a smart card containing $\{IM_1, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ to U.

(iii) U selects a secret key $k_s$ and computes $f = h_1(ID \parallel k_s) \oplus PWD$. Then, U stores $f$ onto the smart card; therefore, it is noted that the smart card of U contains the information $\{IM_1, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$.

G. Login and Registration Phase:
(i) User U first inserts the smart card into a card reader and inputs his/her identity ID, password PW, and secret key $k_{o}$ and also imprints his/her biometrics PP-BIO at the sensor. U then checks whether $h_1(ID \parallel k_o) \oplus h_1(PW \parallel H(PP - BIO)) = f$; if it holds, U computes $K = h_1(ID \parallel h_1(PW \parallel H(PP - BIO)))$, generates a random number $u$, and computes $R_1 = K \oplus ID, R_2 = ID \oplus T_u(K)$, and $R_3 = h_1(ID \parallel T_u(K))$. Lastly, U sends the message $\{R_1, R_2, R_3\}$ to S.

(ii) After receiving the login request message from U, S uses the secret key $k_s$ to derive K by computing $K' = IM_1 \oplus h_1(k_s)$. He/she then computes $ID = R_3 \oplus K$ and $T_u(K) = ID \oplus R_2$, and checks $h_1(ID \parallel T_u(K)) = R_3$; if it is correct, S then generates a random number $v$ and computes $IM_2 = T_v(K) \oplus ID, sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ and $Auth_v = h_1(K \parallel T_v(K) \parallel sk)$. Lastly, S sends the message $\{Auth_v, IM_2\}$ to U.

(iii) Upon receiving the login response message from S, U derives $T_s(K)$ by computing $IM_2 \oplus ID$, and computes $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ to validate whether $h_1(sk \parallel T_v(K) \parallel s) = Auth_v$ is equal to the established $Auth_v$. If it is holds, User successfully authenticates S and computes $Auth_u = h_1(sk \parallel T_v(K) \parallel K)$ and then sends the message $\{Auth_u\}$ to S.

(iv) Upon receiving the message from U, S validates whether $h_1(sk \parallel T_v(K) \parallel K) = Auth_u$. If it is true, S successfully authenticates U; otherwise, S aborts the request. Lastly, U and S have the common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

H. Update Phase:
If User U wants to change his/her password, U first inserts his/her smart card into the card reader and keys in ID, PW, $k_o$, and PP-BIO. Then, the smart card checks whether $h_1(ID||k_o) \oplus h_1(PW||H(PP-BIO)) = f$; if it holds, U submits a new password $PW_{new}$ as well as a new secret key $k_o(new)$. The smart card then computes $f_{new}$, followed by the replacement off with $f_{new}$.

I. Attacker Phase:
(i) Outsider attack: Let A be an active adversary who owns a smart card and can extract the information of the legal user $\{IM_1, h_1(\cdot), h_2(\cdot), f, H(\cdot)\}$. He/she can then easily obtain $h_1(k_{o})$ that is similar for each authorized user and is the hash value of the secret key that is chosen by server S.

(ii) A computes $PWD_A = h_1(PW_A \parallel H(BIO_A))$ and $K_A = h_1(ID_A \parallel PWD_A)$; then, he/she can obtain $h_1(k_{o})$ by calculating $IM_1 \oplus K_A$.

(iii) User impersonation attack: As described in this subsection, an outsider adversary A can also impersonate a legal user U to defraud the server S because he/she can know the hidden value K of U. The details are described as follows:
1. A generates a random number u' and computes $T_u(K)$. $R_2 = ID \oplus T_u(K)$, and $R_3 = h_1(ID \parallel\parallel T_{u'}(K))$.

2. Then, A sends the login request message [$IM_1$, $R_1$, $R_2$, $R_3$] to S.

3. After receiving the login request message from A who pretends to be U, the messages can successfully send S’s verification and S does the following scheme normally. Then, S sends the login response message {Authu, $IM_2$} to A, where v is the random number on the server side.

4. Upon receiving the login response message from S, A computes $T_v(K) = IM_2 \oplus ID \parallel T_{u'}(K) = T_{u'}(K)$, $sk = h_2(T_u(K), T_v(K), T_{u'}(K))$ and $Auth_u = h_3(sk \parallel ID \parallel K)$). Then, A sends the authentication message {Authu} to S.

5. When receiving the message {Authu} from A, S continues to proceed with the scheme without being detected. Lastly, A and S “successfully” agree on a shared session key $s_k$; however, an unfortunate outcome occurs, as S incorrectly believes that he/she is communicating with the legal user U.

(iv) Server impersonation attack: An outsider adversary A can also impersonate a server S to cheat user U because he/she knows the secret value $h_1(k)$ of server S. A performs the following steps:

1. When U is sending the login request message [$IM_1$, $R_1$, $R_2$, $R_3$] to server S, A can intercept this message and compute $K = IM_1 \ominus h_1(k_o)$.

2. A generates a random number $v'$ and computes $IM_2 = T_v(K) \oplus ID$, $sk = h_2(T_u(K), T_v(K), T_{u'}(K)) \parallel Auth_u = h_3(K \parallel T_v(K) \parallel sk)$.

3. Lastly, A sends the login response message {Auth, $IM_2$} to U.

4. After receiving the login response message {Auth, $IM_2$} from A, U continues to proceed with the scheme without being detected. Lastly, U and A “successfully” agree on a shared session key $s_k$; however, an unfortunate outcome occurs, as U mistakenly believes that he/she is communicating with the server S.

Thus, the proposed biometric based password authentication system provides more robustness and security for Telecare Medicine Information Systems (TMIS).

**Experimental Results:**

In this section, the performance of the proposed system is compared to the previous techniques in terms of security analysis and performance analysis. In the proposed approach, the server database contains the information about the patients such as patients ID, mail ID, patient’s biometric information, and their medical information like blood group, diseases which he or she treated by the hospital. In addition, the patient’s doctor information and the next checkup data or appointments of the patient are also included.

**A. Security Analysis:**

The security analysis of the proposed method is evaluated based on the different assumptions such as follows:

(i) The adversary is either user or server and both registered user and server acts as the adversary.

(ii) The adversary is eavesdropping on every communication which is occurred on the public channels.

(iii) The adversary has the ability for changing, deleting or rerouting the captured message.

(iv) The information is extracted from the smartcard by examining the power consumption of the card.

The security analysis is shown in table 1. Thus the table 1 shows that the proposed scheme has more security and robustness compared with the other schemes.

**B. Performance Analysis:**

The performance analysis of the proposed scheme is evaluated in terms of time and message exchange.

---

**Table 1: Security Attributes Comparison**

<table>
<thead>
<tr>
<th>Security Attributes</th>
<th>Modified biometric-based password authentication key agreement scheme</th>
<th>Biometric-based password authentication key agreement scheme</th>
<th>Chaotic map-based password authentication key agreement scheme</th>
<th>Improved chaotic maps-based password authentication key agreement scheme</th>
<th>Chaotic map-based authentication and key agreement scheme with strong anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>User anonymity</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Stolen smartcard attack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Session key security</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Insider attack</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Perfect forward secrecy</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

---
The Chebyshev chaotic map using modified biometric-based password scheme shows that the proposed scheme has better performance than other schemes and it has very minimum amount of time consumption and exchanges number of messages by using the modified biometric-based password.

**Conclusion:**

In this paper, the authentication issues due to different attacks and security failure problems are demonstrated. The authentication problems due to different attacks are removed by the proposed modified biometric based password authentication method. In the proposed method, the three-factor authenticated key agreement method is developed by using the chaotic map-based cryptography for addressing the authentication issues. Therefore, the proposed method is used for realizing the protection of medical data transmitted in the open channel and providing the privacy protection during the remote diagnosing process which is utilized for enabling the patient in order to have the secure and convenient healthcare through the TMIS. Hence, the security analysis and performance analysis are proved that the proposed method has better performance than the other methods. Hence, the proposed method is mostly suitable for different applications in TMIS environments.

**REFERENCES**