J Med Syst (2013) 37:9964
DOI 10.1007/s10916-013-9964-1

ORIGINAL PAPER

# A Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce

**Amit K. Awasthi · Keerti Srivastava**

Received: 16 July 2013 / Accepted: 31 July 2013 / Published online: 16 August 2013


**Abstract** In recent years, the increased availability of lower-cost telecommunications systems and customized patients monitoring devices made it possible to bring the advantages of telemedicine directly into the patient's home. These telecare medicine information systems enable healthcare delivery services. These systems are moving towards an environment where automated patient medical records and electronically interconnected telecare facilities are prevalent. Authentication, security, patient's privacy protection and data confidentiality are important for patient or doctor accessing to Electronic Medical Records (EMR). A secure authentication scheme will be required to achieve these goals. Many schemes based on cryptography have been proposed to achieve the goals. However, many schemes are vulnerable to various attacks, and are neither efficient, nor user friendly. Specially, in terms of efficiency, some schemes are resulting in high time cost. In this paper we propose a new authentication scheme that is using the precomputing to avoid the time-consuming exponential computations. Finally, it is shown to be more secure and practical for telecare medicine environments.

**Keywords** Telecare medicine information system · Authentication · Biometric · Nonce

A. K. Awasthi (✉)
School of Vocational Studies and Applied Sciences,
Gautam Buddha University, Greater Noida 201312, India
e-mail: awasthi.amitk@gmail.com

K. Srivastava
Central Institute of Plastic Engineering and Technology,
Lucknow, India
e-mail: keerti.cipet@gmail.com

## Introduction

Telecare medicine information systems are essential part of this cloud computing age. There are various low-cost handheld telecommunication systems and customized patient monitoring devices. By using these devices advantage of telehealth are reaching directly to the patient home. In such systems, users is connected with various types of networks - wired or wireless. These systems therefore are vulnerable to attackers. To access these services, authentication between both parties becomes an essential need. The host server need authentication to safe its records from unauthorized person. It should ensure the privacy of the patient. On the other hand, patient needs the authentication from server, so that intruder should not be able to impersonate the server.

In 1981, Lamport [9] proposed a solution to the problem of remote authentication using cryptographic hash functions. However, high hash overhead and the necessity for password resetting decreases its suitability for practical use. Since then, many improved password authentication schemes e.g. [10, 12, 14] have been proposed. One of the common feature of these schemes is that the server has to securely store a verification table. If the the verification table is stolen by the adversary, the system may be broken. To resist such a stolen-verifier attack, in 1990, Hwang et al. [7] proposed a non-interactive password authentication scheme and its enhanced version, which additionally uses smart cards. In Hwang et al.'s schemes, the server does not require any verification table. In 2000, Hwang and Li [11] proposed a verification-free password authentication scheme using smart cards based on ElGamal's public-key technique [13]. However, Hwang-Li's scheme doesn't allow users freely choosing and changing their passwords. Furthermore, Hwang-Li's scheme was found to be vulnerable to various impersonation attacks [2, 3, 6].

A remote user authentication scheme mainly employs the possession of a smart cards or such other device and/or the knowledge of a secret (password, etc.) in order to establish the identity of an individual. However, a smartcard can be lost, stolen [15], misplaced, or willingly given to an unauthorized user; and a secret can be forgotten, guessed, and willingly or unwillingly be disclosed to an unauthorized user. Therefore, biometric techniques have emerged as a powerful tool for remote user authentication to resolve these problems. Since it is based on the physiological and behavioral characteristics of an individual, biometrics does not suffer from disadvantages found in traditional authentication methods. Also, biometrics and smartcard have the potential to be a very useful combination. First, the security and convenience of biometrics allow for the implementation of high-security applications regarding smartcards. Second, smartcards represent a secure and portable way of storing biometric templates, which would otherwise need to be stored in a central database

Chaotic cryptography with its random behavior constitutes a potential protection a set in modern cryptography. Few schemes in literature, based on new family of one-way collision free chaotic hash function [1] showed its supremacy over modular exponentiation-based authentication schemes e.g. Diffie-Helman [1] El Gamal [13] and RSA based encryption algorithms [5].

## Related works

### Chaotic hash function

This section briefly reviews chaotic hash function. The proposed scheme is based on the following one-dimensional and chaotic piecewise linear map:

$$x_{i+1} = \begin{cases} x_i/\beta & \text{if } 0 \le x_i < \beta \\ (x_i - \beta)/(0.5-\beta) & \text{if } \beta \le x_i < 0.5 \\ (1 - x_i - \beta)/(0.5-\beta) & \text{if } 0.5 \le x_i < 1-\beta \\ (1-x_i)/\beta & \text{if } 1-\beta \le x_i \le 1 \end{cases}$$

where $x_i \in [0, 1]$, $\beta \in (0, 0.5)$ is the control parameter. The map is piecewise linear, and the parameter $\beta$ ensures that the map runs in a chaotic state when $0 < \beta < 0.5$ It transforms an interval [0, 1] onto itself and contains only one parameter $\beta$. Let $x_i$ be the chaining variable and has initial value $x_0$. That is specified as part of the hash algorithm. $H_0$ is encryption key for the remaining message $M$. Given a remaining message $M$, $H_0$ is a constant which is chosen from (0, 1). Now the three step iteration, 1st to $n$th, $(n+1)$th to $2n$th, and $(2n+1)$th to $3n$th, ensure that each bit of the final hash valuewill be related to all bits of messages. (Refer [4])

### Chaotic map based nonce

The following spatially generated 2D logistic systems can be used in the proposed scheme to generate a nonce (a pseudo random binary sequence). (Refer [8])

$$x_{m+1,n} + w x_{m,n+1} = 1 - (\mu(1+w)x_{m,n})^2$$

Here $x_{m,n}$ is the spatial state of the system, $w$ is a real constant and $\mu$ is a positive parameter. Research shows that when $2 > \mu \ge 1.55$ and $w \in (-1, 1)$, the system is in chaotic state.

Generating a nonce from the orbit of a chaotic map essentially requires mapping the state of the system to {0, 1}. A simple way to generate a bit sequence from a chaotic real valued signal is as follows:

$$b_x = \begin{cases} 1 & \text{if } x_{m,n} > c \\ 0 & \text{if } x_{m,n} < c \end{cases}$$

where $c$ is chosen threshold such that likelihood of $x_{m,n} > c$ is equal to that of $x_{m,n} < c$. We choose 128 bit block in proposed scheme as this is cryptographically secure.

## Proposed biometric authentication nonce based scheme

The proposed scheme consists of four phases: registration, login, authentication, password change. Information held by Remote System: $x$, $h_c(.)$

### Registration phase

Figure 1 shows the registration phase of proposed scheme. In the registration phase user $U_i$ chooses his/her identity $ID_i$ and password $pw_i$, a random nonce $n$ and interactively submits $ID_i$, $E_{pu}(pw_i \oplus n)$ encrypted with public key $pu$ to the registration center. $U_i$ also imprints his/her fingerprint impression $\gamma = (S_i \oplus n)$ at the sensor, and then registration system performs the following operations:

1. Decrypt the encrypted message by the server private key $pr$ and get $\alpha = (pw_i \oplus n)$.
2. Compute $(pw_i \oplus S_i)$ from $\alpha = (pw_i \oplus n)$ and $\gamma = (S_i \oplus n)$.
3. Computes $A_i = h_c(ID_i \oplus x)$ and $X_i = h_c(A_i)$ where $x$ is the private key of the remote system, $\oplus$ is a bit-wise exclusive-OR operation, $h_c(.)$ is a collision free one-way chaotic hash function.
4. Computes $V_i = A_i \oplus h_c(pw_i \oplus S_i)$ where $S_i$ is the extracted fingerprint template of the user.
5. The remote system personalizes the secure information $ID_i$, $X_i$, $V_i$, $S_i$, $h_c(.)$ and saves it into the mobile device system of the $U_i$.

USER $U_i$ REMOTE SYSTEM $S$

$ID_i, pw_i, n, S_i$

$\alpha = (pw_i \oplus n)$

$\beta = E_{pu}(\alpha)$

$\gamma = S_i \oplus n$ $\quad U_i \overset{ID_i,\beta,\gamma}{\longrightarrow} S \quad$ $D_{pr}(\beta) = \alpha = (pw_i \oplus n)$

$\alpha \oplus \gamma = (pw_i \oplus S_i)$

$A_i = h_c(ID \oplus x)$

$X_i = h_c(A_i)$

$V_i = A_i \oplus h_c(pw_i \oplus S_i)$

$U_i \overset{ID_i,X_i,V_i,S_i,h_c(.)}{\longleftarrow} S$

**Fig. 1** Registration phase

Login phase

Figure 2 shows the login phase of the proposed scheme. If $U_i$ wants to login the remote system, he or she opens the login application software, enters identity $ID_i$ and password $pw_i*$ and imprints a fingerprint biometric at the sensor. If $U_i$ is successfully verified by his/her fingerprint biometric, a mobile device will perform the following operations:

1. Computes $B_i = V_i \oplus h_c(pw_i * \oplus S_i)$, and verifies whether $h_c(B_i) = X_i$ or not. If equal the user's device performs further operation; otherwise it terminates the operation.
2. Computes $D_1 = h_c(B_i \oplus T_u)$, where $T_u$ is the current time stamps of the device.
3. At the end of the login phase, $U_i$ sends the login message $m = (ID_i, D_1, T_u)$ to the remote system over an insecure network.

Authentication phase

In the authentication phase, when the remote system receives the message $m = (ID_i, D_1, T_u)$ from the user, the remote system and user perform following operations.

1. The remote system checks if the format of $ID_i$ is invalid or if $T_s = T_u$ where $T_s$ is the current time stamp of the remote system, then rejects the login request.

USER $U_i$ REMOTE SYSTEM $S$

$ID_i, pw_i$

$B_i = V_i \oplus h_c(pw_i \oplus S_i)$

$h_c(B_i) = X_i$

$T_u$

$D_1 = h_c(B_i \oplus T_u)$ $\quad \overset{ID_i,D_1,T_u}{\rightarrow} \quad$ $?ID_i$

$?T_s - T_u \prec \Delta T$

$D_1* = h_c(h_c(ID_i \oplus x) \oplus T_u)$

$D_1* = D_1$

$\overset{D_2,T_s}{\leftarrow} \quad D_2 = h_c(h_c(ID_i \oplus x) \oplus T_s)$

$D_2* = h_c(B_i \oplus T_s)$

$D_2* = D_2$

**Fig. 2** Login phase

2. If $(T_s - T_u) \succ \Delta T$, Where $\Delta T$ denotes the expected valid time interval for transmission delay, then the remote system rejects the login request.
3. The remote system computes $D_1* = h_c(h_c(ID_i \oplus x) \oplus T_u)$. If $D_1*$ is equal to the received $D_1$. It means the user is authentic and the remote system accepts the login request and performs the next step, otherwise the login request is rejected.
4. For mutual authentication, the remote system computes $D_2 = h_c(h_c(ID_i \oplus x) \oplus T_s)$ and then sends a mutual authentication message $D_2, T_s$ to the $U_i$.
5. Upon receiving the message $D_2, T_s$, the user verifies that either $T_s$, is invalid or $T_s = T_u$, then the user $U_i$ terminates this session; otherwise performs the next step.
6. $U_i$ computes $D_2 = h_c(B_i \oplus T_s)$ and compares $D_2* = D_2$. If equal, the user believes that the remote party is an authentic, and it holds mutual authentication between.

Password change phase

When user wants to update his password, he can use following clint side protocol:

1. User inputs his credential $S_i$ and request smartcard reader to update password. After valid authentication system asks old password and new password.
2. User submits old password $pw_i$ and new password $pw_i^{new}$.
3. system computes

$$V_i^{new} = V_i \oplus h_c(pw_i \oplus S_i) \oplus h_c(pw_i^{new} \oplus S_i)$$

and it updates the smartcard information $V_i$ to $V_i^{new}$.

Now information on smartcard is $\{ID_i, X_i, V_i^{new}, S_i, h_c(.)\}$. Thus Password now changed.

## Security analysis

Next, this section shows that the improved scheme is secure against the impersonation attack, privileged insider attack, the stolen verifier attack, and this section analysis the enhanced security features of our improved scheme.

Resistance to guessing attack

A guessing attack involves an adversary tries to get long-term private keys (user's password or server secret and private key), but using non invertible chaotic hash function for any attacker it becomes difficult to extract $A_i$ by knowing $X_i = h_c(A_i)$ . Although the adversary can obtain the secret information stored in the stolen smart card by analyzing the leaked information [15] however adversary could not be able to extract $A_i$.

Resistance to parallel session, reflection attack

In parallel session attack, without knowing the correct password of the user, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server. but our proposed scheme is free from parallel session attack.

Resistance to insider attack

If an insider of $S$ has obtained $U_i's$ password $pw_i$. He can try to impersonate $U_i$ to access other server. In the registration phase of the improved scheme, $U_i$ sends encrypted password with appropriate nonce, i.e., $E_{pu}(pw_i \oplus n)$ thus $pw_i$ will not be revealed to $S$ without knowing remote system's private key.Since the insider can not obtain $pw_i$, the improved scheme can withstand the insider attack.

Resistance to server spoofing attack

The spoofing attack completely solved by providing mutual authentication between user and server.Since remote system $S$ sends mutual authentication message $[D_2]$ to the user in login phase. If an attacker intercepts it and re-send the forged message i.e. $[D_2']$ to user $U$, it will not be verified by authentication phase since $D_2{}^* = h_c(B_i \oplus T_s) \neq D_2'$. Therefore proposed scheme can withstand the spoofing attack.

## Conclusion

This paper proposes a secure Biometric Authentication Scheme for Telecare Medicine Information Systems with nonce with better resistance to the to the impersonation attack, the stolen smart card attack, the privileged insider attack.

**Conflict of interests** The authors declare that they have no conflict of interest.

## References

1. Menezes, A. J., Oorschot, P. C., and Vanstone, S. A., *Handbook of applied cryptography*. CRC Press, 1997.
2. Chang, C. C., and Hwang, K. F., Some forgery attack on a remote user authentication scheme using smart card. *Informatica* 14(3):289–294, 2003.
3. Chan C. K., and Cheng, L. M., Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron*, 46(4):992–993, 2000.
4. Deng, S., Xiao, D., Liao, X., One-way hash function construction based on chaotic map with changeable parameter. *Chaos, Solitons Fractals*, 24:65–71, 2005.
5. Sun, H. M., An efficient remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron*, 46(4):958–961, 2000.
6. Yeh, H. T., Sun, H. M., and Hsieh, B. T., Security of a remote user authentication scheme using smart cards. *IEICE Trans. Commun.*, B(1)(E87):192–194, 2004.
7. Hwang, T., Chen, Y., and Laih, C.-S., Non-interactive password authentications without password tables. In: *Computer and Communication Systems, 1990. IEEE TENCON'90., 1990 IEEE Region 10 Conference on*, Vol. 1, pages 429–431 1990.
8. Liu S., and Sun, L., Cryptographic pseudo random sequence from spatial chaotic map. *Chaos Solitions Fractals* 41:2216–2229, 2009.
9. Lamport, L., Password authentication with insecure communication. *Commun. ACM*, 24:770–772, 1981.
10. Sandirigama, M., Shimizu, A., and Noda, M. T., Simple and secure password authentication protocol(sas). *IEICE Trans. Commun.*, B(6)(E83):1363–1365, 2000.
11. Hwang, M. S., and Li, L. H., A new remote user authentication scheme using smart card. *IEEE Trans. Consum. Electron.*, 46(1):28–30, 2000.
12. Haller, N. H., The s/key(tm) one time password system. In: *Proceedings Internet Society Symposium on Network and Distributed System Seurity*, pages 151-158, 1994.
13. Elgamal, T., A public key cryptosystem and a signature scheme based on discrete logarithm. *EEE Trans. Inf. Theory*, 31(4):469–472, 1985.
14. Chen T. H., and Lee, W. B., A new method for using hash function to solve remote user authentication. *Comput. Electr. Eng.*, 34(1):53–62, 2008.
15. Messerges, T. S., Dabbish, E. A., and Sloan, R. H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.*, 51(5):541–552, 2002.