Publications

Available Online

J. Sci. Res. **13** (2), 407-413 (2021)

JOURNAL OF SCIENTIFIC RESEARCH

www.banglajol.info/index.php/JSR

Cryptanalysis of Zhian Zhu's Scheme and Evaluation of TMIS Smart Card Authentication Schemes

P. Nayak, R. S. Pippal[*]

Department of Computer Science and Engineering, RKDF University, Bhopal, India

Received 13 October 2020, accepted in final revised form 28 February 2021

Abstract

The security for Telecare Medicine Information Systems (TMIS) is extremely vital. In this context, numerous TMIS-based authentication schemes have been introduced, however different types of attacks and inefficiencies render these schemes inappropriate for this scenario. This paper investigates various TMIS-based authentication schemes present in the literature. It additionally compares these schemes based on computation cost and potential security attacks. Further, it also demonstrates that Zhian Zhu's scheme is inaccurate as the server fails to approve and validate the login request message of a user in the authentication phase.

Keywords: Attacks; Authentication; Password; Security; Smart Card; TMIS.

doi: http://dx.doi.org/10.3329/jsr.v13i2.49730 J. Sci. Res. **13** (2), 407-413 (2021)

1. Introduction

With the progression of technology, healthcare services can be given distantly, where sensors measure the patient's condition, feed the information to mobile devices and from where it is sent to heath provider's Telecare Medicine Information System (TMIS). TMIS has given the leverage of movement to both patients and doctors. Patients can login to the system to check their medical records, get test results and history of prescribed medicines. Doctors and physicians can check the history of prescribed medicines, test results and based on those can always change the medicines.

As the communication between a cell phone/smart card and TMIS happens on the public Internet, the entire system is vulnerable to threats associated with open Internet. Privacy and especially anonymity is the greatest obstacle in usage of an e-Healthcare framework globally. In this field, numerous smart card based authentication schemes have been proposed. Later on, more complex and secure authentication schemes were proposed. In e-Healthcare, all authentication schemes begin with the registration phase where the user registers distantly with the TMIS. After successful registration, the user needs to be authenticated before being allowed access to the TMIS. The one-factor authentication

[*] *Corresponding author*: ravesingh@gmail.com

protocols provide effortlessness as the user just needs to remember his/her password for the authentication purposes. On the other hand, two-factor authentication requires smart card in addition to the ID and password, which diminishes the user's comfort level. Further, in three-factor authentication, the user needs to provide his/her biometric information in addition to smart card, ID and password.

The authentication schemes comprise of the following stages:

- Registration Phase: In this phase, the user registers with the TMIS by giving individual information and identity. A password can be picked up at a later stage or at the registration phase and it is subject to change after the first login.
- Login and Authentication Phase: In this phase, the user accesses the services provided by the TMIS by giving his/her identity.
- Password Change Phase: This phase is presented with the goal that the user can refresh his/her password consistently, which limits the probability of attacks because of utilizing a similar password.
- Revocation Phase: In this phase, the user credentials are revoked in case of any compromise.

2. Noteworthy Contribution in this Field

This section reveals recent smart card based authentication schemes for TMIS. In 2012, Zhian Zhu [1] proposed the scheme based on one way hash function. However, this paper will show in next section that Zhian Zhu's scheme [1] is inaccurate. In the authentication phase, the server cannot validate the login request message of a user. Islam *et al.* [2] proposed dynamic ID concept where the user ID is dynamically changed using the timestamp for each session and also kept secret, in order to provide user anonymity. It uses a random number and TMIS's secret key along with an ID and password, in order to resist against the offline password guessing attack. The proposed scheme provides mutual authentication, where at first the TMIS validates the user and then the user validates the server on the basis of current timestamps. In the registration phase, the password and a randomly chosen random number is kept secret even from the TMIS, in order to resist against the insider attack.

Zhang *et al.* [3] exposed weaknesses in the proposed dynamic ID scheme by Islam *et al.* [2] and proved that the scheme does not resist against the server and user impersonation attack, as the adversary can extract the secret information from the smart card using power analysis. Zhang *et al.'s* scheme uses a secret value along with the user ID and does not reveal that to the server, in order to resist against the insider attack [3].

Jiang *et al.* [4] proposed an authentication scheme that encrypts the user ID with the server secret key to ensure user anonymity during the authentication phase. It provides mutual authentication, as the user and the server both authenticate each other before starting any kind of communication. Authentication messages in each session are unique so that the attacker cannot use them to track the user. In the registration phase, the hash of the password along with a random number is sent to the server, in order to resist against the insider attack. However, Mishra *et al.* [5] exposed weaknesses in Jiang et al.'s scheme [4] and proved that the scheme in [4] efficiently resists the impersonation attack, password guessing attack, privileged insider attack, stolen smart card attack and also ensures forward secrecy. Unfortunately, the scheme [4] does not verify the correctness of the user identity and password at the end-user during the password update phase. If a user mistakenly inputs wrong credentials during the password update phase, then the password is updated at the end-user and the session is rejected by the server. As a result, the user will face denial of service.

Tu *et al.* [6] proposed a scheme that is 75 % replica of Zhang *et al.* [3] scheme. Their cryptanalysis shows that Zhang et al.'s scheme [3] only fails to resist against the impersonation attack. So, they proposed an improvement to counter all other known attacks. In their proposed scheme, the user uses a secret value to generate the legal messages during the authentication phase, in order to resist against the user impersonation attack.

Farash *et al.* [7] proposed an authentication scheme to address the weaknesses present in Tu *et al.'s* scheme [6]. The scheme uses a secret value to compute the authentication messages in order to resist against the impersonation attack and offline password guessing attack. Wen *et al.* [8] proposed an authentication scheme that hides the user identity in authentication messages, in order to provide the user privacy. As the ID is hidden, the adversary needs to guess the ID of the user as well as the password, which makes the attack infeasible. It resists against the replay attack, as each message contains the timestamps and a random nonce.

Xu *et al.* [9] proposed an authentication scheme in order to resist against the insider attack and impersonation attack. The scheme uses a random number along with the password in the login and authentication phases in order to resist against the insider attack, offline password guessing attack, user impersonation attack, server spoofing attack and replay attack, as the adversary also needs to guess the random number in addition to the password and ID to make these attacks successful. However, Amin *et al.* [10] proved that Xu *et al.'s* scheme [9] has a design flaw, in the password update phase as it asks for the old password before accepting the new one but it does not verify the old password. This is disastrous if the smart card is stolen, because the adversary can change the password without the knowledge of the old password, as the scheme does not verify the old password. It also fails to achieve strong authentication in the authentication phase, fails to provide revocation mechanism for stolen or lost smart cards, and fails to resist against the strong replay attack.

Lu *et al.* [11] proposed a scheme which conceals user's identity by a one-way hash function in transmitting messages, in order to ensure user anonymity during the login and authentication phase. The scheme uses the server's private key and user's biometric information in login messages, which makes the offline password guessing attack very hard because only the user and the server knows the biometric information and the private key respectively. Giri *et al.* proposed their scheme [12] which is based on the RSA to make it efficient and practical. The scheme works on the assumption that the adversary cannot extract any secret information from the smart card and captured authentication messages, which is obviously not a true assumption as information stored in the smart card can be extracted using different ways.

Li *et al.* [13] have reviewed Amin *et al.'s* scheme [10] and pointed out that it cannot achieve untraceability property of the patient. Besides, their scheme has lack of password check method and denial-of-service attack. To overcome these security threats, they have proposed a robust user authentication scheme for E-healthcare system. After that, Ali-Pal [14] have reviewed Li *et al.* [13] and pointed out that the scheme fails to resist identity and password guessing attacks, privileged insider attack, user impersonation attack and smartcard theft attack. To overcome these shortcomings, they have proposed a new biometrics-based remote user authentication scheme for improving the security in E-healthcare system.

In 2016, Han *et al.* [15] shows that Lu *et al's* scheme [11] leaks user's identity and is vulnerable to impersonation attacks. To enhance the scheme's security, Han et al. propose a new efficient three factor authentication scheme. In order to design a more secure and more efficient scheme based on biometric, Zhang *et al.* [16] propose a new scheme based on secure sketch. Through a careful analysis, a conclusion can be drawn that their scheme is more secure in spite of the higher computation cost.

Use of simulation and expert systems is rising day by day. Global warming has become one of the most important issues now days. In this context, Hoque *et al.* [17] has examined potential gas fields of Bangladesh for the analysis of carbon dioxide sequestration. Konyeha and Imouokhome [18] have developed a web based expert system for the diagnosis of rubber crop disease. It permits the farmers to select disease symptoms and the system diagnoses the diseases of the rubber crop and suggests preventive measures also. There are few other vital research contributions in this field [19-23].

3. Comments on Weaknesses Present in Zhian Zhu's Scheme [1]

In 2012, Zhu proposed RSA based smart card authentication scheme for TMIS. This section demonstrates that Zhu's scheme [1] is inaccurate as it fails to provide mutual authentication between user and the server. In the authentication phase, the server cannot validate the login request message of a user. Here, $\boldsymbol{B_i}$, $\boldsymbol{H_i}$, $\boldsymbol{D_i}, \boldsymbol{X_i}$ are the variables computed at smart card end.

1. At the time of login request creation, user inserts his smart card into a card reader and inputs his password $\mathrm{PW_i}$.
2. The smart card generates a random number $\mathrm{w_i}$.
3. It computes $\mathrm{PW_i}' = \mathrm{h(PW_i||N_i)}$
4. $\mathrm{B_i' = B_i \oplus h(PW_i') = h(ID_i \oplus d) \oplus PW_i' \oplus h(PW_i')}$
5. $\mathrm{h_i = h(B_i'||w_i) = h((h(ID_i \oplus d) \oplus PW_i' \oplus h(PW_i'))||w_i)}$ (1)
6. $\mathrm{X_i = (h_i||w_i)^e \bmod n}$
7. Sends login request $\{\mathrm{ID_i, X_i}\}$ to server.
8. Upon receiving, server validates $\mathrm{ID_i}$

9. If true, computes $(h_i||w_i) = (X_i)^d \bmod n$
10. Computes $h_i' = h(h(ID_i \oplus d)||w_i)$ (2)
11. Verifies whether h_i and h_i' are equal or not.

From equation (1) and equation (2), it is clear that h_i and h_i' are not equal to each other.

4. Analysis of Existing TMIS Smart Card Authentication Schemes based on Computational Cost, Potential Attacks and Security Features Provided

This section presents comparative analysis of existing smart card authentication schemes for TMIS under computation cost and security features provided. Table 1 shows the comparison among various schemes on the basis of potential attacks and security features provided. Table 2 presents the comparison among various schemes on the basis of computation cost associated.

Table 1. Potential attacks and security features of authentication schemes for TMIS.

Scheme	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11
Zhu *et al.* [1]	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Islam *et al.* [2]	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes	Yes
Zhang *et al.* [3]	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes	No	No
Jiang *et al.* [4]	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Mishra *et al.* [5]	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Tu *et al.* [6]	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes	No	No
Farash *et al.* [7]	Yes	Yes	No	Yes	Yes	No	No	No	No	Yes	Yes
Wen *et al.* [8]	Yes	Yes	Yes	No	Yes	No	No	Yes	No	Yes	Yes
Xu *et al.* [9]	Yes	No	No	Yes	No	Yes	No	Yes	Yes	No	Yes
Amin *et al.* [10]	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Lu *et al.* [11]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Giri *et al.* [12]	Yes	Yes	No	Yes	Yes	No	No	Yes	No	Yes	Yes
Ni *et al.* [13]	No	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No
Ali-Pal [14]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Han *et al.* [15]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zhang *et al.* [16]	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Here, A1=Resist insider attack, A2=Ensure efficient password update, A3=Ensure session key verification, A4=Ensure forward secrecy, A5=Resist denial of service attack, A6=Resist off-line password guessing attack, A7=Resist stolen smart card attack, A8=Resist user impersonation attack, A9=Resist stolen verifier attack, A10=Resist replay attack, A11=Provides validity proof

Table 2. Computation cost of authentication schemes for TMIS.

Scheme	User Computations	Server Computations
Zhu *et al.* [1]	$4T_h + 1T_{me}$	$4T_h + 1T_{me}$
Islam *et al.* [2]	$6T_h + 2T_{pm}$	$3T_h + 1T_{pm}$
Zhang *et al.* [3]	$6T_h + 4T_{pm} + 1T_{pa}$	$5T_h + 4T_{pm} + 1T_{pa} + 1T_{minv}$
Jiang *et al.* [4]	$5T_h + 1T_s$	$4T_h + 2T_s$
Mishra *et al.* [5]	$6T_h$	$6T_h$
Tu *et al.* [6]	$5T_h + 4T_{pm} + 1T_{pa}$	$5T_h + 3T_{pm}$
Farash *et al.* [7]	$5T_h + 4T_{pm} + 1T_{pa}$	$5T_h + 3T_{pm}$
Wen *et al.* [8]	$3T_h + 2T_s + 4T_{me} + 1T_{pm}$	$2T_h + 2T_s + 4T_{me} + 1T_f$

Xu *et al.* [9]	$8T_h$+ $1T_s$+ $2T_{pm}$	$7T_h$+ $1T_s$+ $2T_{pm}$
Amin *et al.* [10]	$4T_h$+ $1T_{pm}$	$7T_h$+ $2T_s$+ $4T_{pm}$
Lu *et al.* [11]	$5T_h$+ $2T_{pm}$	$6T_h$+ $2T_{pm}$
Giri *et al.* [12]	$5T_h$	$1T_{me}$+ $4T_h$
Ni *et al.* [13]	$12T_h$	$12T_h$+ $2T_{me}$
Ali-Pal [14]	$18T_h$	$16T_h$+ $2T_{me}$
Han *et al.* [15]	$6T_h$ +$2T_{pm}$	$5T_h$+ $1T_{pm}$ + $2T_s$
Zhang *et al.* [16]	$6T_h$ +$6T_{xor}$	$4T_h$ +$4T_{xor}$

Here, T_h = Time to compute a one-way hash operation, T_s = Time to compute a symmetric encryption operation, T_{pm} = Time to compute a point multiplication/ modular multiplication operation, T_{pa} = Time to compute a point addition operation, T_{minv} = Time to compute a modular inverse operation, T_{me} = Time to compute a modular exponentiation operation, T_f = Time to compute a pseudo-random function operation, T_{xor} = Time to compute an xor operation

5. Conclusion

In this paper, security features and computation cost of recently proposed authentication schemes have been analyzed in the field of Telecare Medicine Information System (TMIS). Further, it is additionally demonstrated that Zhian Zhu's scheme is inaccurate as in the authentication phase; the server cannot validate the login request message of a user. Thus, there is still requirement for secure as well as efficient smart card based authentication scheme for TMIS.

Acknowledgment

The authors would like to thank RKDF University, Bhopal for providing the academic support.

References

1. Z. Zhu, J. Med. Syst. **36**, 3833 (2012). https://doi.org/10.1007/s10916-012-9856-9
2. S. K. H. Islam and M. K. Khan, J. Med. Syst. **38**, 135 (2014).
3. L. Zhang, S. Tang, and Z. Cai, Int. J. Commun. Syst. **27**, 2691 (2014).
4. Q. Jiang, M. Jianfeng, L. Xiang, and T. Youliang, J. Med. Syst. **38**, 12 (2014). https://doi.org/10.1007/s10916-016-0610-6
5. D. Mishra, J. Srinivas, and S. Mukhopadhyay, J. Med. Syst. **38**, 120 (2014). https://doi.org/10.1007/s10916-014-0120-3
6. H. Tu, N. Kumar, N. Chilamkurti, and S. Rho, Peer-to-Peer Netw. Appl. **8**, 903 (2014). https://doi.org/10.1007/s12083-014-0248-4
7. M. S. Farash, Peer-to-Peer Netw. Appl. **9**, 82 (2016). https://doi.org/10.1007/s12083-014-0315-x
8. F. Wen and D. Guo, J. Med. Syst. **38**, 26 (2014). https://doi.org/10.1111/1742-6723.12245
9. L. Xu and F. Wu, J. Med. Syst. **39**, ID 10 (2015). https://doi.org/10.1007/s10916-014-0179-x
10. R. Amin and G. P. Biswas, J. Med. Syst. **39**, 78 (2015). https://doi.org/10.1007/s10916-015-0258-7
11. Y. Lu, L. Li, H. Peng, and Y. Yang, J. Med. Syst. **39**, ID 32 (2015). https://doi.org/10.1007/s10916-015-0221-7
12. D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, J. Med. Syst. **39**, 145 (2015). https://doi.org/10.1007/s10916-014-0145-7

13. X. Li, J. Niu, M. Karuppiah, S. Kumari, and F. Wu, J. Med. Syst. **40**, 268 (2016). https://doi.org/10.1007/s10916-016-0629-8
14. R. Ali and A. K. Pal, Arab. J. Sci. Eng. **43**, 7837 (2018). https://doi.org/10.1007/s13369-018-3220-4
15. H. Lidong, T. Xiao, W. Shengbao, and L. Xikun, Peer-to-Peer Netw. Appl. **11**, 63 (2018). https://doi.org/10.1007/s12083-018-0634-4
16. M. Zhang, J. S. Zhang, and W. R. Tan, J. Inf. Sci. Eng. **32**, 389 (2016).
17. S. M. S. Hoque, M. A. Iqbal, S. I. Ahmed, and M. A. Islam, J. Sci. Res. **11**, 41 (2019). https://doi.org/10.3329/jsr.v11i1.37756
18. S. Konyeha and F. Imouokhome, J. Sci. Res. **10**, 239 (2018). https://doi.org/10.3329/jsr.v10i3.34786
19. V. Sureshkumar, R. Amin, M. S. Obaidat, and I. Karthikeyan, J. Inf. Sec. App. **53**, 102539 (2020). https://doi.org/10.1016/j.jisa.2020.102539.
20. F. M. Salem and R. Amin, Inf. Sci. **527**, 382 (2020). https://doi.org/10.1016/j.ins.2019.07.029.
21. V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. R. Sekar, Fut. Gen. Com. Sys. **100**, 938 (2019). https://doi.org/10.1016/j.future.2019.05.058.
22. V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan, and R. Madhumathi, IEEE Syst. J. (2020).
23. R. Amin, S. H. Islam, P. Gope, K. K. R. Choo, and N. Tapas, IEEE J. Biomed. Health Informat. **23**, 1749 (2019). https://doi.org/10.1109/JBHI.2018.2870319