Survey of Authentication Schemes used for Telecare Medicine Information Systems

Kukki Arya[1], Abhinav Vidwansh[2]

Vikrant Institute of Information Technology & Management
Gwalior (MP), India
[1]arya.kukki@gmail.com

Abstract

The Telecare Medicine Information System (TMIS) has established a connection between patients at home and doctors at a clinical center by using telecommunication systems and physiological monitoring devices. Authentication, security, patient's privacy protection and data confidentiality are important for patient or doctors accessing to Electronic Medical Records (EMR). Remote user authentication is desirable for TMIS to verify the correctness of communicating parties. The password based authentication schemes provide efficient and scalable solutions for remote user authentication. In this context, numerous schemes have been proposed to achieve these goals. However, these schemes are vulnerable to various attacks. Moreover, they are neither efficient nor user friendly. Specially, some schemes require the exponential computation or public key cryptography which leads to very low efficiency for smart card. This paper analyses major contribution in this field and discusses their pros and cons.

Keywords— Authentication, Hash function, Password, Smart card, TMIS

I. INTRODUCTION

In last few decades, telecare medicine information systems enable health-care delivery services due to the increased availability of lower-cost telecommunications systems. These systems are moving towards an environment where automated patient medical records and electronically interconnected telecare facilities are prevalent. It has brought us a lot of conveniences. However, it may also reveal patient`s important information. 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. Therefore, the security of TMIS is vital. TMIS needs a more secure and more efficient authentication scheme. A secure authentication scheme is essential to guarantee that only the authorized patients or users can access the service from TMIS [1, 2, 3].

At present, there are three authentication factors used to achieve mutual authentication between the client and the server: a) something you know (typically username and password); b) something you have (such as identity card or smart card); c) something you are (i.e. biometrics).

One of the famous solutions to counter the drawback of verification table is to encode all the passwords by making use of one way hash function and then store the digest in the verification table stored in the server [4]. However, it consumes more memory space to store the encrypted password. In this approach, size of the verification table increases as the number of users increases. Management of this large sized verification table raises load to the server. In order to counter these problems and limitations, password based smart card authentication scheme has been proposed as a replacement for OTP. Smart card is a tamper resistant integrated circuit card with memory and processor capable of performing computations. Data are stored in the chip's memory and can be accessed to execute and complete various processing applications. Following are the three stages of smart card authentication scheme.

- **Registration phase**. Once the registration request has been received from the user, server calculates the necessary parameters, keeps these parameters into smart card memory and distributes the smart card to the user.
- **Login phase**. The login phase and authentication phase are invoked at the time when user is going to login into the server. In the login phase, the smart card creates the login request using the inputted credentials of user and the necessary parameters stored in the smart card memory.
- **Authentication phase**. After receiving the login request, server checks the validity of the login request by using its own secret key in order to authenticate the requested user.

The rest of the paper is organized as follows. Section II explores major contributions in the field of authentication provided for telecare medicine information system. A comparison of these authentication schemes is investigated in section III. Finally, section IV concludes the paper.

II. LITERATURE REVIEW

Encouraged by Lamport's scheme [4], Haller proposed the prominent S/KEY one time password for an Internet draft RFC 1760 [5, 6]. Though, few researchers have proved that the security of the S/KEY scheme can be breached by server spoofing attacks, replay attacks and password guessing attacks [7-9]. Then after, SAS and OSPA protocols are suggested by Sandirigama et al. [10] and Lin et al. [11] respectively. However, Chen and Ku found that the SAS and OSPA protocols can be breached by two stolen verifier attacks [12]. In order to protect identified security attacks on the verification tables, smart card password authentication scheme has been suggested.

In this field, many important contributions have been noted [13-21]. Subsequently, authentication based on smart card has been deployed continuously in several applications like cloud computing [22], healthcare [23], key exchange in IPTV broadcasting [24], key agreement and authentication for Universal Mobile Telecommunications System (UMTS) [25], authentication in multi-server environment [26], wireless sensor networks [27] and many more.

In 2010, Wu et al. [28] proposed an efficient authentication scheme for TMIS. But, He et al. [29] pointed out that Wu et al.'s scheme [28] could not resist impersonation attack and insider attack. To improve security, He et al. [29] also proposed an improved scheme. Nevertheless, Wei et al. [30] demonstrated that both of Wu et al.'s scheme and He et al.'s scheme cannot achieve two-factor authentication. To overcome the weaknesses, Wei et al. suggested a better authentication scheme for TMIS and claimed that their scheme could withstand various potential attacks. However, Zhian Zhu [31] proved that this scheme is vulnerable to off-line password guessing attack. The author also proposed a new authentication scheme for TMIS. This paper shows that Zhian Zhu's scheme is incorrect. In the authentication phase, the server cannot validate the login request message of a user. Moreover, robust authentication scheme for TMIS has been proposed using one way hash function.

In 2013, Tan proposed an efficient smart card based password authentication scheme by applying biometrics technique and hash function operations [32]. The author claimed that his scheme provides a stronger user authentication function by adopting biometics technique. Further, it establishes secure and efficient session key and has secure password and biometics update function. However, Yan et al. proposed that Tan's scheme may suffer Distributed Denial-of-Service attack and is not practical for the TMIS [33].

To achieve user anonymity, Wang et al. [34] proposed an authentication and key agreement scheme with user anonymity based on ECC. But Pu et al. [35] demonstrated that in Wang et al.'s scheme, the long-term private key stored in the mobile device will be revealed if an adversary gets the device. Moreover, their scheme needs a smart card producing center to maintain the certificates for users' public keys. Pu et al. propose a generic construction of smart card based password authentication scheme [35]. Their scheme does not need to store or verify others' certificates. However, Pu et al.'s scheme requires the high computation cost. Furthermore, the mutual authentication during the key agreement phase applies a password-based two-party authenticated key agreement scheme to establish a secure high-entropy session key. Therefore, the user and the server must share a password beforehand. Khan et al. [36] also found that Wang et al.'s scheme cannot provide user's anonymity and the user's free choice of a password. In addition, Wang et al.'s scheme suffers from the following security issues: vulnerability to insider attack and no provision for a session key agreement. To address these security flaws, Khan et al. proposed an enhanced authentication scheme. But Chen et al. [37] found that Khan et al.'s scheme still cannot protect the user's anonymity. So far, to design an efficient smart card based authentication scheme with anonymity preserving is still a challenging issue.

III. COMPARATIVE ANALYSIS OF EXISTING AUTHENTICATION SCHEMES USED IN TMIS

This section provides a comparison result for existing smart card based authentication schemes proposed for TMIS. Table I shows comparative results in terms of security properties provided. Table II explores comparative analysis for various smart card authentication schemes in terms of computational complexity.

TABLE I COMPARISON OF PROPOSED SCHEME WITH EXISTING AUTHENTICATION SCHEMES USED IN TMIS

Security Properties	**Tan's Scheme [32]**	**Zhian Zhu's Scheme [31]**	**Wei et al.'s Scheme [30]**	**He et al.'s Scheme [29]**	**Wu et al.'s Scheme [28]**
User is allowed to choose and change the password	Yes	Yes	Yes	Yes	Yes
Secure change of password	Yes	***No***	***No***	***No***	***No***
Provides mutual authentication	Yes	Yes	Yes	Yes	Yes
Provides early wrong password detection	Yes	***No***	***No***	***No***	***No***
Provides session key generation	Yes	***No***	Yes	Yes	Yes
Resists impersonation attack	Yes	Yes	Yes	Yes	***No***
Resists guessing attack	Yes	Yes	***No***	***No***	***No***
Resists replay attack	Yes	Yes	Yes	Yes	Yes
Resists privileged insider attack	Yes	Yes	Yes	Yes	***No***

To analyze the computational complexity of the schemes, we define t_s, t_e, t_{inv}, t_h and t_m be the time cost of one scalar multiplication in a group, one modular exponentiation in Z_p, one inverse operation in Z_q, one hash operation and one modular multiplication in Z_q, respectively. According to [38-41], the time cost of all operations satisfies the following: $T_s \approx 29t_h$, $t_h \approx t_m$ and $t_e \approx t_{inv} \approx 240t_m$.

TABLE III COMPARISON OF PROPOSED SCHEME IN TERMS OF COMPUTATIONAL COMPLEXITY

		Tan's Scheme [32]	**Zhian Zhu's Scheme [31]**	**Wei et al.'s Scheme [30]**	**He et al.'s Scheme [29]**	**Wu et al.'s Scheme [28]**
Registration phase	Smart card	$2t_h$	t_h	t_h	t_h	0
	Server	$2t_h$	t_h	$t_e \approx 240t_h$	$t_e+t_{inv}+t_h \approx 481t_h$	$3t_e+t_{inv}+2t_m \approx 962t_h$
Login and authentication phase	Smart card	$5t_h+t_{sym} \approx 7.25t_h$	$t_e+4t_h \approx 244t_h$	$t_e+6t_h+T_s \approx 275t_h$	$t_e+t_{inv}+5t_h+t_m \approx 486t_h$	$4t_h+3t_m \approx 7t_h$
	Server	$4t_h+t_{sym} \approx 6.25t_h$	$t_e+4t_h \approx 244t_h$	$t_e+t_{inv}+5t_h+T_s \approx 514t_h$	$t_e+t_{inv}+4t_h \approx 484t_h$	$t_e+4t_h \approx 244t_h$
Password update	Smart card	$3t_h$	$2t_h$	$2t_h$	$t_e+t_{inv}+2t_h+t_m \approx 483t_h$	$2t_e+2t_{inv}+2t_m \approx 962t_h$

IV. CONCLUSIONS

The telecare medical information system facilitates the patients gain health monitoring and access healthcare-related services over internet or mobile networks. In the present scenario, the mutual authentication between the patient and the telecare server is in great demand. In order to achieve this, several smart card based authentication schemes for telecare medicine information systems have been proposed.

This paper portrays a comparative analysis of major smart card authentication schemes used for telecare medicine information systems (TMIS) in terms of their computational efficiencies and security properties. This effort assists the researchers to work in different directions towards design and development of secure and efficient smart card authentication scheme.

REFERENCES

[1] Adamsk, T., Winiecki, W., Entity identification algorithms for distributed measurement and control systems with asymmetry of computational power, Prz Elektrotechniczn,(2008),No. 05

[2] Cheng, X.R., Li, M.X., The authentication of the grid monitoring system for wireless sensor networks, Prz Elektrotechniczn, (2013),No.01a

[3] Pejaś, J., El Fray , I., Ruciński, A., Authentication protocol for software and hardware components in distributed electronic signature creation system, Prz Elektrotechniczn, (2012),No.10b

[4] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, 1981, pp. 770-772.

[5] N. Haller, "The S/KEY one-time password system," in Proceedings of Internet Society Symposium on Network and Distributed System Security, 1994, pp. 151–158.

[6] N. Haller, "The S/KEY one-time password system," RFC1760, Feb. 1995.
[7] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme," ACM Operating Systems Review, vol. 30, pp. 12–16, Oct. 1996.
[8] T. C. Yeh, H. Y. Shen, and J. J. Hwang, "A secure one-time password authentication scheme using smart cards," IEICE Trans. on Communications, vol. E85-B, pp. 2515–2518, Nov. 2002.
[9] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," Information Processing Letters, vol. 62, pp. 77–80, 1997.
[10] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," IEICE Transactions on Communications, vol. E83-B, pp. 1363–1365, June 2000.
[11] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," IEICE Transactions on Communications, vol. E84-B, pp. 2622–2627, September 2001.
[12] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," IEICE Transactions on Communications, vol. E85-B, pp. 2519–2521, November 2002.
[13] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Security Issues in Smart Card Authentication Scheme," International Journal of Computer Theory and Engineering (IJCTE), vol. 4, no. 2, 2012, pp. 206-211.
[14] Ravi Singh Pippal, Pradeep Gupta and Rakesh Singh, "A Novel Smart Card Authentication Scheme using Image Encryption," International Journal of Computer Applications, vol. 72, no. 9, 2013, pp. 8-14.
[15] Ravi Singh Pippal, Pradeep Gupta and Rakesh Singh, "Dynamic Encryption Key Based Smart Card Authentication Scheme," International Journal of Computer Applications, vol. 72, no. 9, 2013, pp. 15-18.
[16] Ravi Singh Pippal, Rajesh Ahirwar, Shivpratap Singh Kushwah and Pradeep Yadav, "A Secure SCAM (Smart Card based Authentication Mechanism)," International Journal of Computer Applications, vol. 72, no. 5, 2013, pp. 26-31.
[17] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "A Novel Smart Card Mutual Authentication Scheme for Session Transfer among Registered Devices," In: Proceedings of the 3rd IEEE International Advance Computing Conference (IACC-2013), February 22-23, 2013, Ghaziabad, India.
[18] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Highly Secured Remote User Authentication Scheme using Smart Cards," In: Proceedings of the 7th IEEE International Conference on Industrial Electronics and Applications (ICIEA-2012), July 18-20, 2012, Singapore, pp. 1001-1005.
[19] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Security Vulnerabilities of User Authentication Scheme using Smart Card," In: Proceedings of the 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec-2012), July 11-13, 2012, Paris, France, pp. 106-113.
[20] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Comments on Symmetric Key Encryption Based Smart Card Authentication Scheme," In: Proceedings of the 2nd International Conference on Computer Technology and Development (ICCTD-2010), November 2-4, 2010, Cairo, Egypt, pp. 482-84.
[21] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Comparative Analysis of Smart Card Authentication Schemes," In: Proceedings of the 4th IEEE International Conference on Advanced Computing and Communication Technologies (ICACCT-2010), October 30, 2010, Panipat, India, pp. 113-18.
[22] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Enhanced Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing," Informatica, vol. 37, no. 2, 2013, pp. 149-156.
[23] Hu, J., Chen, H. H. & Hou, T. W. (2010). A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards and Interfaces, 32(5-6), 274-280.
[24] Pippal, R. S., Tapaswi, S., Jaidhar, C. D. (2012). Secure Key Exchange Scheme for IPTV Broadcasting. Informatica, 36(1), 47-52.
[25] Hwang, M. S., Chong, S. K. & Ou, H. H. (2011). On the security of an enhanced UMTS authentication and key agreement protocol. European Transactions on Telecommunications, 22(3), 99-112.
[26] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Robust Smart Card Authentication Scheme for Multi- server Architecture," Wireless Personal Communications (Springer), vol. 72, no. 1, 2013. pp. 729-745.
[27] Fan, R., He, D., Pan, X. Z. & Ping, L. D. (2011). An efficient and DoS-resistant user authentication scheme for two-tired wireless sensor networks. Journal of Zhejiang University-SCIENCE C (Computers and Electronics), 12(7), 550-560.
[28] Wu, Z. Y., Lee, Y. C., Lai, F., Lee H. C., and Chung, Y., "A secure authentication scheme for telecare medicine information systems", Journal of Medical Systems (Springer). DOI: 10.1007/s10916-010-9614-9, 2010.
[29] He, D. B., Chen, J. H., and Zhang, R., "A more secure authentication scheme for telecare medicine information systems", Journal of Medical Systems (Springer). DOI:10.1007/s10916-011-9658-5, 2011.
[30] Wei, J., Hu, X., Liu, W., "An Improved Authentication Scheme for Telecare Medicine Information Systems", Journal of Medical Systems (Springer). DOI:10.1007/s10916-012-9835-1, 2012.
[31] Zhian Zhu, "An Efficient Authentication Scheme for Telecare Medicine Information Systems", Journal of Medical Systems (Springer). DOI: 10.1007/s10916-012-9856-9, 2012.
[32] Tan, Z., An efficient biometrics-based authentication scheme for telecare medicine information systems. Przeglad Elektrotechniczny, 89(5):200 –204, 2013.
[33] Xiao-peng Yan , Wei-heng Li , Ping Li. A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems[J], Journal of medical systems, 2013, 37(9972)1-6.
[34] Wang, R.-C., Juang, W.-S., Lei, C.-L., Provably secure and efficient identification and key agreement protocol with user anonymity,J Comput Syst Sci, doi:10.1016/j.jcss.2010.07.004. 2010.
[35] Pu, Q., Wang, J., Zhao, R.-Y., Strong authentication scheme for telecare medicine information systems, J Med Syst,36(2012),2609–2619.
[36] Khan, M. K., et al., Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme,Comput. Commun. 34(2010), No.3, 305–309.
[37] Chen, H.-M., Lo,J.-W., Yeh, C.-K., An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, J Med Syst, DOI 10.1007/s10916-012-9862-y
[38] Fan, Ch.-I. Sun, Huang, W. Z., Vincent, S.-M.,Provably secure randomized blind signature scheme based on bilinear pairing,Comput Math Appl, 2010, No.60,285–293
[39] Koblitz, N., Menezes, A.J., Vanstone, S.A.,The state of elliptic curve cryptography, Design Code Cryptogr, (19)2000, No.2-3, 173–193
[40] Xue,K.M.,Hong, P.L., "Security improvement on an anonymous key agreement protocol based on chaotic maps", Commun Nonlinear Sci Numer Simulat, 2012, No.17, 2969–2977
[41] Menezes, A., Van Oorschot, P. C., Vanstone, S. Handbook of Applied Cryptography, CRC Press, USA, 1997.