Journal of King Saud University – Computer and Information Sciences (2017) **29**, 54–62

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

An enhanced dynamic ID-based authentication scheme for telecare medical information systems

Ankita Chaturvedi, Dheerendra Mishra *, **Sourav Mukhopadhyay**

Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302, India

Received 25 August 2014; revised 24 October 2014; accepted 9 December 2014
Available online 7 November 2015

KEYWORDS

Telemedicine;
Password based authentication;
Smart card;
Security;
Privacy

Abstract The authentication schemes for telecare medical information systems (TMIS) try to ensure secure and authorized access. ID-based authentication schemes address secure communication, but privacy is not properly addressed. In recent times, dynamic ID-based remote user authentication schemes for TMIS have been presented to protect user's privacy. The dynamic ID-based authentication schemes efficiently protect the user's privacy. Unfortunately, most of the existing dynamic ID-based authentication schemes for TMIS ignore the input verifying condition. This makes login and password change phases inefficient. Inefficiency of the password change phase may lead to denial of service attack in the case of incorrect input in the password change phase. To overcome these weaknesses, we proposed a new dynamic ID-based authentication scheme using a smart card. The proposed scheme can quickly detect incorrect inputs which makes the login and password change phase efficient. We adopt the approach with the aim to protect privacy, and efficient login and password change phases. The proposed scheme also resists off-line password guessing attack and denial of service attack. We also demonstrate the validity of the proposed scheme by utilizing the widely-accepted BAN (Burrows, Abadi, and Needham) logic. In addition, our scheme is comparable in terms of the communication and computational overheads with relevant schemes for TMIS.

1. Introduction

The omnipresence and easy access of the Internet, provides a scalable platform for healthcare services. One of the popular health care services is telecare medical information systems (TMIS) which supports healthcare delivery services to the patients' homes. As we are moving from paper based health records to electronic health records, the TMIS offers an easy access of electronic records to remote users. TMIS is making a difference by employing information and communication technologies to enhance the quality of healthcare related services in the management of chronic diseases.

Increasing computation power has made the adversary powerful enough so that he can control communications over the public network (Aloul et al., 2009a; Mishra et al., 2014a; Alfantookh, 2006). Thus, authorized communication is required to ensure in TMIS. To reduce the adversary threat,

* Corresponding author.
E-mail address: dheerendra@maths.iitkgp.ernet.in (D. Mishra).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.12.007
1319-1578 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

smart card based authentication schemes are designed and developed (Aloul et al., 2009b; Mishra et al., 2014b; Al-Muhtadi, 2007), which goal is to address the following attributes:

One time registration: It allows the patient to register once with the medical server and then he can access the services any number of times.

Efficient login phase: A login phase should be capable of detecting incorrect login inputs. In other words, smart card should not execute the login session in the case of wrong identity or password input.

Efficient password change phase: The scheme should be able to quickly detect incorrect inputs in the password change phase.

User-friendly password change phase: A user should be allowed to change his password input and only allows a patient to update his password freely without the medical server's assistance.

Mutual authentication and session key agreement: It allows a patient and medical servers to mutually authenticate each other and establish a common key, which should be constructed with the equal participation of both the user and server.

Security attributes: The smart card based authentication scheme must be able to withstand man-in-the middle attack, impersonation attack, guessing attack, insider attack, replay attack, stolen smart card attack and known session-specific temporary information attack. Moreover, the scheme should support session key agreement, key freshness property, mutual authentication and forward secrecy.

Wu et al. (2012) introduced an efficient authentication scheme for TMIS, which is better than the previously proposed schemes for low computing devices by adding the pre-computing phase. In the pre-computing phase, the user performs an exponential operation, and then stores the calculated values into the storage device such that a user can extract these values from the device whenever he requires. However, He et al. (2012) demonstrated that Wu et al.'s scheme fails to resist an impersonation attack. They also introduced an enhanced scheme and claimed that their proposed scheme eliminates the drawbacks of Wu et al.'s scheme. They also claimed that their scheme is more appropriate for low power mobile devices for TMIS. Although Wei et al. (2012) identified that both Wu et al.'s and He et al.'s schemes are inefficient to meet two-factor authentication, whereas an efficient password based authentication scheme using a smart card should achieve two-factor authentication. They also presented an improved smart card based authentication scheme for TMIS to ensure two-factor authentication. In 2012, Zhu (2012) demonstrated that Wei et al.'s scheme is vulnerable to off-line password guessing attack. He also presented an improved scheme for TMIS and claimed that his scheme could overcome the weaknesses of Wei et al.'s scheme. However, his scheme does not protect anonymity which enables an adversary to track the consumer's current location and login history (Mishra and Mukhopadhyay, 2014). Although consumer's anonymity during message exchange ensures consumer's privacy by preventing an attacker from acquiring a consumer's sensitive personal information.

Chen et al. (2012) proposed a dynamic ID-based authentication scheme for TMIS which protects user anonymity and has less computation overhead. However, in 2013, Lin (2013) demonstrated that user identity is compromised under the dictionary attack and the password can be derived with the stolen smart card in Chen et al's scheme. He also proposed an improved scheme which efficiently resists dictionary attack and protects anonymity. Unfortunately, Lin's scheme does not include the input verifying condition. This makes login and password change phases inefficient. The inefficiency of the login phase causes extra communication and computation overhead. The inefficient password change phase in Lin's scheme causes denial of service attack (DOS) in the case of incorrect input in password change (Mishra, 2015b). The DOS attack does not allow an authorized user to access the resources (Alfantookh, 2006). Xie et al. (2013) showed that Chen et al.'s scheme is vulnerable to an impersonation attack and off-line password guessing attack using a stolen smart card. Additionally, they presented an improved scheme for TIMS to overcome the weaknesses of Chen et al.'s scheme. However, Xie et al.'s scheme also failed to present an efficient login and password change phase (Mishra, 2015b). Cao and Zhai (2013) demonstrated that Chen et al's scheme is vulnerable to an off-line identity guessing attack and undetectable on-line password guessing attack using a stolen smart card. They also proposed an improved authentication scheme to resist guessing attacks. Their scheme efficiently protects anonymity and password guessing attack, but does not present an efficient login phase and has an unfriendly password change phase (Mishra, 2015b). The smart card cannot identify the correctness of the input in the above discussed schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013; Jiang et al., 2014) which either causes DOS attack or makes the password chance phase unfriendly. The schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013; Jiang et al., 2014) present an inefficient password change phase (Mishra, 2015b; Mishra, 2015a) and the schemes (Cao and Zhai, 2013; Jiang et al., 2013; Wu and Xu, 2013) have an unfriendly password change phase as every time before changing the password the user has to establish an authorized session with the server, that is, user cannot independently change his/her password in these schemes. More detailed characterization of security attributes of the schemes (Wei et al., 2012; Zhu, 2012; Lee et al., 2013; Chen et al., 2012; Cao and Zhai, 2013; Xie et al., 2013; Lin, 2013; Xu et al., 2014) is presented in Table 1.

Motivation: Many of the schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013) cannot identify the correctness of input which leads to a denial of service scenario in the case of incorrect input in the password change phase (Mishra, 2015a,b). A single mistake in the password change phase does not allow a user to login to the server using the same smart card. In other words, an authorized user can never use the smart card to login to the server if he/she commits a mistake in password change. It is a serious security pitfall as user's may himself/herself cause denial of service attack. In general, a user cannot be considered an expert who never commits a mistake. It is always be possible that a human may sometimes forget the password or commit a mistake while entering the password. Moreover, a user may have several accounts and may use different passwords