Journal of King Saud University – Computer and Information Sciences (2015) **27**, 193–210

King Saud University

Journal of King Saud University – Computer and Information Sciences

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

A robust anonymous biometric-based remote user authentication scheme using smart cards

Ashok Kumar Das [a,*], **Adrijit Goswami** [b]

[a] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
[b] *Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*

Received 10 October 2013; revised 10 March 2014; accepted 19 March 2014
Available online 24 March 2015

KEYWORDS

Remote user authentication;
Biometrics;
Smart cards;
Hash function;
Cryptanalysis;
Security

Abstract Several biometric-based remote user authentication schemes using smart cards have been proposed in the literature in order to improve the security weaknesses in user authentication system. In 2012, An proposed an enhanced biometric-based remote user authentication scheme using smart cards. It was claimed that the proposed scheme is secure against the user impersonation attack, the server masquerading attack, the password guessing attack, and the insider attack and provides mutual authentication between the user and the server. In this paper, we first analyze the security of An's scheme and we show that this scheme has three serious security flaws in the design of the scheme: (i) flaw in user's biometric verification during the login phase, (ii) flaw in user's password verification during the login and authentication phases, and (iii) flaw in user's password change locally at any time by the user. Due to these security flaws, An's scheme cannot support mutual authentication between the user and the server. Further, we show that An's scheme cannot prevent insider attack. In order to remedy the security weaknesses found in An's scheme, we propose a new robust and secure anonymous biometric-based remote user authentication scheme using smart cards. Through the informal and formal security analysis, we show that our scheme is secure against all possible known attacks including the attacks found in An's scheme. The simulation results of our scheme using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool ensure that our scheme is secure against passive and active attacks. In addition, our scheme is also comparable in terms of the communication and computational overheads

[*] Corresponding author. Tel.: +91 40 6653 1506; fax: +91 40 6653 1413.
E-mail addresses: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), goswami@maths.iitkgp.ernet.in (A. Goswami).
URLs: http://www.iiit.ac.in/people/faculty/ashokkdas/, https://sites.google.com/site/iitkgpakdas/ (A.K. Das).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.03.020

with An's scheme and other related existing schemes. As a result, our scheme is more appropriate for practical applications compared to other approaches.

1. Introduction

Remote user authentication plays an important role in many applications including e-commerce and m-commerce. Several remote user authentication schemes and their enhancements are proposed in the literature to improve the various security flaws in other schemes. The security of the traditional identity-based remote user authentication schemes is based on the passwords. However, simple passwords are easy to break by simple dictionary attacks. In order to resolve such problem, biometric-based remote user authentications are considered for better alternatives since such authentications are more secure and reliable than the traditional password-based authentication schemes (Li and Hwang, 2010). The advantages of using biometric keys (for example, fingerprints, faces, irises, hand geometry, palm-prints, etc.) are (Das, 2011a; Das and Goswami, 2013; Li and Hwang, 2010)

- Biometric keys cannot be lost or forgotten.
- Biometric keys are extremely hard to forge or distribute.
- Biometric keys are extremely difficult to copy or share.
- Biometric keys cannot be guessed easily as compared to low-entropy passwords.
- Someone's biometrics is not easy to break than others.

According to the existing researches, we list some important essential requirements for evaluating a novel biometric-based remote user authentication scheme using smart cards.

Security requirements

The following attacks should be prevented (Li and Hwang, 2010):

- SR1. *Withstand masquerade attacks*In this attack, an adversary may try to masquerade as a legitimate user to communicate with a valid system or masquerade as a valid system in order to communicate with legal users.
- SR2. *Withstand replay attacks*An attacker tries to hold up the messages between two communicating parties and then impersonate other legal party to replay the fake messages for further deceptions.
- SR3. *Withstand man-in-the-middle attacks*In such attacks, an attacker may intercept the messages during transmissions and then can change or delete or modify the contents of the messages delivered to the recipients.
- SR4. *Withstand denial-of-service attacks*If an attacker blocks the messages from reaching the server and the users, the server as well as the users should know about malicious dropping of such control messages.
- SR5. *Withstand parallel session attacks*In a parallel session attack, an attacker may start new runs of the protocol using knowledge gathered from the initial runs of the protocol. Messages from these new runs of the protocol are replayed in the initial run (Pasca et al., 2008).
- SR6. *Withstand stolen-verifier attacks*An attacker must not get/steal user's password and other secret information from the system.
- SR7. *Withstand stolen smart card attacks*The smart card is usually equipped with tamper-resistant device. If the smart card of a user is lost or stolen, an attacker can still retrieve all the sensitive information stored in the stolen smart card's memory using the power analysis attack (Kocher et al., 1999; Messerges et al., 2002). Then using these retrieved information, an attacker can derive other secret information of the communicating parties (the user as well as the server).

Functionality requirements

A biometric-based remote user authentication scheme should satisfy the following functionality requirements (Li and Hwang, 2010):

- FR1. Provide mutual authentication between two communicating parties and after successful authentication, a secret session key should be established between them for future secure communication between the parties.
- FR2. Should be efficient in terms of communication and computational overheads.
- FR3. Allow users to freely choose and change the passwords locally without further contacting the server. Thus, it can reduce the communication and computational overheads, and some possible attacks between two communicating parties over an insecure network.
- FR4. Work without storing the password and verification tables in the system to withstand stolen-verifier attacks.
- FR5. Support without synchronized clocks when the communicating parties are not synchronized with their clocks.
- FR6. Provide non-repudiation because of employing personal biometrics.

Several remote user authentication schemes using smart cards have been proposed in the literature (An, 2012; Chou et al., 2013; Das, 2011a,b; He et al., 2008; Khan and Kumari, 2013; Li and Hwang, 2010, Li et al., 2011). He et al. (2008) proposed a self-certified user authentication scheme for next generation wireless network, which relies on the public-key cryptosystem. In 2010, Li and Hwang proposed an efficient biometric-based remote user authentication scheme using smart card (Li and Hwang, 2010). Though their scheme is efficient, it suffers from several security weaknesses as pointed out in Das (2011a). Li et al. (2011) also proposed an improvement on Li–Hwang's scheme (Li and Hwang, 2010). Later, Das (2011b) showed that Li et al.'s scheme (Li et al., 2011) again fails to provide proper authentication in login and authentication phases because there is no verification on user's entered password after successful verification of