www.s2is.org
International Journal on Smart Sensing and Intelligent Systems
ISSN 1178-5608

ADVANCED SECURE USER AUTHENTICATION FRAMEWORK FOR CLOUD COMPUTING

Rui Jiang
School of Information Science and Engineering
Southeast University, Jiangsu 210096
Nanjing, China
Email: R.Jiang@seu.edu.cn

Submitted: Mar. 17, 2013 ***Accepted: July 22, 2013*** ***Published: Sep. 05, 2013***

Abstract*—*Cloud computing, as an emerging, virtual, large-scale distributed computing model, has gained increasing attention these years. Meanwhile it also faces many security challenges, one of which is authentication. Lots of researches have been done in this area. Recently, Choudhury et al proposed a user authentication framework to ensure user legitimacy before entering into the cloud. They claimed their scheme could provide identity management, mutual authentication, session key agreement between the user and the cloud server, and demanded user password change. However, we find the scheme will easily suffer from some attacks such as the masquerading attack, the OOB (out of band) attack, and the password change flaw through our analysis. In this paper, we first point out the security vulnerabilities to the Choudhury et al's scheme, and present the detailed attacks on the scheme. Then, based on some remote user authentication schemes such as Ku-Chen's scheme and Chen's scheme, we apply the two-factor authentication technology to propose our advanced secure user authentication framework which can overcome above security shortages. Without sending one time key through secure OOB channel, our new protocol is able to ensure that only legitimate users can access the cloud service based on smartcard. In addition, our advanced scheme can hold all the merits of the Choudhury et al's scheme. Formal security analysis, which is based on the strand space model and authentication test, proves that our proposed scheme is secure under standard cryptographic. Also, the simulation results illustrate that our advanced scheme is more efficient on the communication performance than other schemes.

Index terms*:* Cloud Computing, Remote user authentication, Smartcard, Authentication, Formal method.