Multi Factor Two-way Hash-Based Authentication in Cloud Computing

K. DeviPriya, Aditya Engineering College, Andhra Pradesh, India
Sumalatha Lingamgunta, University College of Engineering, Kakinada, India

ABSTRACT
The expansion of Cloud computing is influencing various domains such as education, the banking sector, industries, government, health informatics, and individuals. The characteristics of an easy interface, on-demand access, scalability, and low infrastructure investment have to lead to the fast adaptation of Cloud computing based upon their needs. Despite the advantages, Cloud computing is open to more security risks and attacks especially in terms of communication due to the lack of secure authentication and privacy. In this article is presented a novel hash-based multifactor secure mutual authentication scheme that includes mathematical hashing properties, certificates, nonce values, traditional user ids, and password mechanisms that resist MITM attacks, replay attacks, and forgery attacks. We implemented our proposed method in the Microsoft Azure cloud and the results are evaluated. The security analysis is done by using the Scyther tool and with a formal analysis by using GNY belief logic. The results indicate the proposed scheme is capable of providing strong secure authentication.

KEYWORDS
Authentication, Cloud Computing, GNY belief logic, Hash-Based Algorithms, Microsoft Azure Cloud, Multifactor Authentication, Scyther tool, Security Attacks

INTRODUCTION
Cloud Computing is an innovative technology that offers different services through the internet to the users located anywhere on the globe. According to the NIST “Cloud Computing is a model for enabling and access the various resources with minimal resource management.” (Marston et al., 2011). The essential five characteristics, three services, and four deployment models have been used to serve the user requests according to the their demands (Gong, et al., 2010, Zhang, et al., 2010). The characteristics of cloud are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service(Jadeja, et al., 2012). The service models are referred

DOI: 10.4018/IJCAC.2020040104

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
as IAAS (Infrastructure as a Service), SAAS (Software as a Service), and PAAS (Platform as a Service). Private cloud, public cloud, community cloud, and hybrid cloud are the deployment models of the cloud. These services and deployment models are vulnerable to many security attacks. Examples of these attacks on service layers are Authentication attack, Phishing attack, Man-in-the-Middle attack, Cloud Malware Injection attack (Iqbal, et al., 2016). And there are lot of security problems coupled with the deployment models especially public cloud. (JoSEP et al., 2010). In the public cloud environment, the user does not have control on the internal environment, malware, administrator errors. “iPad subscriber privacy leak”, downtime of Amazon S3, and Gmail’s mass email deletions are all such examples due to lack of proper authentication. It is very important to authenticate the users as currently almost 46% of the global population has access the internet. Hence impersonating the legitimate users that help in conducting frauds and theft the data. The current authentication procedures are password-based authentication, hardware-based authentication, and biometric authentication. Password based authentication is the most popular authentication technique, but it is prone to problems due to simple and guessable passwords, usage of the same password between various services which may lead to the guessing attack / dictionary attack. The difficulty with the smart card based authentication is that the user needs to carry the smart card every time and loss of the smart card is hazardous. The drawback of the biometric authentication is its poor tolerance to changes, improper feature extraction and privacy constraints. The motivation behind the multi-factor authentication is to combine the best methods for strong security in turn resisting the identity theft attack (Raja Rajani, et al., 2016). Multi factor authentication involves two-way authentication in which both entities like the server and client authenticate each other (Tshilombo et al., 2019). Enabling the Multi factor authentication between cloud user and cloud server ensure that user trusts the server and vice versa that provides strong resistance to the Man-in-the-middle attack. The present paper proposes the hash based multi factor authentication scheme that includes password-based authentication, user certificates and cloud certificates as multifactors. Unlike the existing schemes, this scheme employs the mutual authentication with multiple secret factors, anonymity of the userID, and the parameters required for the communication which are transmitted through an open environment in a secure way. (Saad et al., 2006).

The rest of the paper is structured as follows. The Related Work section describes the related work. The proposed authentication scheme “multi-factor mutual hash-based authentication scheme” is included in the next section. The experimental methodology and security analysis are presented in the Experimental setup and Security Evaluation of the Proposed Protocol section, Authentication Protocol Verification is discussed in Authentication Protocol Verification using GNU Logic, and finally the paper is concluded in Conclusion section.

RELATED WORK

Existing studies indicate that general authentication mechanisms like password based authentication schemes, nonce based mutual authentication scheme with smart cards, time stamp based authentication schemes(Awashti et al., 2003, Chan et al., 2001 Chen, et al., 2002, Shen, et al., 2003) are considered as traditional algorithms to access the services from the remote servers which are very efficient but not applicable to the cloud environment due to complexity of maintaining the smart cards.

A.J. Choudhury et al. (2011) proposed an authentication framework which combines userID and password with smart card. This scheme is not adaptable for the public cloud environment, due to smartcards adoption is very typical process and their validation process is easily compromise to the cyberattacks. Banyal et al. proposed (Banyal et al., 2013) a multi factor authentication framework by considering OTP and IMEI number secret authentication factors. IMEI number is device-based factor, if the user wants to access the services from other devices is impractical. Sabout Nagaraju et al. proposed the authentication and authorization scheme for online banking system in the cloud. In this scheme, multi factor authentication scheme is designed that allows only authorized users are allowed
Consumers' Attitudes Toward Mobile Commerce: A Model to Capture the Cultural and Environment Influences
[www.igi-global.com/article/consumers-attitudes-toward-mobile-commerce/38972?camid=4v1a](www.igi-global.com/article/consumers-attitudes-toward-mobile-commerce/38972?camid=4v1a)

Value Facilitation as Antecedent of Service Provider Profitability
[www.igi-global.com/article/value-facilitation-as-antecedent-of-service-provider-profitability/163174?camid=4v1a](www.igi-global.com/article/value-facilitation-as-antecedent-of-service-provider-profitability/163174?camid=4v1a)