Two Factor Authentication using M-pin Server for Secure Cloud Computing Environment

Nitin Nagar, International Institute of Professional Studies, Devi Ahiliya University, Indore, India

Ugrasen Suman, School of Computer Science and Information Technology, Devi Ahiliya University, Indore, India

ABSTRACT

Cloud computing is comprised of major demand from the every group of organization because of easy availability and cost effectiveness. The responsibilities of cloud service providers will become increasing more due to the great progression in every cloud computing deployment model (public, private and hybrid) and service models (SaaS, PaaS and IaaS). In this perspective, cloud computing faces multiple challenges, especially in cloud computing security at all levels (e.g., host, network, application and data levels). Authentication is the constantly the biggest concerned for IT industries to adopt cloud computing environment. The availability, performance, key logger attack, malicious insiders, outsider attacks and service disruptions explore (service hijacking) issues are the key research challenges in the cloud computing authentication level. In this aspect, traditional user name and password is not enough as a single factor (first factor). This paper has proposed a secure cloud computing framework which uses first factor as a crypt user name and password with the ATM pin as a second factor called M-pin. The proposed work focuses on a solution to the threats that are the major issues in the cloud adoption.

Keywords: Authentication, Authorization, Cloud Computing, First Factor, M-pin, Two Factor Authentication (2FA)

1. INTRODUCTION

Cloud computing controls the application, infrastructure and the business processes. It is an integration of all services such as Software as-a Service (SaaS), Platform as-a Service (PaaS), Infrastructure as-a Service (IaaS) and Data as-a Service (DaaaS). These services are used to build IT infrastructure scalable, reliable and cost-effective. Sometimes, conventional data center best fit for the organization, but for business agility and economical reason, cloud is pioneered foundation for the companies. Green cloud is the latest sub area added with cloud computing to improve the data center performance (Litoiu, 2010).

DOI: 10.4018/ijcac.2014100104
SaaS is based on the concept of renting a complete finished application from a service provider rather than buying, installing and running the software on the system. Now, licensing of software is not a critical issue for the users and the organization. PaaS provides a platform to receive the computing control, storage and networking infrastructure as a service via public Internet upon which the applications can be developed and executed. IaaS offered computing and storage capability on demand (Litoiu, 2010). There are different tools available for the needs of individual or organization for deployment of their own cloud infrastructure plan. Cloud infrastructure plans may include different deployment tools such as, Eucalyptus, OpenNebula, OpenStack, Nimbus, ABICLOUD, CloudStack etc. These tools provide different services according to the need of users (Nagar, 2012).

Cloud computing security at all levels (e.g., host, network, application and data levels) is the major concern for IT industries to adopt cloud computing environment. The availability, performance, malicious insiders, outsider attacks and service hijacking are the security issues and highlight the key research challenges in cloud computing environment (Al-Aqrabi, 2012) (Popovic, 2010). Other issues pertaining to data security are data location, data transmission, data availability and data security (Mahmood, 2011). Attackers know that access to an application is the first step towards gaining access to the important information stored, processed, or transmitted in the cloud computing. Attackers have focused their efforts in controlling the user’s applications. Several applications have pathetic access control mechanisms are common with security vulnerabilities (Behl, 2011).

Authentication is a primary security concern in cloud computing. The mechanisms used for assuring a communication is verified for enabling other security features, such as data confidentiality and data origin authentication. Authentication requires a user name and password or any other authentication techniques such as hardware token, software token, digital certificates on smart cards and USB tokens, out-of-band authentication and biometrics. There are various protocols such as, OpenID, UMA, LDAP, Kerberos, Radius and SAML, which provide support to build the authenticate frameworks (Chadwick, 2013).

Cloud computing security is the leading challenge in the field of research. The rest of the paper is organized as follows. The section 2 presents a literature survey on various cloud computing security aspects and its related issues. The section 3 states 2FA mechanism and comparison of various 2FA mechanisms. In section 4, we proposed work with an architectural view for improvement of cloud computing security issues. The section 5 presents experiment results of proposed work with various aspects. In section 6, we presented the discussion with a functionality comparison of other 2FA and the future work of proposed work in the cloud computing. In section 7, we state the conclusion and finally, references of the paper.

2. LITERATURE REVIEW

Cloud security issues have recently gained lots of attention from the research community, with a great deal of the focus on securing the operating system and virtual machine on which the services are deployed (Zhou, 2010). Security issues of cloud computing systems focus on the problems of cloud computing, particularly, the security management models based on security standards and the security issues relating to security standards such as the information technology infrastructure library (ITIL) and open virtualization format (OVF). The cloud service providers can follow these guidelines to secure their cloud. It is very important to address the security issues appropriately; otherwise, they could possibly result in unauthorized access to the systems that ultimately lead towards potential fraud data and compromising the confidential data (Chen, 2012). Today, most of the large IT solution providers are becoming entrusted with store of potentially sensitive data into the cloud environment. It is possible that these
Using the Critical Incident Technique to Identify Factors of Service Quality in Online Higher Education
www.igi-global.com/article/using-critical-incident-technique-identify/47092?camid=4v1a