Chapter 48
Keystroke Dynamics Authentication in Cloud Computing: A Survey

Basma Mohammed Hassan
Benha University, Egypt

Khaled Mohammed Fouad
Benha University, Egypt

Mahmoud Fathy Hassan
Benha University, Egypt

ABSTRACT

Cloud computing needs a strong and efficient authentication system because the user will access his rented part through a faraway connection and it will make the authentication sensor device besides the user place for identification and verification so how to know the user who claimed himself to be the legal user. Keystroke identification system as a biometric authentication technique is strongly Candidate for the security issues in cloud computing technology. Keystroke dynamics as a security system did not need extra hardware because the authentication device will be the existing keyboard based on everyone has a unique style for writing. The other biometric methods are addressed with each advantage and disadvantage along with keystroke method. In this paper, all known studies about keystroke technique are explained and compared between them according to the classification technique, number of the participated users and each study results then introduces a survey on software and hardware of other biometric authentication techniques and after the literature review is addressed then keystroke as a biometric authentication system is suggested to access cloud computing environment because it has many advantages to being a part of the known security systems which spread in our world.

DOI: 10.4018/978-1-5225-8176-5.ch048

INTRODUCTION

Cloud computing security issues (Paranjape et al., 2013) such as access control, authentication and authorization (Emam, 2013) requires a high-guaranteed security model to increase the quality of service and user confidence (Chang et al., 2011; Kim et al., 2012). The internet, as the backbone, provides many resources as a utility to end-users as and when needed basis (Seminar report, 2006), so how to know that the user who request to access his rented part in cloud computing to be the legal individual without using a firm authentication technique. Personal identification methods are the most common mechanisms for authentication in cloud computing; however, it is not a secure way for authenticating users. Moreover, most of the biometric identification techniques (Babich, 2012) require special hardware, thus complicate the access point and make it costly to the ordinary users or even to the companies.

Keystroke dynamics (Rupinder et al., 2014; Monrose et al., 1999; Messerman et al., 2011; Peacock et al., 2004; Bergadano et al., 2002) is a biometric identification technique which depends on user behavior while typing on a computer keyboard (Kaur et al., 2013). It is more secure and does not need any special hardware to the access point. Keystroke dynamics is the most apparent sort of biometrics available on computer components, but it has not yet led to real hardware security applications for cloud computing technology if compared to other biometric techniques.

SECURITY ISSUES FOR CLOUD COMPUTING ENVIRONMENT

Cloud computing is not secure by nature because the implicit security system is often unaware and less visible, which creates a false sense of security and worry about what is actually secured and controlled (Tin, 2015) and this makes the users have no confidence. As a result, reduce the number of subscribers and users of this technology.

Cloud computing poses privacy concerns because the service provider or any other hackers can access data stored on the cloud server at any time. It could alter or even delete information by accidentally or deliberately ways. Access control and user authentication are considered the security technologies used for platforms and controls a process in the operating system not to approach the area of another process (Mell, 2011) so if companies supplied the users by the devices to access the cloud computing servers for authentication process, how can be authenticate the legal individual from a faraway other than the cost of such devices? The following sections show the different between many biometric identification methods and why we suggest keystroke dynamics to access cloud computing.

BIOMETRICS SYSTEM OPERATION

The biometric system can be operated in two modes: enrollment and authentication modes.

In the enrollment mode, the biometric system converts the person's biometric characteristics into a template or profile then stores this in a storage system (Divya et al., 2015). In the authentication or test mode, the biometric system can be used for verification or identification processes i.e. compare the new features collected to the stored templates of the user. Figure 1 shows the typical enrollment and test mode for a biometric system operation.

A biometric system is an automated system capable of (Chaudhary et al., 2015; Anil, 2004):