Chapter 10
Biometric Authentication for Cloud Computing

Tarunpreet Bhatia
Thapar University, India

A. K. Verma
Thapar University, India

ABSTRACT

Cloud computing is a way of providing unlimited storage capacity and enhancing parallel processing capabilities without investing in new infrastructure or licensing new software. Designing a secure data access for cloud computing platform is a big challenge as more and more information is placed over cloud by individuals and companies. It is not enough to authenticate a device, or even a user to a device. Cloud computing requires a level of trust that can only be possible through biometric identity assurance, as biometrics offer the unique ability to bind an identity to an actual user, not just to a logical or physical token or credential. This chapter evaluates cloud security by identifying unique security requirements and attempts to present viable solutions based on biometrics to eliminate possible threats. It provides a comprehensive and structured overview of biometric authentication for enhancing cloud security.

1. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing has redefined computing by replacing a client-server organizational centric model with more scalable, efficient and flexible data centric model. This new model delivers convenient, on-demand network access to a shared pool of computing resources (e.g. server, storage area, applications and services) and treats information, software and infrastructure as utilities (Williams, 2012). Secure, reliable, and non-repudiated identification and authentication are critical to the evolution of Cloud computing. Security has emerged as an obstacle in widespread adoption of virtualization as well as cloud computing. It depends from person to person as well as industry to industry how they analyze the concept of security in Cloud Computing. “Security breaches usually entail more recovery efforts than acts of God. Unlike proverbial lightning, breaches of security can be counted on to strike twice unless the route of compromise has been shut off” (FedCIRC). These days, users have dozens of different user name and

DOI: 10.4018/978-1-5225-0983-7.ch010

password pairs to remember so they compromise with safe password practices and put themselves at risk. Organizations and users have become victims of increasing cyber frauds, identity and data thefts which cost global society over USD 388 billion in the last year. Cloud and web services provider need to give their users a better and secure way of using these web services. Cloud authentication requires verification of an individual's identity and associated provisioned right to access data and services in the cloud.

A very simple and appealing solution is biometric authentication, which allows a user to place his finger on top of a scanner, look at the camera or say a passphrase. Your fingers, your eyes and voice are always with you, right? And others people cannot imitate this. What a better way than recognizing their users with cloud based biometrics: a password free user authentication. Biometrics is based on unique traits that can prove individual's physical presence and can neither be stolen, lost, guessed or shared with anyone.

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics such as fingerprints, retina, iris, voice, and signature scan etc (Jain, Ross, & Prabhakar, 2004). The probability of two people sharing the same biometric data is virtually negligible. Biometrics ensure that a person trying to access your network and applications is actually a sanctioned user, and not in possession of a stolen smart card or someone who found, hacked or cracked a password. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. Biometrics Research Centre (BRC) supported by Hong Kong Government and China Government has been playing a leading role in developing biometric projects past 26 years. It provides biometric authentication based on steady features like fingerprint, palm print, voice, face etc and biometrics diagnosis based on dynamic features like DNA, tongue, pulse etc (Zhang, 2006).

The security architecture in cloud environment is illustrated in Figure 1. The inner layer deals with different deployment models of cloud: private, community, public and hybrid. The layer above it representing delivery models: SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastruc-

Figure 1. Security architecture in cloud