ISSN 2229-5518

Data Security in Cloud Computing for Biomatric Application

Prof . D. M Dakhane, Mr. Amit A. Arokar

Abstract— In just the past few years, the amount of biometric data records—typically fingerprints, increasingly rapidly—has expanded wildly as a variety of agencies are called upon to use the latest identification and verification technologies to better target people who, for example, are trying to enter illegally.In many ways, the idea is an exploratory one. It's an attempt to both quantify the scope of the biometric database size explosion and to examine whether cloud computing—a still evolving technology that promises to be limitless in the amounts of data it can analyze and to distribute data rapidly to anyone, anywhere—can tame the biometric overload.With that in hand, we will create a test database, seeded with hundreds of records of biometric data, and run it on a cloud computing platform to document expected gains from implementing cloud computing solutions. "Cloud computing may be the only way to handle vast, unstable query loads—differentiated data in any number of formats and with any number of relationships," Data Security is considered as major aspect in cloud environment while using an application. This Data security can be implemented with respect to user authentication and authorization using cryptography system.

1 INTRODUCTION

Cloud computing has emerged as an innovative and disruptive technology for ALL industry.

Cloud computing is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion. Billing models for these services are generally similar to the ones adopted for public utilities.On-demand availability, ease of provisioning, dynamic and virtually in_nite scalability are some of the key attributes of cloud computing.

An infrastructure setup using the cloud computing model is generally referred to as the \cloud".
The following are the broad categories of services available on the cloud:

- Infrastructure As A Service (IAAS)
- Platform As A Service (PAAS)
- Software As A Service (SAAS)

This cloud is generally available as a service to anyone on the internet. However, a variant called private cloud" is increasingly becoming popular for private infrastructure that has some of the attributes of the cloud as mentioned above.

Amazon Web Services (AWS) is one of the major players providing IAAS. They have two popular services { Elastic Compute Cloud (EC2) and Simple Storage Service (S3). These services are available through web services. The client tools can use EC2 and S3 APIs to communicate with these services. The popularity of these APIs have encouraged other cloud
products to provide support for them as well.
Eucalyptus is a software available under GPL that helps in creating and managing a private or even a publicly accessible cloud. It provides an EC2-compatible cloud computing platform and S3-compatible cloud storage platform. Eucalyptus has become very popular and is seen as one of the key open source cloud platforms. Since Eucalyptus makes its services available
through EC2/S3 compatible APIs, the client tools written for AWS can be
used with Eucalyptus as well.
Ubuntu Enterprise Cloud, UEC for short, is a stack of applications from Canonical included with Ubuntu Server Edition. UEC includes Eucalyptus along with a number of other open source software. UEC makes it very easy to install and con_gure the cloud. Canonical also provides commercial technical support for UEC.

Identity data management and credentialing provide the basis for an array of important security and program decisions, including allowing access to highly sensitive information over a remote network, granting entry through a border control point, providing government benefits, and targeting an individual for additional surveillance or detention. To manage these accesses, organizations independently collect identity information and issue credentials.

- **Identity data management.** Identity data management includes establishing and processing identity information that must be collected and verified. The degree of verification performed defines the degree of confidence that can be placed in the accuracy of the information. Processing identity information requires assigning a unique identifier to the identity that can be used to correlate different attributes that belong to the same identity. Mechanisms that provide this information to authorized parties, while protecting it against intentional or unintentional modification and access, are an essential element of an identity data management system. Once identity information has been established and processed, that information can be acted on to achieve mission objectives.

- **Credentialing.** An identity credential is something that is presented by a user to verify his or her identity when attempting to gain access to a resource. Examples of credentials include username/password pairs, biometrics, digital certificates, or paper forms. Identity credentials are linked to identifiers and are issued and registered by credential management systems. A good credential is difficult to forge or alter—and can be verified at the time of use

2 Literature Review & Related work:

Cloud Architectures are designs of software applications that use Internet-accessible on-demand services. Applications built on Cloud Architectures are such that the underlying computing infrastructure is used only when it is needed (for example to process a user request), draw the necessary resources on-demand (like compute servers or storage), perform a specific job, then relinquish the unneeded resources and often dispose themselves after the job is done. While in operation the application scales up or down elastically based on resource needs.

Instead of building your applications on fixed and rigid infrastructures, Cloud Architectures provide a new way to build applications on on-demand infrastructures

A survey conducted by *IDC* (International Data Corporation) suggests thatcl oud services are still in the early adoption phase. There is a long list of issues cloud service providers need to address. The survey has rated security as the most prominent concern [9]. Buyya [17], provide a survey on current state of the
art in cloud computing and identify key challenges that must be addressed in order to make cloud computing a reality.

Cachin et. al. [18], in their survey, give insight into the well known cryptographic tools for providing integrity and consistency for data stored in clouds.
The security solutions explored and discussed by them are keeping a local copy of the data, use of hash tree, protocols such as Proofs of Retrievability (POR), and Proofs of Data Possessions (PDP), Digital Signatures etc. These solutions still require a testing on some live data to validate their suitability and ease of use. A whitepaper by AWS (Amazon Web Services) discusses physical security, backups, and certifications in their context [10]. Similarly, other providers suchas Google, Microsoft etc. have discussed the security issues in cloud computing [19,20].

Heiser and Nicolett [21] have identified seven prominent risks that customers must assess in order to utilize cloud computing infrastructure. In addition to these seven issues, we have also identified several other major issues that must be addressed by the cloud service providers.
These issues include data server security, privileged user access, and data portability. We also present virtualization specific security issues in detail.

Manchala et. al. [7] have build a trust model in a distributed computing paradigm. To the best of our knowledge, none of the work so far, give a direction to address the security challenges, specifically in cloud environments. Despite the fact that, there are solutions to address the prominent security issues, a mechanism to measure the security risk from the perspective of a service user is strongly needed. Trust models have been studied in distributed information systems [6,7]. Adopting some of the ideas of trust modeling, our work identifies a key set of trust variables and a resulting trust matrix, based on security issues in cloud computing.

Sussman and Booz Allen alumnus James Hutchinson came up with the concept of using cloud computing—Internet-based applications—to drive up the performance of these large biometric databases

3 Analysis of Problem.

Biometric devices are very widely & popularly used all over world as a personal identity verification and authentication, most of the modern day biometric application are desktop or client server based which can be used in local area network but when scope such verification system increases to a Global level a web based application is required to authenticate user situated in different geographical locations and processing will happen with centralized SaaS based application implemented on cloud server.

4 Proposed Work and Objectives:

The proposed study aims at developing such SaaS application with security features with following modules:

4.1 ***Identity management*** is the process of establishing, verifying, and processing identity data for individuals who have or might need access to an organization's resources, and of issuing one or more credentials to the individual that can authenticate the identity in the future.

4.2 ***Access management*** is the process of combining authenticated identity data with other attributes to determine the individual's authorizations and privileges.

4.3 ***Data integrity & Security Management*** is process of providing integrity to data and security of so vast data on cloud server.

4.4.1 ***Change management*** is process of allowing or denying access rights & privilege to various components of the application to its users.

4.4.2 ***SaaS Application*** on Human Resource management application would be developed and implemented as a model application.

5 Desired Implications:

The implication of the current study work can be stated as ….

Development of a SaaS application for Human Resource Management. Role based usage of application implementing security in user authentication , access control and privileges. Developing desktop application and service for reading data from attached Biometric device with Data Security in cloud Computing.

6 Conclusion

"Cloud computing may be the only way to handle vast, unstable query loads—differentiated data in any number of formats and with any number of relationships," Data Security is considered as major aspect in cloud environment while using an application. This Data security can be implemented with respect to user authentication and authorization using cryptography system.

7 References:

[1] Jaliya Ekanayake, Student Member, IEEE, Thilina Gunarathne, Student Member, IEEE, and Judy Qiu "Cloud Technologies for Biometrics Applications"IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 6, JUNE 2011

[2] Booz Allen Ideas Festival Leveraging the Cloud for Big Data Biometrics http://www.boozallen.com/ 2010

[3] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma
"Towards Analyzing Data Security Risks in Cloud Computing Environments"
International Institute of Information Technology,Hyderabad, India

[4] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing "Data Security Model for Cloud Computing"Department of Electronic Science and Engineering, National University of Defense Technology,ChangSha,China Email: darner248@sina.com
ISBN 978-952-5726-06-0 Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) *Qingdao, China, November 21-22, 2009.*

[5] Jaliya Ekanayake, Student Member, IEEE, Thilina Gunarathne, Student Member, IEEE, and Judy Qiu "Cloud Technologies for Bioinformatics Applications". IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 6, JUNE 2011

[6] Cloud Computing Security:making Virtual Machines Cloud-Ready www.cloudreadysecurity.com 2008

[7] Greg Boss, Cloud Computing IBM 2007.10

[8] Carolyn J Dawson, July 26, 2011 "ScaleMatrix, Digitus Biometrics Partnership to Provide Secure Cloud Center"http://dark-fiber.tmcnet.com/

[9] http://www.infosecurity-magazine.com/