Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometric Identification and Token Generation Approach for Implementing Cloud Identity Management

Archana Salaria*
M.tech Student, Department of CSE,
Lovely Professional Univesrity, Phagwara,
Punjab, India

Harshpreet Ahluwalia
Assistant Professor, Department of CSE,
Lovely Professional University, Phagwara,
Punjab, India

Abstract— Cloud computing is a paradigm that reduces the headache of the consumer because they don't have need to manage hardware and software. That is the duty of experience sellers to manage the hardware and software. Generally identity management manages the identities of individuals, their principals, authentication, authorization and rights. While appealing the services from the cloud, cloud user has to give their personal information such as Name, Address, Credit Card Number, Date of Birth etc. So there is need for proper security measures and framework. Biometric Identification also plays significant role in cloud identity management. This paper proposed a secure and cheap cloud identity management by using SHA algorithm

Keywords— Cloud computing, Identity Management, Biometric Identification

I. INTRODUCTION

Cloud computing technology has been designed to solve IT management issues and to run suitable applications. There are mainly two benefits of cloud to user. Firstly Cost and secondly ease of use. The two main concerns of cloud users are security and trust. There are mainly three categories of cloud computing:

- Public cloud
- Private cloud
- Hybrid cloud

II. IDENTITY MANAGEMENT

Identity management (IDM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost , downtime and repetitive tasks.[1]. In cloud computing there is a need of high and proper security because all users' data is kept on the service provider side. That's why Identity management plays an important role in cloud computing. It is the initial step toward accessing the services from cloud.

There are mainly three perspective of Identity management:

A. Pure Identity Management

In pure identity management, without regard to access there is identity creation, management and deletion.

B. User Access Paaradigm

In this earlier user uses the smart card to log on to a service.

C. Service Paradigm

This is a system that provides on-demand, online and presence based services.

III. LITERATURE SURVEY

In [2], biometric authentication as a service that is a ground-breaking approach for the tough authentication in web environments based on the software as a service model. It may be the both the SaaS systems and biometric technologies negatively correlate with observed privacy and data protection risks. They also states the list of evaluation criteria for BioAaaS systems from a data protection that comprises both biometric and SaaS. They further applied these procedure on a prototype implementation of SaaS-complaint biometric authentication service that is based on keystrokes dynamics for the categorization of the enterprise. The results conforms the part of the prototype to the technical data protection requirements. They also show at the organizational level, the conclusion of the service agreement as well as the control of a trust-worthy provider shall be remaining there.

In [3], Identity management plays a vital role in cloud computing. Cloud computing mainly provides on demand services at cheap rate and several user accesses the cloud services. Cloud computing keeps the many user's data on the

service providers side. So there is more chances of threats that harm the user's data. To reduce the impact of threats, there is need to for proper privacy and security. Identity management is the initial step for securely access any data from cloud. This paper gives the overview of Identity life cycle management and patterns in cloud computing.

In [4] Cloud computing technology has been designed to solve IT management issues and to run suitable applications. There are mainly two benefits of cloud to user. Firstly Cost and secondly ease of use. The two main concerns of cloud users are security and trust. Useful features of federated identity management are user management and Single Sign on . Some problems that arise in federated identity management are identity theft, misuse of identities and platform trustworthy. The three main concepts in federated environment and cloud authentication are OAuth, OpenId and SAML. This paper give the overview of the security issues of federated identity in the cloud authentication and presents the proposed model to solve the problem of identity theft in federated environment. The problem definition of this paper is misuse of user identity information through SSO capability in SP's and IDP's. The way of solving vulnerabilities is federated identity architecture (FIA). But the present FIA doesn't have better way to save user's information from harm. So Platform for Privacy performance project (P3P) has been released as a standard & by integrating P3P into FIA.

IV. PROPOSED WORK

This paper proposed a biometric authentication with token generation approach. In this , the functionality of designed model is divided into three parts:

- Sign in
- Upload file
- Download file

The main work of designed model is token generation. The architecture of model is multitier architecture. To make a secure identity management the whole process is divided into three parts:

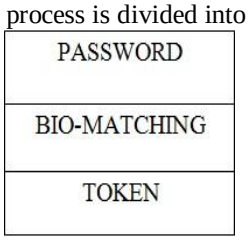

Fig. 1 Multitier Architecture

- Firstly user will authenticate itself by entering password.
- Secondly will match fingerprint template.
- Third Token.

For upload or download file, user has to match the template of fingerprint. When Template matches, then a token is generated. When user want to download the file he /she he has to again match the template and enter token which is generated at upload time.

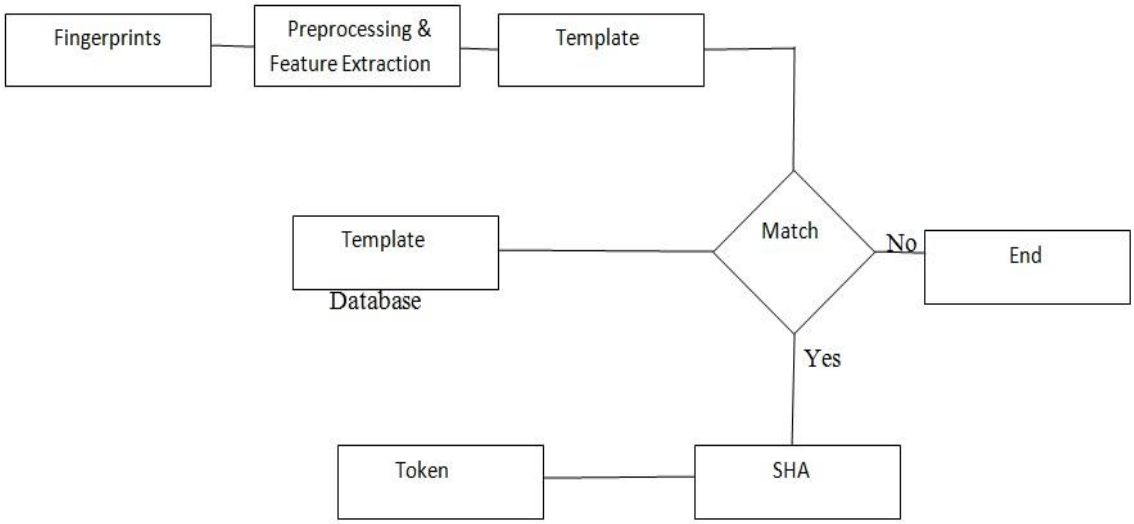

Fig. 2 Token Generation

V. CONCLUSIONS AND FUTURE SCOPE

Cloud computing is a new paradigm. At present, as access of cloud service increases so there is need of high security and access control. So that authorized users access the services that are intended for them. This dissertation proposed a new access control mechanism using biometric to increase the authorization and authentication.

This mechanism merges the biometric to the SHA to create tokens which allow authorized user to access the files of the cloud. This is implemented using cloud analyst and Matlab.

The future work is to implement this mechanism in real cloud environment and to find out more threats to the system.

REFERENCES

[1] The Wikipedia website.[Online].Available: http://en.wikipedia.org/wiki/Identity_management .

[2] Senk, Christian, and Florian Dotzler. "Biometric Authentication as a service for enterprise identity management deployment: a data protection perspective." In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, pp. 43-50. IEEE, 2011.

[3] Gopalakrishnan, Anu. "Cloud computing identity management." SETLabs briefings 7, no. 7 (2009): 45-54.1

[4] Guo, Chunfang, and Ying Wang. "Application of federated identity management in ERP system." In Service Operations and Logistics, and Informatics, 2008. IEEE/SOLI 2008. IEEE International Conference on, vol. 2, pp. 1971-1974.

[5] Jain, Anil, Lin Hong, and Sharath Pankanti. "Biometric identification." Communications of the ACM 43, no. 2 (2000): 90-98.

