Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.884 – 888

RESEARCH ARTICLE

Identity Management System to Ensure Cloud Security

Miss. Priyanka S. Rathod, Prof. Mr. R.R. Keole

M.E (CS-IT) SGBAU, INDIA
M.E (CS-IT) SGBAU, INDIA
priyankas.rathod@rediffmail.com; ranjitkeole@gmail.com

Abstract— ***Cloud computing can provide infinite computing resources on demand due to its high scalability in nature, which eliminates the needs for Cloud service providers to plan far ahead on hardware provisioning. Security is the biggest challenge to promote cloud computing currently. Trust has proved to be one of the most important and effective alternative means to construct security in distributed systems. Multi located data storage and services in the Cloud make privacy issues even worse. In order to efficiently and safely construct entities trust relationship in cloud and cross-clouds environment, identity management services are crucial in cloud computing infrastructures to authenticate users and to support flexible access control to services, based on user identity properties (also called attributes) and past interaction histories . Such services should preserve the privacy of users, while at the same time enhancing interoperability across multiple domains and simplifying management of identity verification.***

Keywords— Authentication, Cloud computing, cross –clouds environment, Distributed system, identity management

I. INTRODUCTION

Cloud services make easier for users to access their personal information from databases and make it available to services distributed across Internet. The availability of such information in the cloud is crucial to provide better services to users and to authenticate users in case of services sensitive with respect to privacy and security. Users have typically to establish their identity each time they use a new cloud service, usually by filling out an online form and providing sensitive personal information. This leaves a trail of personal information that, if not properly protected, may be misused. Therefore, the development of identity management systems suitable for cloud computing is crucial. An important requirement is that users of cloud services must have control on which personal information is disclosed and how this information is used in order to minimize the risk of identity theft and fraud. Cloud computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present as a strong barrier for users to adapt into Cloud Computing systems. Cloud computing successfully uses information technology as a service over the network and can provide end-users with extremely strong computation capability and huge memory space while

with low cost. Security is the biggest threat to adopt cloud computing. Cloud Computing is a general term for anything that involves delivering hosted services over the Internet. Dangers of cloud computing include criminal hacking, inappropriate access by rogue administrators, and the uncertainty of where data resides in a world where notions of privacy differ and regulations vary across national borders. Some people also cite the possibility of online terrorism or even an all-out cyber war as a threat to cloud computing. Corporations and individuals are concerned about how security and compliance integrity can be maintained in this new environment. Identity Management System which will ensure Cloud Security.

II. ARCHITECTURE

Cloud computing can provide infinite computing resources on demand due to its high scalability in nature, which eliminates the needs for Cloud service providers to plan far ahead on hardware provisioning. This is given by the following architecture diagram. We ensure that our structure is secure and that the client's data and applications are protected and we have taken proper security measures to protect the users' information..As known, cloud computing revolves around three major people. The user(s) of the organization who load the data in the cloud, the Cloud Service Provider and the remote user(s) who access the cloud

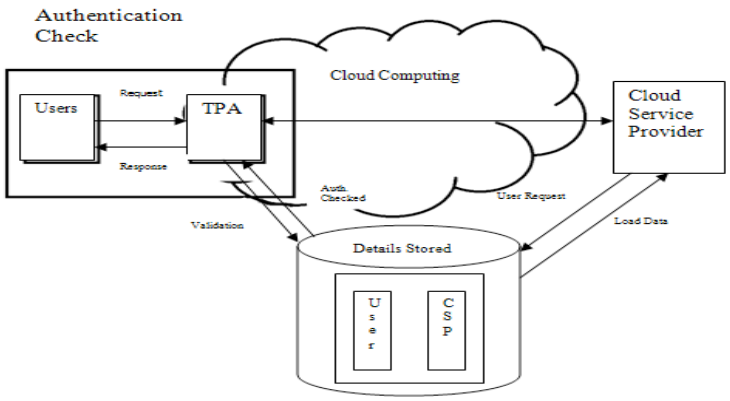

Fig.1 System Architecture

Users

User can be a person or a group of people who belong to an organization. We have provided a broad category- Users, which includes all of them who are involved in loading, accessing and modifying the data in the cloud. They are formally called as the Clients of the cloud Even if we can provide reasonable assurances over the security and integrity of data stored in the cloud, a second major issue to consider is the security of user access to these resources to prevent unauthorized use. The clients can be: A non-technical end user who accesses services through a browser or via applications such as disk backup to remote storage, a developer who employs dynamic resource allocation in clouds to speed application or solution creation or an system administrator who does not build clouds but deploys onto them.

Cloud Service Provider (CSP)

As cloud services have been built over the internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the internet. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure. A cloud provider offers many services that can benefit its customers such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and the use of network and infrastructure facilities. The CSP receives the request and uses it to verify the user's identity from the database. Thereby; we perform dual check for the Identity of the Users of the cloud. Only if the user is an authenticated one, he is allowed to load access or modify the cloud's data. CSP's job in our architecture is to verify the authentication of the user and to maintain the cloud for the organization. The cloud storage provider must be able to provide an encryption schema for the stored data, access control for their data to prevent an unauthorized user from accessing the data, and provide a backup service for their data.

Multi-Cloud Database

The migration of cloud computing from a single cloud to multi-clouds to ensure the security of user's data is extremely important. Fig.2 gives a general overview of the cloud computing environment. Part A represents the client side, which sends data inquiries to servers or instances in the cloud service provider in part B. The data source in part B stores the data in the cloud side which is supposed to be a trusted cloud. In addition, the privacy of any query the client has made must be maintained. But one cannot guarantee the cloud provides a trusted service.

Third Party Auditor (TPA)

The Third Party Auditor uses database for authenticating the user alone. When the user accesses the cloud for the first time, his identification details like Username and Password are entered into the database. The Third Party Auditor is the

person who checks and ensures that the cloud is accessed by an authenticated user. The user sends his response in the form of Username, Password and the requestor loading, accessing or modifying the data in the cloud. TPA is responsible for validating the user.TPA obtains the Username and Password of the user and enters it into the database if the user is logging into the cloud for the first time. For every successive logins, TPA checks for authentication of the user. Once the TPA verifies the authentication of the user, it sends the request to the Cloud Service Provider

Third Party Auditor (TPA)

The Third Party Auditor uses database for authenticating the user alone. When the user accesses the cloud for the first time, his identification details like Username and Password are entered into the database. The Third Party Auditor is the person who checks and ensures that the cloud is accessed by an authenticated user. The user sends his response in the form of Username, Password and the requestor loading, accessing or modifying the data in the cloud. TPA is responsible for validating the user.TPA obtains the Username and Password of the user and enters it into the database if the user is logging into the cloud for the first time. For every successive logins, TPA checks for authentication of the user. Once the TPA verifies the authentication of the user, it sends the request to the Cloud Service Provider

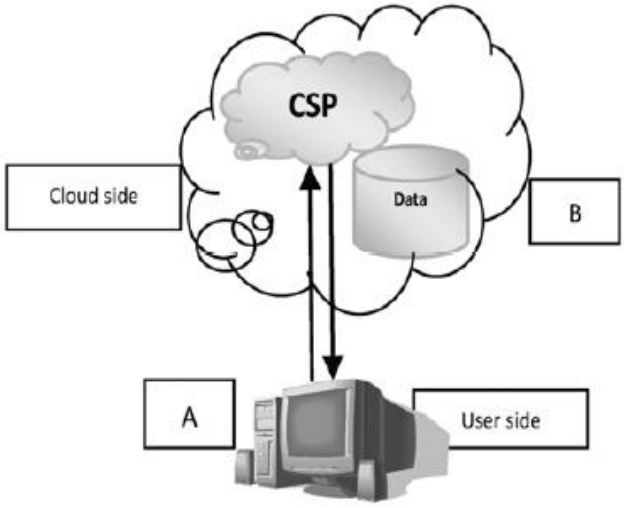

Fig.2 General Overview of User/Cloud Model

III. TRANSPOSITION OF AUTHENTICATION USING FEDERATED IDENTITIES

To achieve security, it is needed to define a security policy which consists of a set of rules that indicates how a system should provide its services by establishing the operating limits of the users within the system and also determine the way in which information and resources are managed, protected and distributed in a given system. Having established security policies, systems must perform the formal descriptions of a behaviour conform to the security models. These models are classified in three basic types

1 - Discretionary model which is based on identity, or simply on user information.

2 - Mandatory or compulsory model which is based on rules, and

3 - Model which is based on roles or allow users' access to resources according to activity performed on the system.

The technologies of Web services focus mainly on ensuring security in the interactions between two unknown entities which possess different security infrastructures.

The vast majority of service providers are protected by some authentication mechanisms. Thus providers are required to keep a record of all customers. Therefore to access the resources, customers should provide their digital identity or carry registration in the system. However, there are problems with identity management both for users and service providers since there is a great quantity of information to handle. The objective of Identity management is to achieve integration of policies, business processes and technologies in order to seize control of access to resources in a secure manner, ensuring the confidentiality of users' information. The identities can be managed in three different ways.

Traditional, centralized and federated.

1- In the traditional model, each service provider provides identities and credentials so that their services can be accessed. Each client has unique and specific identifiers for each service.

2- The centralized model is based on the principle that there is only one identity provider responsible for managing identities that can be used in different departments within the same domain.

3- The federated model allows domains where there are service providers as well as providers of identities and credentials. It is allowed that identities of a certain domain accesses other domains provided that there exist prior agreements between the parts.

IV. USER AUTHENTICATION PLATFORM USING PROVISIONING IN CLOUD COMPUTING ENVIRONMENT

In Fig.3, it shows the authentication of a user in a cloud computing environment, and the related technologies required for the same. When a user registers, it adds personal information that is stored in an appropriate location. In a system, there is a service provider that offers user identification (ID) to perform authentication.

The User sends his request along with the Username and Password to the TPA. The request may be one of the following.

1) ***Request to load data into the cloud***

The user(s) of the organization may require to load data into the cloud for the remote user(s) of their organization. This might require the CSP to double check the user's identity before it allows him to add the data.

2) ***Request to access the data in the cloud***

The remote user(s) of the organization may require to access the data in the cloud. They utilize the internet facility to get access to the CSP to request it for the data. The CSP responds to his request after verifying his authenticity

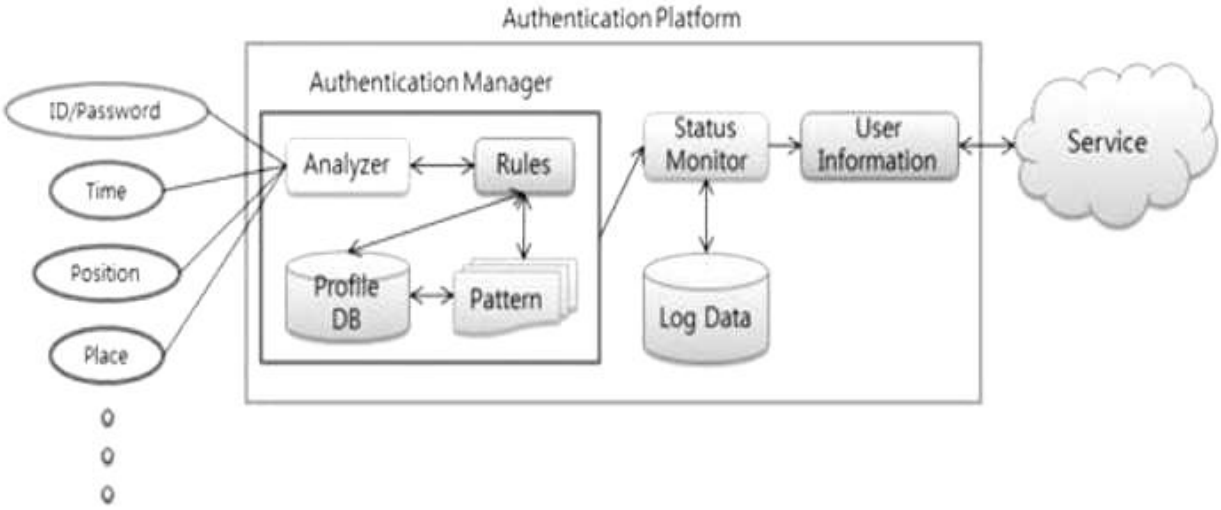

Fig.3 Platform of authentication

.

3) ***Request to modify the data in the cloud***

The user(s) of the organization may require to modify the data present in the cloud. This request is processed by the CSP after the user's verification. The TPA after receiving the request provides the user's details to the CSP. The CSP verifies the authenticity of the User by using his Password. This is done by "Password Checking". The CSP uses its database which contains the Password generated by it from the Salt value provided by the TPA from First Time authentication. This generated Password is verified with the Password obtained from the TPA in this process.

V. CONCLUSIONS

It is clear that, although the use of cloud computing has increased rapidly; cloud computing security is a major issue in the cloud computing environment. Users do not want to lose their private information as a result of malicious insiders in the cloud. In addition, a loss of service availability has recently caused many problems for a large number of cloud users. The authentication manager verifies the user's profile. Authentication may rely on reliable federated entities. Information deemed confidential needs to be protected, thus providers seeks technological innovations that guarantees protection and privacy of information users. In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of user's data in cloud data storage, we proposed an effective and flexible security framework in cloud computing

ACKNOWLEDGMENT

I express my sincere thanks to **Prof P.L.Ramteke, HOD of CSE dept of HVPM, COET, Amravati** for allowing me to present this paper also I express my heartiest thanks to **Prof. R.R.keole Assist. Prof. of HVPM, COET, Amravati** for his valuable guidance while preparing this paper and guiding me time to time. Also all the friends and Staff who help me in preparing this paper.

REFERENCES

[1] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Repor

[2] Anya Kim, John McDermott, Myong Kang,n "Security and Architectural Issues for National Security Cloud Computing",2010 IEEE 30th International Conference on Distributed Computing Systems Workshops

[3] "Authentication Methods and Techniques", Christopher Mallow.
[4] "Guidance for Identity & Access Management V2.1", Cloud Security Alliance, April 2012,
[5] Hiroyuki Sato, Atsushi Kanai, Shigeaki Tanimoto, "A Cloud Trust Model in a Security Aware Cloud" 2010 10th Annual International Symposium on Applications and the Internet.

