Insight into Cloud Security issues

Aishwarya C.S. [1]
Department of Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India.
aishwaryasoundar@yahoo.com [1]

Revathy.S [2]
Department of Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India.
revsan007@gmail.com [2]

***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, this paper proposed a new cloud security framework. In our paper, we provide an Identity Management System which will ensure Cloud Security. We claim that the prosperity in Cloud Computing literature is to be coming after those security and privacy issues having been resolved.**

***Keywords*- cloud computing, security framework, identity management system.**

I. INTRODUCTION

Cloud Computing is becoming a well-known buzzword nowadays. Many companies, such as Amazon, Google, Microsoft and so on, accelerate their paces in developing 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. Even more concerning, though, is the corporations that are jumping to cloud computing while being oblivious to the implications of putting critical applications and data in the cloud. In our paper, we concentrate mainly on the security provided to the cloud. We provide an Identity Management System which will ensure Cloud Security.

II. SYSTEM ARCHITECTURE

Cloud Computing is a general term for anything that involves delivering hosted services over the Internet. In our paper, we concentrate mainly on the security provided to the cloud. We provide an Identity Management System which will ensure Cloud Security. This is given by the following architecture diagram.

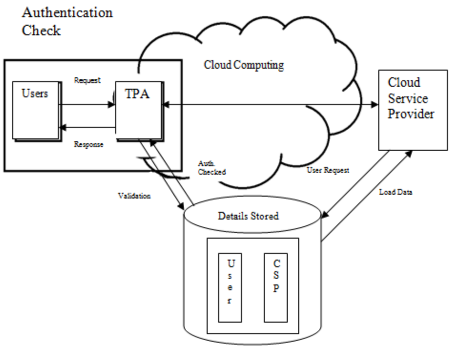

Figure 1. System Architecture

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 (CSP) and the remote user(s) who access the cloud. In our paper, we talk about the following three persons who are participating in the cloud.

A. 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. 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 IT system administrator who does not build clouds but deploys onto them. All these clients are authenticated twice in our system to ensure Data Protection and Application Security in the cloud.

B. Third Party Auditor (TPA)

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 request for 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.

C. Cloud Service Provider (CSP)

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 authenticated user(s) from an organization requests the CSP to maintain the cloud with certain data for all the remote user(s) to access them. The remote user(s) who maybe in need of certain data from his organization can request the CSP to provide him with the same, which is carried out after the authentication process. Thus, CSP forms a basic part in the cloud system which ensures secure data transfers among the clients.

D. Authentication Check

This block takes into account all the users who load, access and modify the cloud as a single entity- Users. There is another person involved in this process of checking the authentication- TPA. The user sends his response in the form of Username, Password and the request for loading, accessing or modifying the data in the cloud. The TPA enters the Username and Password of the user if he is logging into the cloud system for the first time. Else, the TPA verifies the username and password using the database. Once the user's authentication is checked, the TPA sends the user's request to the Cloud Service Provider (CSP), which again verifies the user's identity and responds to the request through the TPA.

E. Database Involved

There is a mention of a single database in our architecture which is utilized by both the TPA and the CSP. TPA uses this 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. So, the user's table in this database contains only the Identification details of the user- Username and Password. The next time when the user logs in, the TPA checks his authentication with the help of this database. There is a separate table which holds the data required for the CSP- the actual data of the user(s). The CSP again re-checks the identity of the user. After the user is verified, his request is responded to by means of the TPA. Thus, we ensure total security of data in the cloud.

III. FIRST TIME AUTHENTICATION

As mentioned earlier, all the users are supposed to register with the cloud for the first time they log in. In this process, we take into consideration the User, TPA and the CSP. The procedure which takes place here is depicted in the following architecture.

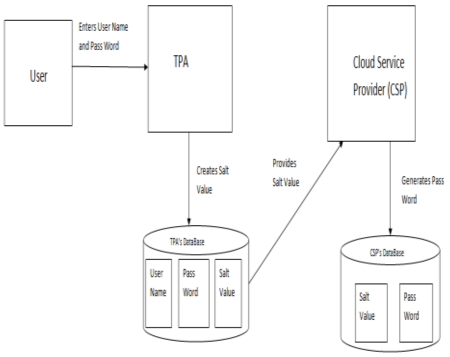

Figure 2. First Time Authentication

The above architecture is followed for all of the users in the cloud. Each user who is entering into the system logs into the system with his Username and Password. Once the login details are provided to the TPA, it generates a “Salt value”, which is a 12-bit number specific to each user’s Password. This salt value is stored along with the Username and Password in TPA’s database. The salt value is provided to the CSP.

The CSP then generates the Password for that particular user for the first time. This Password generated from the salt value along with the original Password received by the CSP is stored in CSP’s database. Thus, this process involves the use of two databases- one for TPA and other one for CSP. The base behind this *First Time Authentication* is by using the “salt value”.

This process is carried on by all the users in the organization who load, access and modify the data of the cloud. This is the basic step to be followed before any data is loaded or is made available to the user.

IV. SUCCESSIVE LOGINS

The user after registering into the cloud is able to load new data into the cloud or access or modify the data present in the cloud. The modification process may include: updation, insertion or deletion of the data in the cloud. These Data Manipulation processes can be carried out only after the user is authenticated after he logs into the cloud system. This process is described using the following diagram.

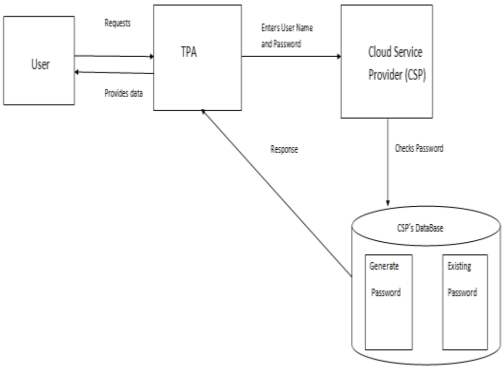

Figure 3. Successive Logins

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.

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, *Successive logins.* The “Password Checking” process is depicted using the following data flow diagram.

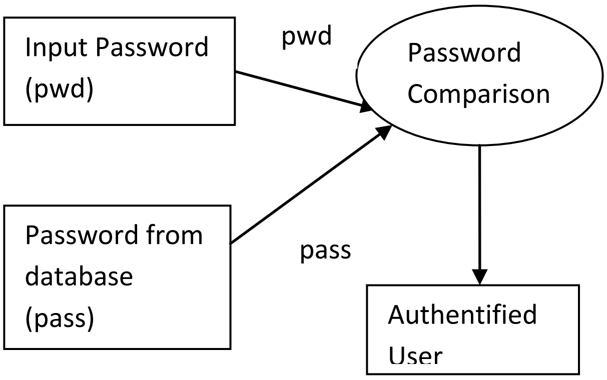

Figure 4. Data Flow Diagram for Password Checking

Once the Password Checking is done and if the user is identified successfully, the CSP responds to his request by sending the requested data to the TPA. The TPA then sends this response to the requesting client. This process is followed each time the user logs into the system henceforth.

V. CONCLUSION

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. 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. Thus this paper proves to be a true enhancement to the security issues relating to the cloud.

REFERENCES

[1] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues" 2009 IEEE International Conference on Services Computing.

[2] 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.

[3] Tharam Dillon, Chen Wu, Elizabeth Chang, "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[4] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and
Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report
2008/489, 2008, http://eprint.iacr.org/.

[5] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou," "Security and Privacy in Cloud Computing: A Survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids.

[6] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure coded
Data," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

[7] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono," On Technical Security Issues in Cloud Computing" 2009 IEEE International Conference on Cloud Computing.

[8] Xue Jing ,Zhang Jian-jun , "A Brief Survey on the Security Model of Cloud Computing", 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

[9] M. Jensen and N. Gruschka, "Flooding Attack Issues
of Web Services and Service-Oriented Architectures,"
in Proceedings of the Workshop on Security for Web
Services and Service-Oriented Architectures (SWSOA,
held at GI Jahrestagung 2008), 2008, pp. 117–122.

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