ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

SECURING CLOUD DATA COMMUNICATION USING AUTHENTICATION TECHNIQUE

[1]PARISHA TYAGI, [2]VIRENDRA KUMAR

[1]Department of Information Technology, Suresh Gyan Vihar University, Rajasthan, India
[2]Department of Electronics & Communication, Suresh Gyan Vihar University, India

ABSTRACT

CLOUD computing, one of the novel techniques for computing is based on non-hardware networks, simultaneous and distributed computing, profitable computing, and service-based structure. Cloud computing is of vital importance and has highly affected the IT industry. It is very important in academics as well as the industry. We already know about four basic utilities i.e. Water, gas, electricity, and telephone. Cloud computing is the fifth one in the list of these utilities.

Cloud computing, undoubtedly is one of the most convenient approaches for storing our data in the form of a cloud but at the same time our data stored should be safe so that it is not moisutilised and no wrong user can get an access to it.

Here, we propose a scheme where data owner, third party auditor and data consumer all will be able to access the cloud on the same site using authentication technique. This will be beneficial in lowering the costs and other capital expenses, increase the efficiency of the working of the system, constrain the size, offer flexibility, real time working and much more.

1. INTRODUCTION

No doubt the cloud computing brings many perks for academic researchers, and likely cloud users, but the problems with the security in cloud computing are serious hindrances which, if not properly taken care of, will degrade its extensive applications and usage in the future.

The most important security issue in cloud computing is security and privacy of the data stored as the data stored is on the internet as a cloud and not on any hardware. Managing the data is another vital concern. In this form of

ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

computing users provide their data to the cloud service providing unit for storing and using it according to the need, where the cloud service provider is mostly a commercial unit which cannot be fully trusted. Data is a very important resource for any organization, and the secret data of any company should not be leaked to its competitors or the consequences can be grave.

Thus, the data in the cloud should first of all be safe and accessible to only the authorized users, in other words, data should be kept confidential. This is the first but not the only requirement. Flexibility and fine-grained access control is also strongly desired in the service-oriented cloud computing model. For example, in a school, the information system is required to restrict the access of students' personal records to certain clerks and the information regarding the marks of the students to their class teachers only. Here access and control of sensitive data is either required by legislation (e.g., HIPAA) or company regulations. Earlier, user's computer needed to have data as well as the software but now cloud computing is possible without the computer actually having any data or even the software.

2. HOW CLOUD COMPUTING WORKS

2.1 BASIC COMPONENTS

- Resources: In cloud computing more than one user share the resources.
- Vast reach: Cloud computing can reach a large no. of systems.
- Flexibility: Resources can be increased and decreased as per the requirement.
- Payment: According to the resources used and time taken.

2.2 ARCHITECTURE OF CLOUD COMPUTING

Cloud Computing Service Models

- **Cloud Software as a Service (SaaS):** Application and Information clouds, Use provider's applications over a network.
- **Cloud Platform as a Service (PaaS):** Development clouds, Deploy customer- created applications to acloud, cloud provider examples Windows Azure, Google App Engine, Aptana Cloud.
- **Cloud Infrastructure as a Service (IaaS):** Clouds for

ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

infrastructure, Processing of the rent, storing the data, capacity of the network, and many more computing assets.

Cloud computing deployment models

- **Private cloud:** Where infrastructure is shared for a specific group.
- **Public cloud:** Bought by the public.
- **Hybrid cloud:** Containing more than one clouds.

2.3 CLOUD COMPUTING BENEFITS

Cloud computing offers lower computer costs. It also helps to achieve improved performance. Moreover, it reduces software costs, provides instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability. It is beneficial in not only lowering the costs but also other capital expenses, increases the efficiency of the working of the system, constrains the size, offers flexibility, real time working and much more.

Many profit based cloud computing systems have been built by different companies e.g., EC2 and S3 by Amazon, and Blue Cloud by IBM among the IaaS systems, Google App Engine and Yahoo Pig among the PaaS systems, and Apps and Sales force's Customer Relation Management (CRM) System by Google among the SaaS systems.

2.4 CLOUD COMPUTING DRAWBACKS

Requires a constant Internet connection, does not work well with low-speed connections, can be slow, features might be limited, stored data might not be secure, and stored data can be lost.

2.5 CLOUD COMPUTING PROVIDERS

Amazon Web Services (AWS) -include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others. Salesforce.com - Delivers businesses over the internet using the software as a service model. Google Apps › Software-as-a-service for business email, information sharing and protection. And other providers Proof-point Sun Open Cloud Platform, Workday and etc.

3. PROBLEM DEFINITION

To ensure the data security in cloud computing environment. We aim to design a new security model for achieving following goals and objectives.

ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

- **Access Control:** In our proposed scheme, if a user wants to access a file or the function then first he/she is required to get the privilege from the authentication module. In our scheme, the authentication module will be the third party auditor. This third party auditor will be capable of authenticating data owner and the user of the data. This third party auditor will be appointed by the cloud service provider.
- **Authentication Data Security:** In our proposed scheme, the authentication module will play an intermediates role. Neither the cloud service provider nor the user of the data will be able to access the authentication data from it.

4. SOLUTION

We are proposing a novel 3-tier model to provide security to users data in cloud computing. The first tier is responsible for data owner and user of cloud authentication. The second tier is responsible for encrypting data owner's data. It is also responsible for protecting user's data from unauthorized access. The third tier is responsible for providing data decryption. It is shown below in figure:

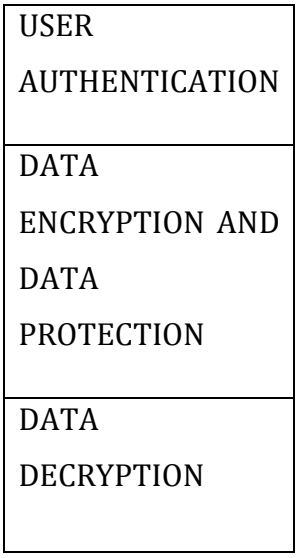

Figure: Proposed Model

Earlier the data user, third party auditor ad data consumer used to be on different sites. the data owner uploaded the data on the cloud and sent it to third party auditor. The data consumer who used to be on a different site needed to authenticate itself in order to access the data. In our new model, the data owner, third party auditor and data consumer all will be on the same site. The data owner will first need to login with its pre decided username and password and then it will be able to upload data on the cloud. Similarly, the consumer will need to enter its pre-assigned username and password in order to download the data from the cloud.

5. ADVANTAGES

- Access Control: In our proposed scheme, if a user can not access a file or

ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

the function without obtaining the privilege from the authentication module. In our scheme, the authentication module will be the third party auditor. This third party auditor is capable of authenticating data owner and the user of the data. This third party auditor will be appointed by the cloud service provider.

- Authentication Data Security: In our proposed scheme, the authentication module is playing an intermediates role. Neither the cloud service provider nor the user of the data is able to access the authentication data from it.
- In our proposed scheme, the third party auditor and users data is on same site. So the time required for the authentication purpose and data encryption and decryption is less in comparison to previous schemes. In previous schemes, the data and the third party auditor were on separate site. It is clear that in that case the time required for authentication will be more.

6. CONCLUSION

In our proposed scheme, the third party auditor and users data is on same site. So the time required for the authentication purpose and data encryption and decryption is less in comparison to previous schemes. Thus this scheme is more efficient with regard to time consumption.

In previous schemes, the data and the third party auditor were on separate site. It is clear that in that case the time required for authentication will be more.

This scheme will also require less cost as all the operations will be carried out from the same site.

REFERENCES

[1] Microsoft Azure, Online

[2] Amazon Web Services at http://aws.amason.com.

[3] R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, A. Fox, R. Griffith, A. D. Joseph [4] M. R. Tribhuwan, V. A. Bhuyar, Shabana Pirzade, “Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management”, IEEE ART Com 2010.

[5] International Journal of Electronics Communication and Computer Engineering, Volume 3, Issue 3, ISSN 2249071X, June 2012.

ISSN: 2348-4098
VOLUME 02 ISSUE 06 JULY 2014

[6] V. Sandhya, A Study on Various Security Methods in Cloud Computing, International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.

[7] Vishwagupta, Gajendra Singh, Ravindra Gupta, Advance Cryptography algorithm for improving data security, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.

[8]. Simarjeet Kaur, Cryptography and Encryption in Cloud Computing

[9] Birendra Goswani, Dr. S. N. Singh, Enhancing Security in Cloud computing using Public Key Cryptography with Matrices, International Journal of Engineering Research and Applications, Volume 2, , July-Aug 2012.Issue 4, 339-344

[10]. G. Jai Arul Jose, C. Sanjeev, Dr. C. Suyambulingom, Implementation of Data Security in Cloud Computing, International Journal of P2P Network Trends and Technology, Issue 1Vol 1, ,2011.