Engineering Universe for Scientific Research and Management
(International Journal)

A Universe of Research
ISSN(ONLINE) : 2319-3069

Vol. 7 Issue 10
October 2015

Cloud Security

Anushree Pandya[1], Jitendra Dangra[2] and Dr. M.K. Rawat[3]
LNCT Indore CSE Department, RGPV Bhopal, Ujjain, Madhya Pradesh, India[1]
LNCT Indore CSE Department, RGPV Bhopal, Ujjain, Madhya Pradesh, India[2]
LNCT Indore CSE Department, RGPV Bhopal, Indore, Madhya Pradesh, India[3]
anushree.pandya01@gmail.com[1], jitendra.dangra@gmail.com[2], drmkrawat@gmail.com[3]

Abstract:
Cloud computing is delivering services by reducing data ownership, improved scalability, agility to business, infrastructure cost reduction and availability of resources just in time.
Cloud Computing is becoming the heart or the central theme for all sort of computing. Cloud is a remote place, at which user can upload data, can download data, can do processing of data, etc. Cloud provides space, computing power, platform and many more services on rent. This paper presents a brief introduction to the concept of clouds & its services. This paper also presents the issues related to the security of data in cloud environment. A few modern attribute based encryption models for the data security have been discussed. This paper also proposes a novel security model for the cloud computing environment. The proposed model combines the advantages of the hierarchical model and the third party auditor based model.

1. Introduction

Cloud Computing [1] is a very new model so there is no single definition has been accepted by the cloud users. Different researchers gives number of definition of cloud computing is by them prospective. But we consider the definition provided by NIST (National Institute of standards and technology) Information Technology Laboratory is as follows:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

By discussion cloud computing is not a single technology but it is the combination of several technologies which enables a new way for IT growth.

2. Cloud Computing Architecture

NIST (National Institute of Standards and Technology) is [2,3] a Standard institution all over the world for their work in the field of Information Technology. I shall present the working definition provided by NIST of Cloud Computing. NIST defines the Cloud Computing architecture by describing five essential characteristics, three cloud services models and four cloud deployment models (Cloud Security Alliance, 2009, p14)

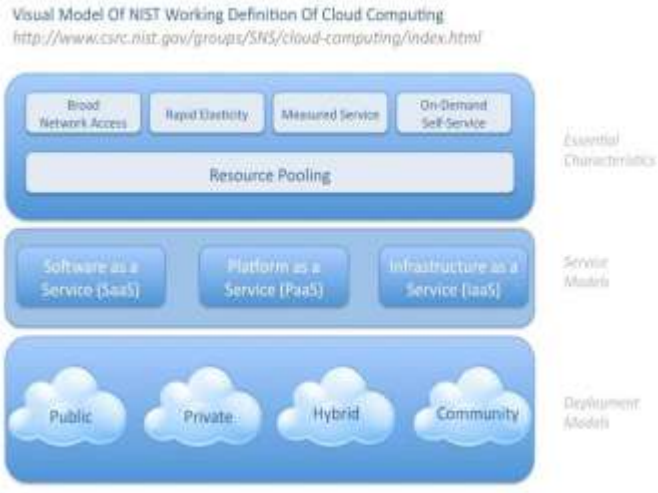

Figure 1: Visual model of NIST Working Definition of Cloud Computing (Cloud Security Alliance, 2009, p14)

3. Cloud key Characteristics[4]

NIST definition states that every cloud infrastructure essentially having the five characteristics which are described below:

- ***On-demand self-service***

The on-demand aspects of Cloud Computing mean that a consumer can use Cloud services as per requirement, without any interrupt of the Cloud service provider. Self-service is user friendly interface, where consumers can adopt computing capabilities such as storage and networking by requesting for the necessary IT resources.

- ***Broad network access***

Cloud service access via internet from a broad range of client platform (e.g. desktop computer, laptop computer, mobile phone, thin client) and enable accessing the services from anywhere across the world by standard platform.

- ***Resource pooling***

Resources are shared with in the cloud service providers. This means that multiple consumers may be using the same set of resources at the same time, and that consumer have no control or knowledge of exact location or details of provided resources.

- ***Rapid Elasticity***

Cloud having ability to expand and reduce IT resources rapidly and elastically

- ***Measured Service***

Cloud systems automatically control and optimize resource use by providing a metering capability to the type of services (e.g. storage, processing, Bandwidth, or active user accounts). Cloud computing enables by virtualization but it is not the necessary attribute.

Security Issues in Cloud computing There are some key security issues and they are as discussed below:

- ***Access issues***

Cloud computing has the threat of accessing the sensitive and critical information. The management of identities and directory services to provide access control. It also takes into account the assessment of an enterprise's to conduct cloud based Identity and Access Management (IAM).

- ***Privacy issues***

Privacy is the main concern to be considered here, and if the cloud services can't provide the level of privacy it can be considered as the main security threat. These privacy issues are mainly irritating across the public clouds, where the access to the clouds is through the public domains.

- ***Availability and backup***

In general most of the client software's and databases are maintained across the remote locations across cloud computing. If the required resources are not available at peak times and even the backup failing across the clouds, this situation definitely leads to lots of security issues.

- ***Data proliferation issues***

Most of the cloud service providers share the information or data to a group of organizations and this situation leads to data proliferation issues. It will be very easy in public cloud to copy the data from different data centers and this finally leads to lots of security issues. There are some chances where the original copy of data can be deleted due to misuse of data proliferation.

- ***Lack of control***

Enterprises mostly don't know where their data is physically stored and which security mechanisms are in place to protect data i.e. whether the data is encrypted or not and if yes, which encryption method is applied also if the connection used for data to travel in the cloud is encrypted and how the encryption keys are managed (Window Security, 2010).

Techniques/ Parameters	KP-ABE[5]	EKP-ABE[6]	CP-ABE[7]	CP-ASBE[8]	HIBE[9]
Access Control	Low High if associated with re-encryption technique	Better than KP-ABE	Average Realization of complex Access Control	Better than CP-ABE	Comparatively low
Efficiency	Average High for broadcast type encryption	Higher than KP-ABE Only allow constant cipher text	Average Not efficient for modern enterprise environments	Better than CP-ABE Less collusion attacks	Better Lower when compared with ABE schemes
Computational overheads	High	Reduces the computations	Average	Lower than CP-ABE	Higher

Table 1: Comparison of various cloud security schemes

4. Proposed System

In our proposed model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. In our model, both data and auditor are present at the cloud servers site. It is responsible for performing functions at all the three layers. The first layer is USER AUTHENTICATION

The second layer is DATA ENCRYPTION AND DATA PROTECTION The third layer is DATA DECRYPTION

Trusted Authority Client

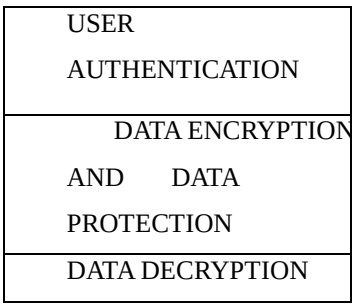

Figure 2: Proposed Model

5. Expected Outcomes

A Novel model which will posses following advantages:

- ***Computational Overhead:***

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.

- ***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.

- ***Scalability:***

We extend HASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower-level third party auditor. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability.

- ***Expressiveness:***

In new scheme, a user's key is associated with a set of attributes, so new scheme is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC) [18]. Thus, it is more natural to apply new scheme, instead of KP-ABE, to enforce access control.

6. Conclusion

The concept of cloud computing with its services are presented herewith. The challenges in the cloud security are also elaborated in detail. This paper also presented a new model for the cloud security. The proposed model combines the advantages of the hierarchical model and the third party auditor based model.

REFERENCES:

1. [1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.
2. [2] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
3. [3] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
4. [4] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.
5. [5] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
6. [6] Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing Attribute-based Encryption with Attribute Hierarchy," In Proc. of ChinaCom'09, Xi'an, China, 2009.
7. [7] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", In Proc. of ICALP'08, Reykjavik, Iceland, 2008
8. [8] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.
9. [9] .Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.