ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Data Confidentiality for Secure Cloud Computing Through Homomorphic Encryption

Dipti Singh Galav
Chhattisgarh Swami Vivekanad Technical
University:Computer Application
Rungta College of Engg. & Tech.
Bhilai, Chhattisgarh

Dr. S. M. Ghosh
Chhattisgarh Swami Vivekanad Technical
University:Computer Science
Rungta College of Engg. & Tech.
Bhilai, Chhattisgarh

Praveen Shrivastav
C. V. Raman University,Computer Application .
Bhilai, Chhattisgarh

Abstract: Cloud computing is the latest emerging technology because of their some ultimate properties like multitenancy, pay-per-use, elasticity and self provision of resources. Instead of all these features many organization do not want to move toward cloud computing. Security is major challenge in cloud computing.When we are putting our data in cloud, it should not be guaranteed that our data is safe. In this paper we are proposing an application which executes operations on encrypted data without decrypting it, in this way we would maintain confidentiality of data in cloud.

Keywords: Cloud computing, IaaS, PaaS, SaaS, Homomorphic Encryption

I. INTRODAUCTION

Cloud computing is a technology which shifts traditional computing technology. It provides different services like IaaS, PaaS, SaaS in different clouds like private cloud, public cloud, protected cloud and hybrid cloud; internet is base for providing such type of services. It reduces cost of storage, economy scale and computing. Like each and everything has two side, it has also the other side which transforms advantages of cloud into catastrophic disadvantage. Cloud security is major area which prevents the users for using cloud services. In 2014 a conference was conducted on "Secure Cloud" by cloud security alliance, European Union Network and Information Security Agency, in this conference it is clear that a cloud will be secure if it focuses on some issues like, legal issues, incident reporting, cryptography, critical information infrastructure, certification and compliance, protection. Cloud must provide:-

a. Data confidentiality
b. Data integrity
c. Authentication

In this paper we focus on data confidentiality, we propose an application of Homomorphic encryption through which cloud users do not need to decrypt the data when data is sending to the cloud provider for performing operations on data.

II. BACKGROUND

There are many definitions of cloud computing but in this paper we will prefer NIST's definition .The NIST definition[1] of cloud computing is (NIST 2009a):

"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."

NIST's definition is defined by three services, five key characteristics and four deployment models they are:

Cloud Delivery services Models:

There are three types of services provided by cloud providers:

a. Infrastructure-as-a-service(Iaas):

The IaaS service is the lowest service model and offers infrastructure resources as a srvice, like raw data storage, processing power and network capacity. The customer can use IaaS service to deploy operating systems and applications. In this customer does not need to manage cloud infrastructure his control is limited to only operating syestem, storage and application.

b. Platform-as-a-service(PaaS):-

PaaS provides operation and development of platforms. Customer does not need to manage infrastructure, they can only deploy and run their application.

c. Software-as-a-service(SaaS):-

It offers applications to the customer. Customer has to manage the applications, operating system and infrastructure also.

A. Cloud Deployment Models:

There are four types of deployment models in cloud:

a. Public cloud:

This architecture runs publically means there is entrusted users who are not employee of any specific organization. This is totally managed by cloud service provider.

b. Private cloud:

This model runs within a single organization, there are trusted users. There is a contractual agreement between organization and cloud service provider.

c. Community cloud:

This model runs by a community within a single organization, there are trusted users. It is simply like private cloud.

d. Hybrid cloud:

This model is combination of public, private and hybrid model. There are both types of users, trusted and entrusted. Entrusted users are prevented to access the private and community services.

B. Characteristics of Cloud Computing:

There are some features of cloud computing is explained:

a. On-demand network access:

Cloud computing resources can be procured and disposed by the consumer without interaction with the cloud service provider.

b. Resource pooling:

It enables the sharing of virtual and physical resources by multiple users, “dynamically assigning and releasing resources according to consumer demand”(NIST 2009a).

c. Broad network access:

Cloud services are accessible over the network via standardized interfaces, enabling access to services not only by complex devices but also by light weight devices like smart phones.

d. Rapid elasticity:

Cloud capabilities can be easily increased if the demand rises, and releasing the capabilities when the need for drops.

e. Measured services:

Cloud computing enables the measuring of used resources, it provides the “pay-per-use” model.

III. SECURITY IN CLOUD COMPUTING

“Cloud Security Alliance, European, Union Network and Information Security Agency and Fraunhofer Institute for Open Communication System organized a conference on SECURE CLOUD in 2014”, [2]in this conference it is clear that cloud will be secure if it focuses on following issues:

a. Legal Issues
b. Incident Reporting
c. Cryptography
d. Critical Information Infrastructure
e. Certification and Compliance

Gartner has discussed [3] seven security issues in cloud computing, following are:-

a. Privileged user access
b. Regulatory compliance
c. Data location
d. Data segregation
e. Recovery
f. Investigative support
g. Data lock-in

“Security Issues in Cloud Computing (2011)”, it focused on distributed architecture of cloud computing to provide on-demand services to customer, when companies are using these services they are facing some security issues, this paper identifies security risks within cloud computing [4].

“Cloud Security Alliance (2010)”, Cloud security has identified seven security threats of cloud computing [5]:-

a. Abuse use of cloud computing
b. Insecure application programming interface
c. Malicious insiders
d. Shared technology vulnerabilities
e. Data loss

IV. HOMOMORPHIC ENCRYPTION

In cloud computing when cloud service provider needs to operate the data then customer has to disclose their data, hence there is a need of a mechanism through which customer do not need to disclose their data, it is possible only through homomorphic encryption.

Homomorphic encryption is used to perform operations on encrypted data without knowledge of private key [6].

Definition:

An encryption is homomorphic if , there are two forms Enc(a) and Enc(b), any arbitrary function f is possible to compute operations on Enc(f(a, b)), where f can be +, × Without knowing the private key. In homomorphic encryption, only two operations i.e. addition and multiplication of raw data is possible.

a. Additive Homomorphic Encryption:-

A homomorphic encryption is additive if,

$\mathrm{Enc}\ (x \oplus\ y) = \mathrm{Enc}(x) \otimes\ \mathrm{Enc}(y)$

b. Multiplicative Homomorphic Encryption

A homomorphic encryption is multiplicative if,

$\mathrm{Enc}\ (x \otimes\ y) = \mathrm{Enc}(x) \oplus \mathrm{Enc}(y)$

V. PROPOSED METHOD

In cloud environment to secure client’s data from cloud service provider we are using homomorphic encryption in our proposed method [8].

A. Broker trusted model:

This model calculates trustworthiness between cloud users and cloud service providers. In this model cloud broker plays an important role in cloud environment. It maintains trust value for cloud user and cloud service provider, also updates values after each interaction. This trust score depends on the interaction between cloud users and cloud service providers [7].

a. Begin
b. Find trust score of cloud service provider by using broker trust model.
c. Determine cloud service provider is whether blacklisted or whitelisted based on their trust score.
d. If cloud service provider is blacklisted, then Use homomorphic
e. Else use standard TLS/SSL
f. End

VI. CONCLUSION

In this paper, we have observed the security problems in cloud computing. In this paper we are trying to maintain data confidentiality in cloud. We are using broker trusted model,

By using this model we are calculating trust score of cloud service provider. If cloud service provider is blacklisted then there will be use of homomorphic encryption, although it is very difficult task because implementation of homomorphic encryption is not feasible. Many of the researches are being in this area.

VII. REFERENCES

[1] Blank M. et. Al. 2011, NIST Definition of Cloud Computing, published by National Institute of Standardand Technology

[2] "Secure Cloud In 2014", presented by Cloud Security Alliance.

[3] http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html.

[4] Curran et. Al., "Security Issues in Cloud Computing", published in august 2011, Elixir Network Engineering

[5] "Seven Security Threats in Cloud Computing 2010", presented by Cloud Security Alliance.

[6] Tebaa et. Al. 2012,"Homomorphic Encryption Applied to Cloud Computing", vol. I 2012 WCE journal.

[7] Uikey et. Al. 2013,"A Broker Based Trust Model for Cloud Computing Environment", vol. 3 Issue 11 IJETAE journal.

[8] Ukil et. Al. 2013,"A Security Framework in Cloud Computing Infrastructure", vol. 5 no.5, 2013 IJNSA journal.

[9] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670. (Article in a conference proceedings)