Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.9, 2015
www.iiste.org

A Trusted Model for Secure Cloud Environment

Dipti Singh Galav
Chhattisgarh Swami Vivekananda University

Dr. H. R. Sharma Dr.SMGhosh
C.S. V.T. U.

Abstract
Cloud computing is an emerging technology that gives a tremendous changes in IT industry. It has ultimate features like multitenancy, elasticity, pay-per-use, self provision etc. But the customers are still hesitant to adopt cloud computing due to security and privacy. In this paper we propose a trust model which secures client's information from both insiders and outsiders. In this model calculation of trust is based on their compliance report which has been promised in service level agreement.
Keywords: cloud computing, trust, compliance, SLA, symmetric encryption

I. Introduction

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. Basic reason is lack of trust of client on service provider which prevents the users for using cloud services.

In this paper we are proposing a trust model in which in which user's data will be in encrypted form, also check whether a cloud service provider is trusted or not which will be depend on the compliance have been promised in service level agreement. Since encryption of data and maintain security key , assigning security key to cloud service provider for performing operations is complicated task for cloud users, hence in this paper we are introducing a trust reporter who will be certified by any standard organization such as cloud security alliance. Trust reporter will work at client side that will be responsible for determining trusted cloud service provider, for assigning secret key to cloud service provider.

II. Backgroud

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.

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.

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. Related Works

"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

"**Compliance based Trustworthiness Calculation Mechanism in Cloud Environment**", this paper design and simulate a trust model which uses compliance monitoring mechanism to build trust between client and service provider. In this paper a trust calculation is based on the compliance monitoring report. Compliance report is aggregation of compliance from peers [3].

"**A Trusted Third Party (TTP) Based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment**", this paper develop an encryption scheme by combining both symmetric and asymmetric algorithm which provides strong data confidentiality, including renewable public key certificate through trusted third party [4] .

"**AES Proposal: Rijndael, AES Algorithm**", in this paper Rijndael algorithm was accepted as an Advanced Encryption Standard by National Institute of Standard and Technology. In this scheme a plain text is divided into a fixed size blocks, these blocks will be processed through ten rounds of encryption iterations which make it more complicated for attacker [5].

"**Global Trust: A Trust Model for Cloud Service Selection**", this paper describes assessment of trust in cloud computing and proposed a new trust model which is based on QoS selection and certain trust model, which extend opinion trust model [6].

"**A Trust Model of Cloud Computing based on Quality of Service**", this paper describes how service level agreement is prepared combining quality of service requirements of user and capabilities of cloud service provider. Also proposed a model which performs better than First in First out model and similar models [7].

IV. Proposed Model

In this section we are introducing our proposed model, in which it performs the following tasks:-

1. Encryption of client's data

2. Provide secret key to trusted party
3. Finalization of SLA between client and service provider
4. Generation of trust report by trusted party
5. Assigning secret key to service provider by trusted party
6. Transfer of cipher text to service provider

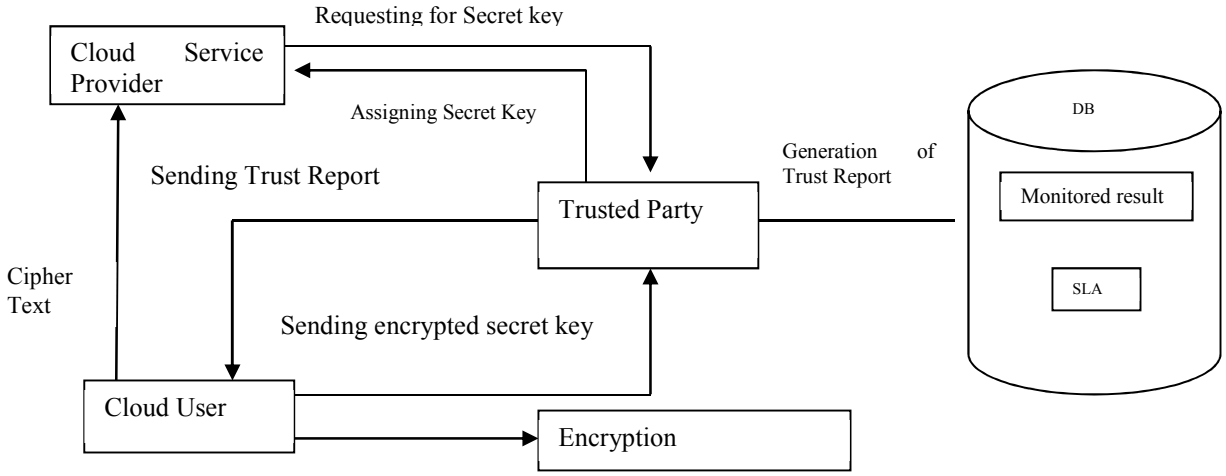

Figure 1 "Trusted Model for Secure Cloud Computing"

Following steps are discussed in detail as follows:

Step 1: Encryption of Client's Data:-

Before uploading their data to cloud server client has to be encrypted their data. Here we will prefer Advanced Encryption Standard-x (AES-x) where x is a size of secret key using Rijndael algorithm which has been chosen by panel of NIST in 2005.

In this algorithm a plain text is divided into a fixed size blocks and these blocks are highly randomized so that it is infeasible for attacker to break it.

Step 2: Provide Secret Key to Service Provider:-

For securing communication among three entities i.e. cloud service provider, trusted party and cloud user. We use public key cryptography, RSA algorithm is used for checking digital authentication.

After encryption of client's data, client transfer the secret key which can be encrypted using public key infrastructure to trusted party. Trusted party is also responsible for verification of client's data.

Step 3: Finalization of SLA between Client and Cloud Service Provider:-

After negotiation a contract is signed between client and cloud service provider called Service Level Agreement (SLA) which includes availability, performance, security and privacy of data, disaster recovery expectation, location of data, portability of data etc. SLA should act as guidelines for handling potential problem. SLA should be very specific on certain terms and conditions to avoid betting.

Step 4: Generation of Trust Report by Trusted Party:-

Trusted party is responsible for generating trust report. For generating a report it compares parameter of SLA with monitored results and services which is used by client. Trusted party maintains a database for storing monitored results which can be combination of services which are used by client or may be gathered from peers. Based on these reports it will be feasible for client to find out whether a cloud service provider is trusted or not.

Step 5: Assigning Secret key to Service Provider Through Trusted Party:-

Trusted party performs the following tasks:

a. To identify cloud service provider's identity
b. To check whether a cloud service provider is trusted or not

To identify cloud service provider's identity:

Trusted party will identify cloud service provider's identity by using decryption cryptography such that

$D_{uk->cspm} < E_{vk->cspm}(MD_{comp})> = H(mi)$

Where H is cryptographic hash function implementing on a small block of (mi).

To check whether a cloud service provider is trusted or not

Based on trust report trusted party will verify whether a cloud service provider is trusted or not, also verify that promises which have been made in SLA will be fulfilled or not, based on these report trusted party assign the secret key to cloud service provider.

Step 6: Transfer of Cipher Text to Cloud Service Provider:-

After assigning a secret key to service provider by trusted party , client will send cipher text to service provider .

V. Conclusion

The proposed trusted model ensures that the client's data will be secure. In this model client's data will be in encrypted form. It also verifies whether a service provider is trusted or not. It also reduces client's complexity of maintaining secret key, assigning secret key with the help of trusted party.

In future we will verify this model MATLAB technology. We are implementing an equation which calculates trust score that will be beneficial for this model.

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] Sidhu Jagpreet et. Al. 2014, "Compliance based Trustworthiness Calculation Mechanism in Cloud Environment" published by Elsevier B. V.
[4] Rizvi Sayed et. Al. 2014, "A Trusted Third Party (TTP) Based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment published by Elsevier B. V..
[5] Daeman J. et. Al 1999., "AES Proposal: Rijndael, AES Algorithm", presented at National Institute of Standard and Technology .
[6] Filali F. et. Al. 2015"Global Trust: A Trust Model for Cloud Service Selection", Published in IJNIS
[7] Paul Manuel. "A Trust Model of Cloud Computing based on Quality of Service", is supported by Kuwait University,Research Grant No.[WI07/11]

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar