RESEARCH ARTICLE OPEN ACCESS

Validating Metering and Billing In Cloud Computing

Jasjit Singh Samagh
M-Tech in Computer Science, JCDMCOE,sirsa
Haryana-India

ABSTRACT
Cloud Computing is a new class of network based computing that takes place over the Internet. Cloud computing has changed everyone's thought of infrastructure, architecture, software, delivery systems etc. With the development of this technology security issues are seriously raising its head. In order to address such security issues many steps have been taken by the cloud providers. Among the security issues, billing verification method play an important role by which the service user can ascertain that the charges being made by the cloud provider for computational purpose is in accordance with the amount of work done by him. In view of above I propose solution for achieving security on metering and billing procedure. By the use of this method the chances of billing being tempered by the cloud provider become negligible. The said approach is useful in the development of cloud computing security and business thereof.
Keywords:- Cloud Computing, Security, Billing, Metering, Tempering

I. INTRODUCTION

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet,

- basically a step on from Utility Computing
- a collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform).
- Using the Internet for communication and transport provides hardware, software and networking services to clients

These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface).

A number of characteristics define cloud data, applications services and infrastructure:

- **Remotely hosted**: Services or data are hosted on remote infrastructure.
- **Ubiquitous**: Services or data are available from anywhere.
- **Commodified**: The result is a utility computing model similar to traditional that of traditional utilities, like gas and electricity - you pay for what you would want

The various cloud deployment models are shown below:

- **Public Clouds:**

In public cloud vendors dynamically allocate resources on a per-user basis through web applications. For example: Drop Box, Sky Drive and Google drive.

- **Private Clouds:**

Due to security and availability issues more and more companies are choosing Private Clouds. It provides more secure platform to the employees and customers of an organization. For example Banks, In banks all the employees and customers can access the bank data which is assigned to them particularly.

- **Hybrid Cloud:**

Hybrid cloud is the combination of the Public cloud and private cloud. In this type of cloud services the internal resources, stays under the control of the customer, and external resources delivered by a cloud service provider.

- **Community Cloud:**

The community cloud shares the infrastructure around several organizations which can be managed and hosted internally or by third party providers.

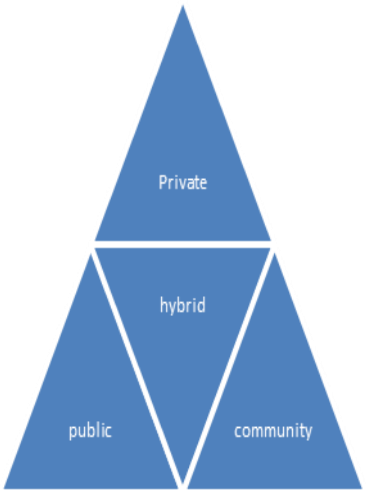

Figure 1.1 Deployment models

Various Service models of cloud are:

- **SAAS(Software as a service) -** It is concerned with web application usages services.
  SAAS provides following services:-
  - Support running multiple instances on it
  - Develop software that runs on cloud

  E.g. Gmail , Facebook

- **PAAS (Platform as a service)** – It is concerned with developing, testing, deployment and maintenance
  PAAS provides following services:-
  - Platform allowing developers to create program that run in the cloud
  - It include several application services which allows easy development

  E.g. Google app Engine.

- **IAAS (infrastructure as a service)** – It is concerned with storage, processing and network services
  I AAS provides following services:-
  - Consists of database servers and storage
  - Highly scaled and shared computing infrastructure

II. SECURITY ISSUES ON CLOUD

Companies are moving rapidly in cloud as they provide the best resources available in the market in a short time i.e. within the blink of eye and also reduce operations' cost. But with more and more information is moved to the cloud the security concerns have started to develop.

Some of the security issues are as follow:-

- Data breaching is the biggest security issue where a capable hacker can easily get into a client side application and get into the client's confidential data.
- Denial of Service (DoS) is also a major threat wherein the user is granted partial or no access to his/her data. Companies now use cloud 24/7 and DoS can cause huge increase in cost both for the user and service provider.
- Connection eavesdropping is also a major threat that means that a hacker can scan your online activities and reproduce a particular transmission to get into your private data. It can also lead to the user to illegal or unwanted sites.
- Data loss is also a threat where a malicious hacker can steal the data or any natural/man-made disaster can destroy the data. In such cases an offline copy of the data is a big advantage.
- Compatibility between different cloud services is also an issue. If a user decides to move from one cloud to another the compatibility ensures that there is no loss of data.
- Insufficient understanding of cloud technologies can lead to unknown levels of risk. Companies move to cloud because it provides substantial reduction in cost but if transfer is done without proper background learning, the problems that arise can be even greater.
- Safe storage of encryption keys is also a problem. Even if you are using encryption for enhanced security, safe keeping of the key becomes an issue. Who should be the owner of the key? User seems to be the answer but how diligent and careful can he/she be will decide the security of the data.
- Inefficient and flawed APIs and interfaces become easy targets. IT companies that provide cloud services allow third party companies to modify the APIs and introduce their own functionality which in turn allows these companies to understand the inner workings of the cloud.

III. METHODOLOGY, ALGORITHM AND IMPLEMENTATION OF VALIDATING THE BILLS

Cloud is utility based computing system in which we pay for it similar as we pay for utilities like electricity, water and gas. These utilities are measured by number of units consumed. But in cloud no proper way is established which show that we charged for the same, we utilized. Not any cloud provider gives the information about the resources utilized and real reporting time to the end user. So it makes fear in the mind of user, whether the computational task provided by the cloud service was executed completely and the billing charges counted by enterprises are fair or not. Then how we can assure that cloud provider uses fair method of billing. This type of problem especially arises in the huge database system where a lot of transaction happens in small amount of time. Our scheme confirms the billing security cycle of cloud provider. When client search a query in huge database system which store lack of records.

The proposed design is as follows:
Step1: Divide the whole database into small parts called slices, denoted as M1, M2…..Mn

Step2: Execute search query for particular record.

Step3: If record found in first attempt, calculate Message Authentication Code (MAC) of first slice as

S1 = MAC (M1)

Else

{

Calculate Sn = MAC (M1+M2+…+Mn)

}

Step4: Send calculate MAC to client node

Step5: Repeat step 2 to 4 on third party trusted system for same search query

If (TSn = CSn) then

{Result ok}

Else {tempered}

TSn = MAC at trusted third party system.

CSn = MAC at cloud server.

The benefit of this method is the verification of billing procedure and provides the proper security system to user for cloud. Figure illustrates our proposed solution

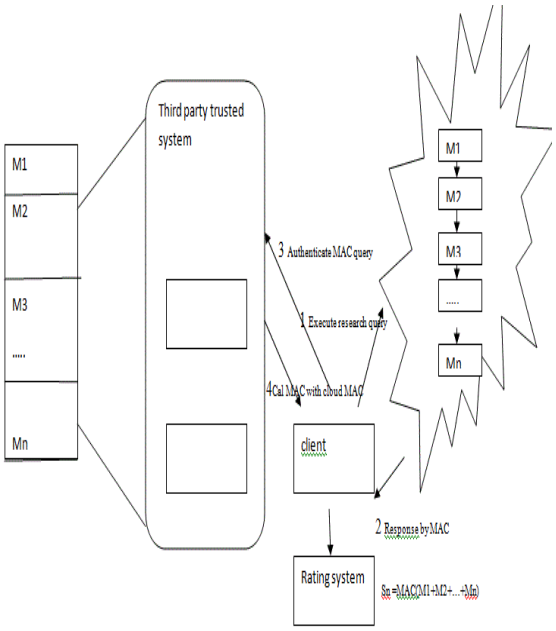

Figure: Validation of billing procedure

Evaluation procedure

In this part we store the results of experiments, if the percentage of success or correctness is more than 95% we assign 5* to the cloud provider. If the success rate lies between 80% to 90% than 3* and if percentage of success is between 70% to 80% the single * is assigned to cloud. These results are published to the open systems, so users or enterprises would check the prestige level of cloud before adopt the service of that cloud. By following these results customers attracted towards reliable cloud provider. So the working strategies of cloud provider will improve and don't tamper with billing methods to give reliable services to the cloud.

Attack Scenario

The cloud provider's server may skip some part of database during the query search in order to avoid extravagant computation overhead. This results in providing incomplete information from server to client.

Our architecture prevent this harmful behavior of server as it returns unique message digests of the slices which can be verified with trusted third party storage. Our scheme has confined protection for users when cloud service provider and trusted third party collude and send fake digest to the victim client. Clients can easily avoid this scenario by hosting there data on government accredited or world standardized trusted organizations. Client may use various trusted third parties and contacting multiple servers to verify the results.

V. CONCLUSION AND FUTURE WORK

The proposed scheme gives a proper solution for security of billing charges and to give reliable services without tempering to the end user. The results of our method are upgraded to some government organized sites to show the performance result of our system. However there are some technical and non technical realities that make security somewhat difficult to deliver in a cloud. The cloud presents a number of new challenges in data security, privacy control, compliance, application integration and service quality. It can be expected that over the few years, these problems will be addressed. According to our research knowledge there will be lot of more work is required. Firstly there will be proper resource provisioning method will established to scale the requirements of users needs. The problems related to security issues of data reside on cloud will also be sort out. The major problem of data security is due to the fact that both the data and the programs reside over provider's premises. So no security is provided to user side to ensure that their data is secure from other users and service providers is also getting proper charges. Now these days methods are being developed that provide transparency over billing in public systems. Still this field requires a lot of work to do.

REFERENCES

[1]. "Security Issues for Cloud Computing"- Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham ,April-June 2010

[2]. "Security In Cloud Computing Using File Encryption" ,Ashish maheta , MAY-JUNE 2012)

[3]. "Security In Cloud Computing Using File Encryption",Mr Tejas P.Bhatt and Asst Prof Ashish Maheta , November- 2012

[4]. "Cloud Data Security using Authentication and Encryption Technique" , Sanjoli Singla, Jasmeet Singh , July 2013

[5]. Ch-15 "Cloud Computing" by Mark Baker

[6]. Ch-12 "Cryptography and Network Security" by William Stallings