RESEARCH ARTICLE OPEN ACCESS

MAC in Cloud Security

Jasjit Singh Samagh
M-Tech Department of Computer Science and Engineering,
JCDM College of Engineering,
Barnala Road, Sirsa,
Haryana-India

ABSTRACT

Growth of cloud computing has changed everyone's thought of infrastructure, architecture, software, delivery systems etc. At the same time it requires minimal investment in hardware, software, in training the human resources etc. It encompasses various elements from grid computing, virtualization, autonomic computing into innovative development of architecture. With the development of this technology security issues are also seriously raising its head. In order to address such security issues many steps have been taken by the cloud providers. Encryption in cloud computing is one of such steps. Among the security issues billing verification method play an important role by which the clients can ascertain that the charges being affected by the cloud provider for computational purpose is in accordance with the amount of work done by such a client. For achieving security of data of service user we use message authentication code. By the use of this method the chances of tempering the data by the cloud provider or third party become negligible. The said approach is useful in the development of cloud computing security.

Keywords:- Cloud Computing, Security, MAC, Encryption, Authentication

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.

➢ **Commodfied**: 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.

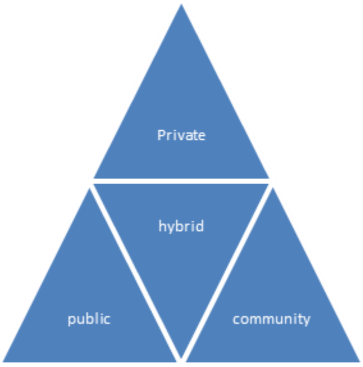

Figure 1.1 Deployment models

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. VIRTUALIZATION AND VIRTUAL MACHINE

Virtualization:
Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. You probably know a little about virtualization if you have ever divided your hard drive into different partitions. A partition is the logical division of a hard disk drive to create, in effect, two separate hard drives.

Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.
There are three areas of IT where virtualization is making head roads, network virtualization, storage virtualization and server virtualization

Virtual Machine:

A virtual machine is a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer. A virtual machine behaves exactly like a physical computer and contains it own virtual (i.e, software-based) CPU, RAM hard disk and network interface card (NIC).

An operating system can't tell the difference between a virtual machine and a physical machine, nor can applications or other computers on a network. Even the virtual machine thinks it is a “real” computer.

Nevertheless, a virtual machine composed entirely of software and contains no hardware components whatsoever. As a result, virtual machines offer a number of distinct advantages over physical hardware.

IV. METHODOLOGY

For the purpose of application of MAC in securing the cloud from various forms of attack the following methodology is used as shown in figure 1.2

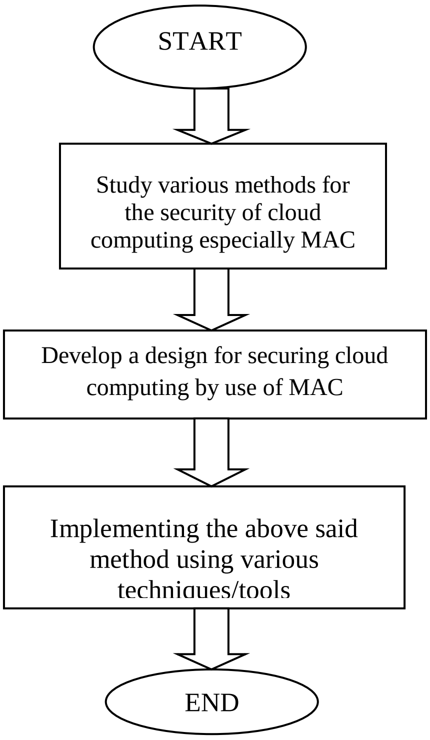
START
Study various methods for the security of cloud computing especially MAC
Develop a design for securing cloud computing by use of MAC
Implementing the above said method using various techniques/tools
END

Figure1.2 Methodology

V. IMPLEMENTATION

To implement the MAC for securing cloud computing we use different software tools including CYGWIN, HADOOP, JAVA and ORACLE. With the use of above tools, we can make the cloud and through it, we have to develop one application and run that application in the cloud environment. It is MAC that resolves the security related problems at cloud and give confidence to the user to shift on cloud. It helps maintaining integrity over cloud. We implemented MAC with the help of DBMS-CRYPTO package. The package is compatible with oracle10g only. We entered many messages in oracle 10g that is installed over all machines, the data is entered from the server side or either may be from client side now issues the command of distributed file system and map reduce and then this task is distributed according to the setup interior working engine system, then a query is fired to show some result when require, then the field accessed by server to find particular record to satisfy the query, then MAC of fields is calculated sent to user by this package. It can also be used to store data in encrypted form over cloud network and no one can access your stored data without your knowledge or permission because in this package there is need to supply a key by user. Then at the timing of retrieving of data you can apply same procedure for retrieving of data. This will enhance your data integrity.

VI. CONCLUSION AND FUTURE

Cloud computing growth is in its awful phase due to its value propositions of low costs, improved performance, unlimited storage capacity and increased computational power. Enterprises across all sectors are eager to adopt cloud computing but the security is required to accelerate cloud adoption on large scale. Currently cloud computing security issues have lot of loose ends which create uncertainties in the mind of potential user. Until a proper security module is not placed, the enterprises or single users are unable to leverage the advantages of this growing technology. Present techniques would not very efficient to stop tempering with cloud charges. The proposed scheme gives a proper solution for security of data and to give reliable services without tempering to the end user.

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 lot of more work is required to be done. Firstly the 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 sorted 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 also. These days methods are being developed that provide security over open and public systems. Still this field of information requires a lot of work to be done.

REFERENCES

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

[2] “Virtualization”, Margaret Rouse, December 2010

[3] “Security In Cloud Computing Using File Encryption” ,Ashish maheta , MAY-JUNE 2012)

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

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

[6] Ch-15 "Cloud Computing" by Mark Baker

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