MAC Implementation in Cloud Computing

B.S Sarada
Dept. of Computer Science, India International School in Japan

Abstract
Cloud computing compromises of 3 important terminologies in the world of computing – infrastructure, storage and application. Cloud computing is replacing the usual network architecture with its performance and availability. The drawback that is noted with cloud computing is 'Security'. The security issues in cloud haven't got a permanent solution so far. In this paper, we discuss a solution to eavesdropping and man in middle attack by introducing message authentication code (MAC) method. The cloud architecture used here is P2P in nature, ie no master server exist. The peer to peer approach enables the fault tolerance property when a server failure occurs.

Keywords
Cloud Computing, P2P, Security, Message Authentication Code

I. Introduction

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business requirements over the internet so that it will be easily accessible and available. Cloud resources can be rapidly accessed and easily scaled, with all processes, applications, and services provisioned on demand, regardless of the type of the user and location of the user. Since the services and resources are available any time it increases the efficiency of the company lending the resources thereby giving better profit. The delivery of the product can be done on time with minimum infrastructure and cost. Cloud provides a solid support to companies in developing new products. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud.

The major concern with cloud computing is with security. Cloud providers have identified the cloud security concern and are working hard to address the problem. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.

Different models of cloud computing have various ways of exposing their underlying infrastructure to the user. This influences the degree of direct control over the management of the computing infrastructure and the distribution of responsibilities for managing its security.

With the Software as a Service (SaaS) model, most of the responsibility for security management lies with the cloud provider. SaaS provides a number of ways to control access to the Web portal, such as the management of user identities, application level configuration, and the ability to restrict access to specific IP address ranges or geographies.

Cloud models like Platform as a Service(PaaS)allow clients to assume more responsibilities for managing the configuration and security for the middleware, database software, and application runtime environments. TheInfrastructure as a Service (IaaS) model transfers even more control, and responsibility for security, from the cloud provider to the client. In this model, access is available to the operating system that supports virtual images, networking, and storage.

II. Threats in Cloud Computing

Cloud faces the major types of threat in the network. The threat in cloud hasn't got a solution so far as in usual network. The threats in cloud are described below:

A. Denial of Service Attack

The aim of a denial of service attack is to deny legitimate users access to a particular resource. When the high workload on the flooded services notifiesby Cloud Computing operating system then it will startproviding more computational power to cope with theadditional workload. Thus, the server hardwareboundaries for maximum workload to process will not hold much for longer time there by saving the time. In that sense, cloud system is trying to work against the attacker, but if the attacker is stronger then he could damage the service availability entirely starting from a single flooding point to the end of the service data. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single entry point data and damage the whole system.

B. Man-in-the-middle Attack

The man-in-the-middle attack (often abbreviatedMITM). As the name indicates, a man-in-the-middleattack occurs when someone between you and the person with whom you are communicating is activelymonitoring, capturing, and controlling yourcommunication transparently. It is also defined as activeeavesdropping where attacker makes independentconnections between users and relays messages betweenthem. Man-in-the-Middle attacks are often referred to as"session hijacking attacks", in which the intruder aims togain access to a legitimate user's session without the knowledge of the client and server who is transmitting it.

C. Network Sniffing

A sniffer is an application or device that can read,monitor, and capture network data exchanges and readnetwork packets. Data packets are transmitted fromone network device to another which causes the risk thatoutsider could see our data. Sniffing is used to see whattype of traffic is being passed on a network and to lookfor things like passwords, credit card numbers, and soforth.

D. Port Scanning

Port scanning can be defined as "hostile Internet searches for open 'doors,' or ports, through which intruders gain access to computers". The basic step is simply sends out a request to connect the target host on each port sequentially. It is the technique used to identify open ports and services available on a network host but it also used by hackers to target victims. If repetitive port scans are made, a denial of service can be created. Hackers typically utilize port scanning because they can easily identify services which can be broken. They conduct tests for open ports on Personal Computers that are connected to the web for accessing it.

E. SQL Injection Attack

There is a big influence of web application on our life.Several business houses and governments and society ingeneral depend on this. All these web applications areaccessed via internet therefore security risks associatedwith it. Usually RDBMS

(Relational DatabaseManagement Systems) is used for database by webapplications .They provide interface to the user toinput the information in the form of SQL statementswhich are executed on the RDBMS. By using SQLinjection, malicious user can alter the protected data, leak the sensitive information or crash the entire system.

F. XML Signature Element Wrapping

In cloud computing, clients are connected via a web browser or web service which increases the probability of web services attacks in cloud computing. XML signature element wrapping is common attack for Web service. XML sign are designed to facilitate integrity protection and origin authentication for a variety of documents types. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attackerwould like and moving the original element to somewhere else on the SOAP message. Suppose we use a signature to secure the transmit data then outsider can't be able to change that data. But this attack allows a malicious user to change the signed information what is being sent. Combination of WS-security with XML signature to a particular component in the system.

G. Browser Security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just send a request and wait for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. . As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user. But SSL support point to point communication means the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user by installing sniffing packages on intermediary host.

H. Flooding Attacks

The most significant feature of the cloud system is toprovide dynamically scalable resources. Once there aremore requests from clients, cloud system repeatedlyincrease its size. Flooding attack is basically distributing a large amount of non-sense requests to a certainservice. Once the attacker throws a batch of unusedrequests by providing more resources cloud system willattempt to work against the requests, ultimately system all resources are consumed by the system and it is notable to serve normal user requests. These attacks charges extra cost to the consumer for the usage of resources.

I. Cloud Malware Injection Attack

Cloud malware injection attack is to make attempt toinject a malicious service, application or even virtualmachine into the cloud system depending on the cloudservice models (SaaS, PaaS and IaaS) In order to perform this attack, the first step of intruder is to generate his personal vindictive application. Once the vindictive software is entered into the cloud structure the attacker had to trick the cloud system to treat the malicious software as a valid instance. If successful user ask for the vindictive service then malicious is implemented.Attacker can also upload virus program in to the cloudsystem. Once the cloud system treats it as a valid service, the virus program is automatically executed and the cloud system infects the virus which can cause damage to the cloud system completely within short time.

J. Incomplete Data Deletion

In cloud computing, replicas of data is placed in overdifferent server because of this data does not removecompletely. This is known as Incomplete Data Deletion. When a request to delete a cloud resource is made,most operating systems this will not remove accuratelyAccurate data deletion is not possible because copies ofdata are stored on another sever but are not available.

III. Security Measures

- The security in cloud can be implemented in different ways. The implementation methods are listed below:
- Implement a secure program that can maintain any issues that can happen in the cloud network.
- Implement and maintain a good cloud infrastructure.
- Maintain confidentiality in the data stored in the cloud storage space available at different locations.
- Implement identity checking when the client is trying to access the data from the client data storage.
- Implement intrusion management using the algorithms available and test the cloud security applications for certain duration of time.

1. Securing Data at Rest

Cryptographic encryption is certainly the best practice and in many U.S. states and countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self-encrypting drives that implement the TCG's Trusted Storage standards. Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

2. Securing Data in Transit

Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

3. Authentication

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorised users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The TPM can easily provide stronger authentication than username and passwords. TCG's IF-MAP standard allows for real-time communication between the cloud provider and the customer about authorized users and other security issues. When a user is fired or reassigned, the customer's management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within seconds of time it happens inside the network. If the fired user is logged into the cloud, they can be immediately disconnected. Trusted Computing enables authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

4. Separation Between Customers Present in the Cloud

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation. In addition, the TPM can provide hardware-based verification of hyper visor and VM integrity. The TNC architecture and standards can provide strong network separation and security.

5. Cloud Legal and Regulatory Issues

To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion. Trusted Storage and TPM access techniques can play a key role in limiting access to data stored in cloud storage space.

6. Incident Response

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehaviour. An automated response or at least automated notification is the best solution. TCG's IF-MAP (Meta data Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and of user misbehaviour when it happens at any location.

IV. Proposed System

The proposed system of cloud is different from the basic cloud system architecture. Here we were implementing the security method in a cloud system with P2P network. The advantage of using P2P is fault tolerance property, ie, even if one server fails the client won't feel the lag in processing of data. It will be done immediately by another one server and formatted data is available to client on time.

There are multiple servers involved in this network and collection of servers we call as cluster. Here in one cluster we have database which stores metadata of every server data which can be accessed by multiple clients at a time. The metadata contains information regarding the location of the file, control information, accessibility of file details. So whenever a client want to access a file it need to send request to database, from there only it will be redirected to the location it's searching.

The Message Authentication Code (MAC) [6] method implementation is as follows:A sends B a message M encrypted by their shared secret key K. Because a third party is unable to recover the plaintext of the message without the knowledge of K, confidentiality is provided. Now let's examine how encryption mechanism can provide message authentication. Generally, B is assured that the message is from A, because A is the only person (other than B) who is able to generate the cipher text that can be decrypted using K. Further, if M is fully recovered, B knows none of the bits of M have been altered.

In the architecture shown in fig 1, the MAC is implemented between each server communication. The servers when transmitting the data will encrypt the data using the shared secret key K. When a client wants to access the data in any of the server he will provided with the key of the server alone and thus preventing the client from accessing the data in other servers. The main purpose of encrypting the data between the servers is to avoid the eavesdroppers to view the data and also to avoid Man in the middle attack. If the data is in encrypted format its tough for the hackers to access the data and destroy them.

The architecture operation is as follows:

1. The client sends the request to access the data through the gateway. This entity can transfer the request or response between the Client App with the network and can lead the request to the database where the location address of the server is available.
2. The gateway forwards the request to database and database will check in its entry for the data the client has client. If the metadata is having the keyword specified by the client the database will redirect the client to corresponding server along with it key will be send.
3. The client now can access the data using the key provided and perform the needed task. The client is only granted the permission to access the data it has requested.

The database of the architecture contain the details like control information, key of the server data, metadata and also the location. Each pair of servers will have a secret key shared between them. The database will store the key of these pairs.

When one of the servers fails the secret key is shared to the new server to access the data and process it. The database architecture is shown in fig. 2.

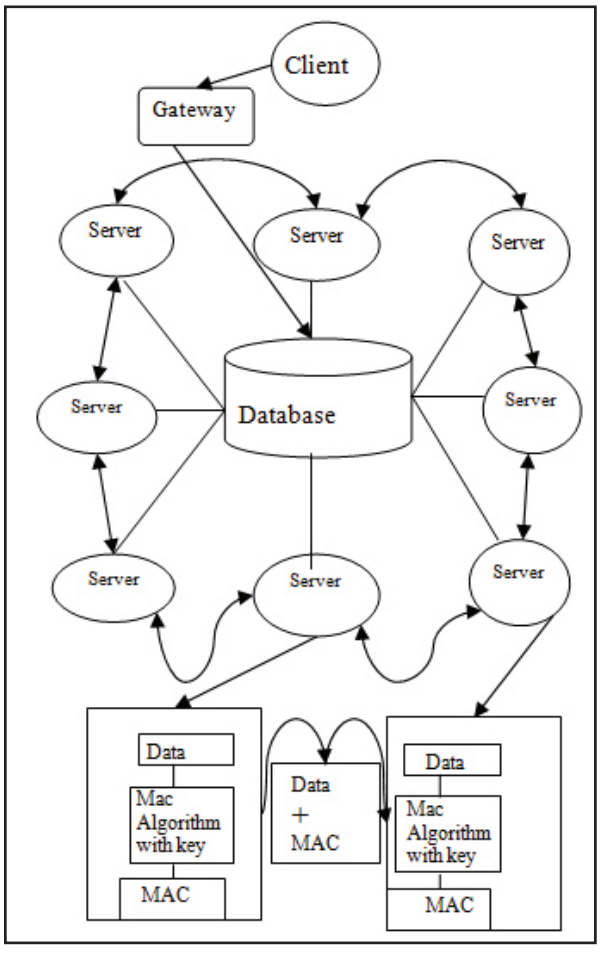

Fig. 1: System Architecture

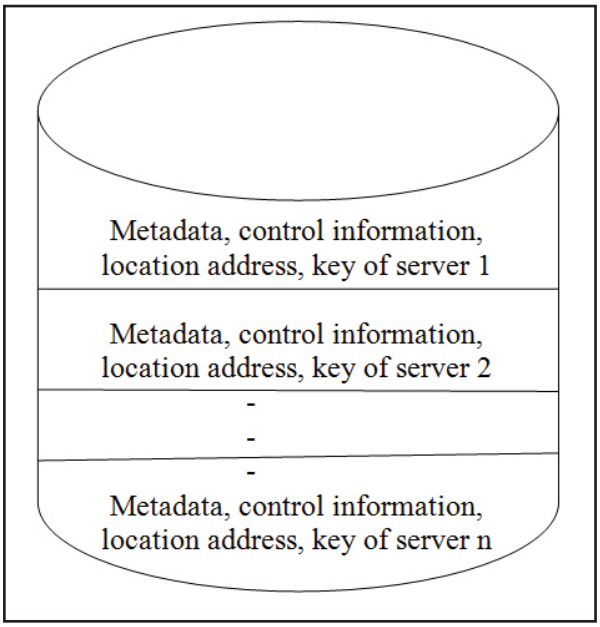

Fig. 2: Database Architecture

V. Conclusion and Future Work

The advantage of a system without central entity architecture is that it prevents the bottleneck that could arise when a large number of clients are trying to access the data in the servers. When a central entity is controlling this task it will take time to process the request from each client and redirect. And also it won'tknow how to redirect the server data processing when one of the servers fails. The next advantage of the proposed system is that it is providing security to the data stored in the servers. The big clients are concerned very much about the security in the cloud. If proper authentication and confidentiality can be provided to data in the cloud then a large number of clients will start to use the cloud features which will give advantages like less maintenance, better performance etc.

The future work that can be made in this system is to provide security at the gateway itself so that only authorized clients only will access the servers. The next step that can be performed is to implement security to data in the cloud using either DSA or RSA algorithm.

References

[1] Harjit Singh,"Current Trends in Cloud Computing A Survey of Cloud Computing Systems", In: International Journal of Electronics and Computer Science Engineering.

[2] NishaBawaria, Kamlesh Namdeo, Pankaj Richhariya "High Performance AAA Security for cloud computing in hierarchical", In: International Journal of computer Applications Vol. 132, No. 15, December, 2015.

[3] Anurag S Barde,"Cloud computing and its vision", International Journal of Electronics and Computer Science Engineering, Vol. 2, No. 4 July 2013.

[4] Komal Verma, Rajiv Pandey, Arpit Gupta,"Cloud computing: Does it call for distributed file system", International Journal of computer applications,Vol. 131, No. 13, December 2015.

[5] Karamjit Singh, Isha Kharbanda, Navdeep Kaur,"Security issues occur in Cloud Computing and there Solutions", In: International Journal on Computer Science and Engineering (IJCSE).

Sarada B S received her M.tech degree in Information Technology from Hindustan Institute of Technology and Science, Chennai, India, in 2011 and the B.tech degree in Computer Science and Engineering from Kerala University, Kerala, India, in 2009. She started her carrier as corporate trainer and quality auditor in NeST Technologies (now acquired by Quest Technologies) in 2011. She enrolled as an Assistant Professor of Mar Baselios College of Engineering and Technology in 2012, and was responsible for teaching the engineering and research (M-tech) talents. Pursuing international experience, she flew to Japan on 2014 and joined as a faculty in charge of Computer Science and Administrator of India International School-Japan, Yokohama in 2015 till date. Her research interests include cloud computing, network security, networking and cloud security.