Providing Security to Cloud Computing through MAC

Paridhi Singhal
Department of CSE, Mody Institute of Technology & Science,
Lakshmangarh, Rajasthan, India
prachisinghal333@gmail.com
www.mitsuniversity.ac.in

Niranjan Lal
Department of CSE, Mody Institute of Technology & Science,
Lakshmangarh, Rajasthan, India
niranjan_verma51@yahoo.com
www.mitsuniversity.ac.in

Manoj Diwakar
Department of CSE, Dehradun Institute of Technology,
Dehradun, Uttarakhand, India
manoj.diwakar@gmail.com
www.dit.edu.in

Abstract

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing share distributed resources via network in the open environment thus it makes security problems. So we are in great need of encrypting the data. We proposed a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system though MAC. In this paper some important security services are including like authentication, encryption and decryption are provided in Cloud Computing system.

Keywords: Security, Credentials, Data Encryption, MAC, Authentication.

1. Introduction

Cloud computing providers offer their services according to three fundamental models [1]: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS). Where IaaS is the most basic and each higher model abstracts from the details of the lower models Fig 1. In 2012 network as a service (NaaS) and Communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem.

The advantage of cloud is cost savings and the prime disadvantage is security, so we need to secure cloud from the unauthorized users.

Cloud computing is used by many software industries nowadays. Since the security is not provided in cloud, many companies adopt their unique security structure [2]. (For eg. Amazon has its own security structure). Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle in this paper. Since the data placed in the cloud is accessible to everyone, security is not guaranteed. We proposed a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system with Message Authentication Code (MAC). In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.

This paper is organized as follows in section 2 we have discussed some characteristics of cloud computing. In section 3 advantages of cloud computing. In section 4 Literature survey. I section 5 we describe existing security mechanism is used in cloud. In section we have proposed a cloud security with MAC and. Finally we conclude the result.

2. Characteristics

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics"[3, 12, 14]:

2.1. On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2.2. Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

2.3. Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand [4, 12].

2.4. Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time [5, 12].

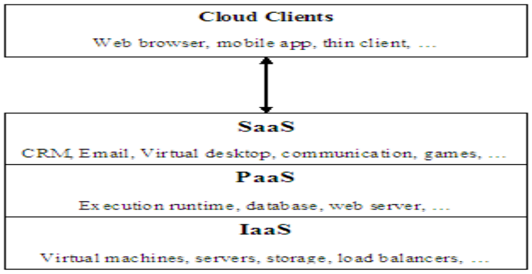
Cloud Clients
Web browser, mobile app, thin client, ...
SaaS
CRM, Email, Virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, ...
IaaS
Virtual machines, servers, storage, load balancers, ...

Fig 1. Cloud infrastructure

2.5. Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [6, 14].

3. Major Advantages of Using Cloud Computing

As cloud computing has taken hold, there are ten major benefits that have become clear,

- Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
- Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
- Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.
- Streamline processes. Get more work done in less time with less people.
- Reduce capital costs. There's no need to spend big money on hardware, software or licensing fees.
- Improve accessibility. You have access anytime, anywhere, making your life so much easier!
- Monitor projects more effectively. Stay within budget and ahead of completion cycle times.
- Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.

- Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs.
- Improve flexibility. You can change direction without serious "people" or "financial" issues at stake.

4. Literature Review

4.1. Online data storage using implicit security

The Davies, D., and Price, W describe the use of a data partitioning scheme for implementing such security involving the roots of a polynomial in finite field. The partitions are stored on randomly chosen servers on the network and they need to be retrieved to recreate the original data. Data reconstruction requires access to each server, login password and the knowledge of the servers on which the partitions are stored. This scheme may also be used for data security in sensor networks and internet voting protocols [7, 12]. The authors have described an implicit security architecture suited for the application of online storage.

In this scheme data is partitioned in such a way that each partition is implicitly secure and does not need to be encrypted. These partitions are stored on different servers on the network which are known only to the user. Reconstruction of the data requires access to each server and the knowledge as to which servers the data partitions are stored. Several variations of this scheme are described, which include the implicit storage of encryption keys rather than the data, and where a subset of the partitions may be brought together to recreate the data.

4.2. Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing

The third party auditor (TPA) as shown in Fig 2, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance [3]. They may also dynamically interact with the CS to access and update their stored data for various application purposes.

The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users.

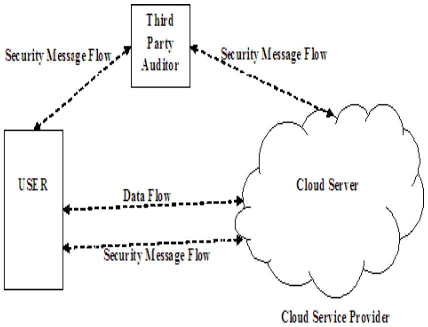

Fig 2. The architecture of cloud data storage service

Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation.

We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users [8]. Fig 2. [9].

The architecture of cloud data storage service The Cloud Computing model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called Cloud servers, and service requesters, called clients. Often clients and servers.

5. Existing System

To introduce an effective third party auditor (TPA) for privacy and security, the following fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements.

This scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The security and performance is justified through concrete experiments and comparisons with the state-of-art.

In cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful eployment of the cloud architecture. Another problem is that data stored in the cloud does not remain static [10].

6. Proposed System

The Proposed Network consists of three backup sites for recovery after disaster. The backup sites are located at remote location from the main server. If any one of the paths fails it uses alternate path working [9]. The encrypted file will be creating during back up sites. The data will be decrypted during recovery operation. Proposed a cross platform integration model using secure communication via the Internet and the utilization of a key for security.

6.1. Data Backup Operation

Client sends the data to the server which is known as Main Server. At the same time data is also back up to Multi Servers. In this method for data backup it involve with three Multi Server such as (SA1 (Server, Application), SA2, SA3, etc…).

6.2. Operation

Multi-server sends the key ID to our mail ID.

6.3. Data Encryption

The data is to be encrypted figure3 in multi-server. In encryption the data that has to stored in a cloud cannot be stored in a text format due to security reasons so it must be transformed into an encrypted format. This method deals with the encrypts the data before it is taken as back up in multi server. To encrypt the data's MAC (Message Authentication Code) is used.

6.4. Message Authentication Code

A function of the message and a secret key that produces a fixed length value, known as a cryptographic checksum or MAC that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K. when A has a message to send to B, it calculates the MAC as a function of the message and the key: MAC = C (K, M),

Where,

M= Input message
C= MAC function
K= Shared secret key
MAC= Message authentication code

The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC.

If we assume that only the receiver and the sender know the identity of the secret key, and if the received MAC matches the calculated MAC, then,

- The receiver is assumed that the message has not been altered. If an attacker alter the message but does not alter the MAC, then the receiver's calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to know the secret key, the attacker cannot alter the MAC to correspond to the alterations in the message.
- The receiver is assumed that the message is form the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper MAC.
- If the message includes a sequence number (such as is used with HDLC, X.25 and TCP), then the receiver can be assured of the proper sequence because an attacker cannot successfully alter number.

6.5. Authentication

Suppose the data is deleted in the client system. Then we authenticate the data through following procedures: Find the key in our email id. Give the file name and date in login form. Where MAC is used [11, 13]:

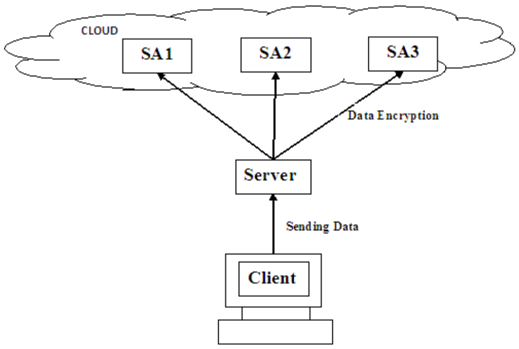

Fig 3. Data Backup

- There are number of applications in which the same message is broadcast to a number of destinations. Examples are notification to users that the network is now unavailable or an alarm signal in a military control center.
- Another possible scenario is an exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages. Authentication is carried out on a selective basis, message being chosen at random for checking.
- Authentication of a computer program in plaintext is an attractive service. The computer program can be executed without having to decrypt it every time, which would be wasteful of processor resources.
- For some applications, it may not be of concern to keep messages secret, but it is important to authenticate messages. An example is the Simple Network Management Protocol Version 3.
- Separation of authentication and confidentiality functions affords architectural flexibility. For example, it may be desired to perform authentication at the application level but to provide confidentiality at a lower level, such as the transport layer.

7. Conclusion

Authentication is necessary in Cloud Computing. After referred the papers we proposed a new idea that Secure Cross Platform Communication in a cloud through MAC. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. Cloud Databases are an emerging type of non relational databases which do not follow relational algebra and are generally key-value oriented systems which are used for storing internet scale data and provide easy programmatic access. The main goal is to securely store and manage data that is not controlled by the owner of the data. The data are stored in cloud environment Cloud security here is solved by providing a credential for data in the cloud. This credential can be used to retrieve data from the cloud in a secure manner.

8. References

1. Shucheng Yu., Cong Wang†, Kui Ren†, Wenjing Lou., "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society for publication in the IEEE INFOCOM 2010.
2. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010.
3. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.
4. Loud Security Alliance, "Security guidance for critical areas of focus in cloud computing", 9, [Online] Available : http:// www.cloudsecurityalliance.org.
5. Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta, Manoj Diwakar, "ffective Ways of Secure, Private and Trusted Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, 2011.
6. A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep, 2009.
7. Abhishek Parakh, Subhash Kak, "Online data storage using implicit security", 2009.
8. H. Shacham, B. Waters, "Compact proofs of retrievability", in Proc. of ASIACRYPT 2008, vol. 5350, pp. 90–107,
9. S.Sajithabanu, Dr.E.George Prakash Raj, "Data Storage Security in Cloud", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011
10. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010.
11. Niranjan Lal, Mrityunja Singh, "VoIP over the 802.11 WLAN Network" International Transaction in Applied Sciences (ITAS) , Vol.2, No.1 Jan 2010 (PP.191-200),India
12. Niranjan Lal, S.Qamar, Mayank Singh, "Detailed Dominant Approach Cloud Computing Integration with WSN" 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness , Springer Digital Library(LNCS) January 11–12, 2013
13. Davies, D., and Price, W. "Security for Computer Networks", New York: Wiley, 1989.
14. Niranjan Lal, S.Qamar "Internet-ware cloud computing: Challenges" International Journal of Computer Science and Information Security (IJCSIS) , Vol. 7, No. 3, March 2010(pp.206-210)Pennsylvania, USA.