Enhancement of Security for Data Storage in Cloud

M. Hemaanand [1], K.Varalakshmi[2]

[1]Department of Computer Science and Engineering, SRM University, Chennai, India
hemaanandit@gmail.com

[2]Assistant Professor, Dept of Computer Science and Engineering, SRM University, Chennai, India
Varalakshmi.kk@gmail.com

Abstract-***Cloud computing is the use of computing resources such as hardware and software that are delivered as a service over the internet.Since the user's data are usually processed or stored remotely in unknown machines,user may not have full control over the data and it can be accessed by some third party.The data stored in the cloud should be decentralized in order to adapt to nature of cloud. In the existing system the jar file is used to hide the data which can be subjected to attack. To overcome the above problem the proposed system uses the Steganography method .In this method the data is hidden behind the image and the image is converted into a Jar file and stored in the Cloud, when the data access take place the reverse process is carried out to get the original data and the user is allowed to access the contents in the data. When the data is accessed by the user a separate logger is created to keep track of the user and it is periodically sent to the data owner***.

Keywords: cloud computing, data sharing, jar, logger, steganography.

1. Introduction

Cloud is a collection of computers and servers that are publicly accessible via the Internet. In a world that sees new technological trends bloom and fade on almost a daily basis, one new trend promises more longevity this trend is called Cloud computing .Cloud computing portends a major change in how we store information and run applications. Cloud computing allows to access all the applications and documents from anywhere in the world, freeing user from the confines of the desktop and making it easier for group members in different location to collaborate. With Cloud computing, the software programs are not running from the personal computer, but rather they are stored on servers and accessed via the internet. This hardware is typically owned and operated by a third party on a consolidated basis in one or more data centres locations. The machine can run any combination of operating system;it's the processing power of the machine matter, not what their desktop look like.

1.1 Types of Service

Several technologies exist for cloud computing such as Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS).

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web servers.IaaS clouds often offer resources such as images in a virtual-machine image-library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

1.2 Types of Cloud

In cloud computing different types of deployment models are available, they are

a. Public cloud

Public cloud application, storage and some other resource are provided to the user by the service providerand these services can be either free or offered on a pay-per-use basis.

b. Private cloud

Private cloud is different from that of public cloud, in this type a separate cloud infrastructure is created for the organisation and it is managed internally or by a third-party.

c. Hybrid cloud

Hybrid cloud is the combination of two or more clouds (public and private)that remain unique entities but are bound together, providing the benefits of multiple deployment models.. Hybrid cloud architecture requires both on-site resources and off-site server based cloud infrastructure.

d. Community cloud

In community cloud the infrastructure is shared between several organizations from a specific community with common requirementswhich can be managed internally or by means of some third party. These are mainly used by the organization who need to work on group projects.

Since the data stored in the cloud can be accessed by some third partythe proposed system uses some of the security mechanism such as Steganography and jar conversion method to overcome the attack against the data stored in cloud.

2. Related Work

In [1] the authors proposed a new approach which can be used to track the user while accessing the source database and whenever copying occurs between the databases, where as in ordinary database it is very difficult to keep track of the user. In order to provide consistency between the databases

the data's should be written in high level cross points which can be used to identify the source.

The main aim of Elliptic Curve Cryptography is to simplify the key management system. As in [2] the Ecc is generally used in the wireless location instead of cryptographic method such as RSA. These systems can be executed with much smaller elements which provides greater benefits; such benefits are particularly needed in the wireless location where the memory and the battery power are limited. The Ecc is mainly used between two parties who need to exchange the data in secure manner.

The DanBoneh, et al. [3] describesidentity-based encryption scheme, which simplifies certificate exchange between the users in the e-mail system. For example when the mail transferred to the system it can encrypted using the public key and there is no need to obtain the certificate. The data is decrypted by the trusted third party and send to the user. It also reduces the cost and complexity of public key system compared to the traditional system.

Cloud computing is one of the rapidly growing technology that can be used to provide service to user at place and any time. Since the data stored in cloud can be accessed by many users at the same time it needs some scheduling mechanism, mainly the data size need to be reduced since the data stored in the cloud is pay per usage.

2.1 Drawbacks

- It does not provide any authentication or security to the user's data that is stored in the cloud.
- Not suitable for small and medium level storage users.
- User's data are processed in unknown machines.
- User may not have full control over the data.

3. Proposed Solution

The proposed solution overcomes the security issues in the cloud computing since the data that is sent from the client machine to the cloud is subjected to attack. Several security mechanism has been devised which can be used to maximize the security provided to the data. The novel approach of this method is to secure the file that is stored in the cloud by means of steganography. The method provides best defensive mechanism to detect and react against attack.

3.1 Data creation

The Data owner initially creates the data thatis to behidden in the image and archives them by means of Java Archive (JAR). It also simplifies certificate management systems. The jar file consists of two components the outer jar and the inner jar. The outer jar is used for authentication purpose and the inner jar contains the encrypted data, which is displayed to the user when the authentication succeeds.Once the file has been archived the jar file is stored in the cloud.

3.2 Data Access

The data can be accessed by any user based on the authentication; it also provides various kindsof service based up on the user. Whenever the data is accessed by the cloud service provider it is verified based up on OpenSSL trusted certificate authority, and the user is verified by the technique called SAML-based authentication, which issues certificates by verifying the user's identity based on his username.

Once the authentication succeeds, the cloud service provider or the user will be allowed to access the data enclosed in the JAR file. Based up on the configuration settings defined at the time of creation, the JAR will provide, data access or will provide only logging functionality.

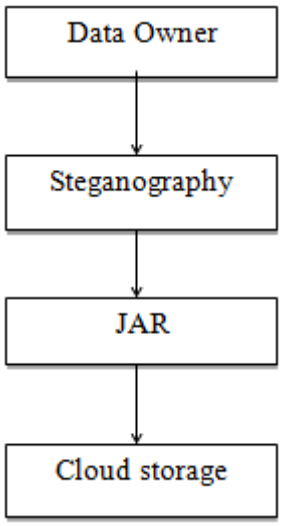

Figure 1. Overview of the cloud secure storage

3.3 Generation of Records

To overcome the attack against the data stored in cloud and to track the unauthorized user log records are generated automatically, whenever the data access occurs. The logs contain the name of the system, ip address, date, time and year. The log records are sent to the data owner periodically and it is dumped whenever the file size exceeds the limit.

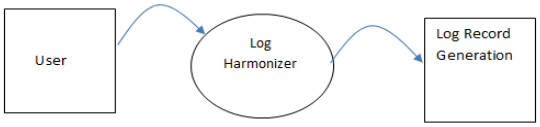

Figure 2. Log Record Generation

3.4 Types of Mode

In order to inform the user about their data usage the complementary method uses two kinds of auditing modes, such as push mode and pull mode.

The former method periodically sends the logs to the data owner or user, this action will be triggered whenever the time elapses for certain period based on the temporal timer inserted as a part of JAR file. It also ensures that the size of the log file does not exceed the limit specified by the data owner. This method is mainly used whenever there occurs a large number of accesses to data stored in the cloud.

The later method allows the data owner to retrieve the logs whenever needed; this method is mainly used to monitor the data usage that is stored in the cloud. The owner can retrieve the logs by means of FTP command using the command prompt.

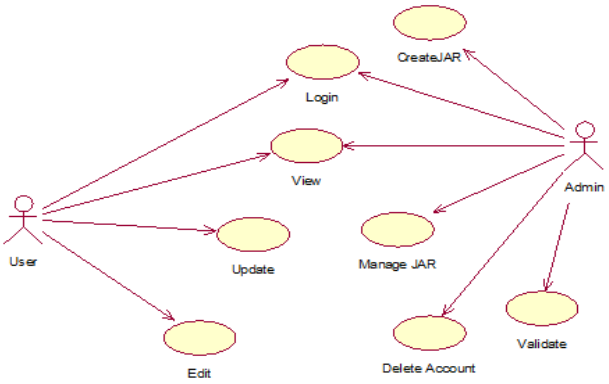

Figure 3. Use case diagram

Advantages

- It provides end-to end accountability in a highly distributed fashion.
- Uses Steganography and JAR compression technique to overcome the attack against the data stored in the cloud.
- It provides defence against man in middle attack, dictionary attack, Disassembling Attack, Compromised JVM Attack.
- Loggers are used to keep track the user

4. Conclusion and Future Work

Cloud computing is going to be the next big wave in computing. Even though it has many benefits, such as better hardware management, better and easier management of data since all the data is located on a central server and provides access to the data at time and anywhere, the major concern is security, Since the data stored in cloud is subjected to attack. To overcome the above problem this paper focus on the issues of security in the cloud computing. It enhances the security by hiding the data behind the image by means of steganography, which is then converted into JAR file and stored in the cloud. In future timing mechanism can be added so that the user can access the file only for the particular period of time specified by the owner of the data.

Acknowledgment

I express my sincere thanks to Ms. K. Varalakshmi, Assistant Professor and Dr. D. Malathi Head of the Department for providing guidance during the course of this work.

References

[1] P. Buneman,A. Chapman, and J. Cheney “Provenance Management in Curated Databases,” Proc. ACM SIGMOD Int’l Conf. Management of Data (SIGMOD ’06), pp. 539-550, 2006.

[2] Kristin lauter, Microsoft Corporation “The Advantages of Elliptic Curve Cryptography for Wireless Security” pp.1536-1284, 2004.

[3] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[4] Gilles Barthe, FedericoOlmedo, and Santiago ZanellaBeguelin” Verifiable Security of Boneh-Franklin Identity-Based Encryption”IMDEA Software Institute, Madrid, Spain pp.1-17.

[5] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Guptaand Manoj diwaka ” Effective Ways of Secure, Private and Trusted Cloud Computing”. Vol. 8, Issue 3, No. 2, May 2011 ISSN (Online): 1694-0814 pp.412-421.

[6] Gawali M. B., R. B. Wagh& S. P. Patil ”Enhancement for data security in cloud computing environment” Computer Engineering Dept., RCPIT , Shirpur, India, Computer Engineering Dept GECA, Aurangabad, India. ISSN No: 2231 – 6965, VOL- 1, ISS- 3 2012 pp.19-24.

[7] Trusted Java Virtual Machine IBM project, Available: http://www.almaden.ibm.com/cs/projects/jvm/, 2012. Visited on December, 2012.

[8] OASIS Security Services Technical Committee, “Security Assertion Markup Language (saml) 2.0,” Available: http://www.oasis-open.org/committees/tchome.php?wg abbrev=security, 2012. Visited on December, 2012.