Techniques for Securing the Data in Cloud Computing

Ms. Seema Kumari[1], Mr. Prakash Pathak[2], Ms. Ishita Madan[3]

[1] Research Scholar, CSE, MD University, Rohtak, Haryana, India
[23]Assistant Professor, CSE, WCTM, Gurugram

---***---

Abstract - *Cloud computing is visualized as the next-generation technology. It is an Internet based technology where quality services are provided to users including data and software, on remote servers .Cloud computing is also called Data outsourcing as a third party provides storage services to user. This is more cost effective for the user as there is no need of purchasing expensive hardware and software for data storage. Before data out sourcing can become possible, the data provider needs to guarantee that the data is secure, be able to make transactions, and the transactions must also be secure and not visible to the data provider. In this paper, we will discuss current techniques for securing client's data on remote cloud server.*

Key Words: Data Security, Cloud, integrity, confidentiality, outsourcing.

I. INTRODUCTION

Cloud computing denotes a major change in how we store information and run applications. Now Instead of running programs and data on an individual desktop computer, everything is hosted in the "cloud"—a shared pool of computers and servers accessed via the Internet. Cloud computing provides the facility to access all the documents and application from anywhere in the world and allows multiple group members to collaborate from different locations. One of the biggest feature of cloud computing which is widely used is Data storage capability. Several free and reliable online storage services available to the users are Microsoft SkyDrive, Apple iCloud ,Google Drive, Amazon S3, Dropbox and Gspace. As we get to know so many advantages of cloud computing but everything has some pros and cons both and cloud computing is not an exception. There are some doubts in users mind before moving towards cloud computing.

As the use of cloud computing becomes widespread, security of the outsourced user data becomes an important research topic.

The parameters that are taken into consideration for data security are Confidentiality, Integrity, and Availability. The problem of outsourcing data faces the following obstacles:

Confidentiality:- Can we trust some third party and share our private data with them? Does our data remain confidential over cloud? Though a service provider gives the guarantee of protecting the privacy of user data, the reality is that the data is physically located in some country and is subject to the local rules and regulations. Some of the countries allowed the vendor to access the user's Data according to their rules and Regulation. Under such circumstances it becomes crucial for the user to ensure the security of their data before putting the data over cloud.

Availability:-Does the data that we have stored on cloud would be available whenever we required it i.e. Availability of data. When user is fully relied on data stored at cloud storage, it becomes essential that it would be easily accessed.

Integrity:- The data outsourcing party must give guarantee to the user that the data that they have stored on cloud would not be modified or altered by any unauthorized user.

These are some doubts which come in the mind of every user or organization who wants to switch to cloud computing. In this paper, we will discuss some techniques used for providing security of data storage in cloud computing.

II. LITERATURE REVIEW

Many of the researches have been done till so far in which different security techniques have been discussed.

In [1], a data protection model was proposed where data is encrypted using Advanced Encryption Standard (AES) before launching in the cloud, which ensured data security. Data encryption is traditionally used to provide confidentiality while outsourcing data to cloud service provider. Hacigumus et al. [2] discusses a method for executing queries over encrypted data, at the cloud service provider's site and suggests splitting a query into two parts, namely the server query and client query. The server query is executed over the encrypted data at the service provider side and the other part over the result of server query, at the client side.

Hore et al. [3] describes techniques for building privacy preserving indices on sensitive attributes of a relational table, and provides an efficient solution for data bucketization.

Agrawal et al.[4] highlights the benefits of using the order preserving Encryption scheme(OPES) for querying numeric data.

Private Information Retrieval (PIR) was first discussed in [5]. PIR protocol hides the queries performed by the user on a public database, stored on a set of servers. The PIR protocol provides the privacy of user queries which tends to hide the user's intensions from the service provider.

After that a new protocol Symmetric Private Information Retrieval (SPIR) has been developed.

Its main concern was the privacy of user data.

One of the most widely used techniques for data outsourcing is Secret Sharing techniques. Shamir's Secret sharing [6] method and Rabin's Information Dispersal [7] Algorithm (IDA).

III. DISCUSSIONS

Problem statement

Two main challenges of cloud computing are security and reliability. Clients needs guarantee that their data which is stored on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available. Some of these techniques are:

Encryption: In this technique complex algorithm are used to hide the original information with the help of encryption key. The data is converted into unreadable form called cipher text and then stored on remote server storage.

Authentication processes: In this process, a login mechanism is used to verify that the only authenticated user is accessing the cloud data. It requires creating a user name and password.

Authorization practices: A list of Authorized client is used to identify, who can access data stored on cloud system.

However, many people still worry that data saved on a remote storage system could be accessed by other clients and they will alter it. . Hackers could also attempt to steal the physical machines on which data are stored. An employee from cloud service provider could alter or destroy data using his or her authenticated user name and password. Instead of all these risks, clients are adopting cloud computing widely. Cloud storage companies are investing a lot of money to make sure that their clients data would be safe. They are trying to limit the possibility of data theft or corruption.

We are discussing some techniques here that are helping how to get security on cloud storage and for different clients by reading the different research paper. In this article we look at the Trusted Platform Module (TPM). TPM provides confidentiality and integrity in clouds. Kerberos is a technique which is used to authenticate the users and SLA Proof for retrieving written serializability, and freshness in clouds.

IV. A TRUSTED STORAGE SYSTEM FOR THE CLOUD

"A Trusted Storage System "store the data as well as it needs confidential storing also and maintain the integrity of the data.

To achieve confidentiality and integrity of the data, cryptographic techniques can be used to encrypt data

To encrypt the client's data within the cloud, Encrypted file systems (EFS) is used .In EFS user's data is encrypted with the help of encryption key which changed the original data into cipher text which is unreadable for other users. It develops the Integrity of the data within the cloud. Five protocols are developed which ensure that the client's data is stored only on trusted storage servers, Data is copied only on trusted storage servers, and guarantee that the data owners and other privileged users of that data access the data securely. The system is based on trusted computing platform technology [8].

A. Encrypted File Systems

EFS (Encrypted File System) meant for encrypting stored files. Encryption procedures occur at the file system level not at the application level. Encryption is transparent to the user. Cryptographic techniques are used for encryption; hence user doesn't need to manage keys in encryption. Below diagram shows the process of

Encryption using EFS:

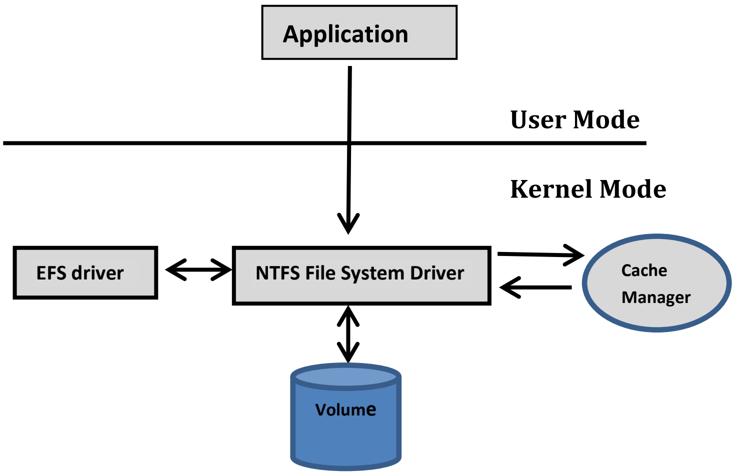

Figure 1: Example of flow of an encryption process in an Encrypting File system

Process explanatory steps are as follows.

1. Application writes data to an encrypted file
2. NTFS places data in file system cache.
3. Cache manager writes data to disk via NTFS.
4. NTFS ask EFS driver to encrypt file contents headed to disk.
5. NTFS writes encrypted file contents to disk.

B. Trusted Platform Module

What is a TPM?

The Trusted Platform Module (TPM) is a computer microchip or a microcontroller which performs various task related to security and cryptography. This technology provides the tools to authenticate the computer platform. The tools or objects can include certificates, encryption keys, passwords, and integrity metrics of a platform. The TPM can be used in the process of remote attestation of a platform of a machine which will be discussed further later. The chip is installed on the motherboard of a computer. The TPM communicates with the rest of the system by using a hardware bus. The TPM implementation of that specification as a chip. The specification is provided by the Trusted Computing Group [10].

Result of Trusted Storage system: TPM model provide security for system administrative level. But there is no solution for individual users because cloud is maintained by third party on network. By using this proposed system, administration can achieve confidentiality and integrity of the data stored only on trusted storage server.

V. ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH EFFECT OF KERBEROS

This technology ensure cloud storage security with the help of Kerberos authentication service. That is by implementing the Kerberos; storage security would be achieved for users. Kerberos is defined for creating the ticket and granting ticket for each user. This technology focuses more on user to provide better security. [9].

Kerberos operation

Kerberos uses the technique of strong encryption method and complex ticket granting algorithm [9] so that user can be authenticated on network. In this a session key is used which allow encrypted data stream over an IP network for each user. If new user wants to use the cloud then he should make profile on network by providing the information. After registering with Kerberos, the user will get his user ID and password which will also store on server Database.

Each user must follow following steps for using cloud data:

- Log on to system by using user ID and password.
- User will send the request for ticket granting ticket to the Authentication Server.
- Authentication server verifies user's credential in database; create the ticket and session key. Results are encrypted using key derived from user password.
- User will send the request cloud service granting ticket to Ticket Granting server.
- TGS will send the Ticket and session key to the user.
- Workstation sends ticket and authenticator to cloud server provider.
- Server verifies ticket and authenticator match, if verified, and then grant access to service.

VI. ENABLING SECURITY IN CLOUD STORAGE SLAs WITH CLOUD PROOF

One more technique for cloud storage security is based on "Enabling Security in Cloud Storage SLAs with Cloud Proof"

This presents a secure storage system specifically designed for cloud, named as Cloud proof. In cloud proof customers can detect if the integrity of data is violated, violation of write-serializability, and freshness. They can also prove these violations to a third party [13].

System Overview of cloud proof:

Cloud Proof has the following four goals.

Goal 1: Customers should know if service provider has violated the integrity of data, freshness, and write-serializability. User's data must be confidential from outsiders. It can be achieved by encrypting the data they store on the cloud.

Goal 2: Customers should be able to prove cloud violations whenever they happen.

Goal 3: Cloud Proof should provide read and write access control in a scalable way. Since we are dealing with enterprise sizes, there may be thousands of users, many groups, and terabytes of data. We want to remove data owners from the data access path as much as possible for performance reasons. Owners should be able to rely (in a verifiable way) on the cloud for key distribution and access control, which is a highly challenging task.

Goal 4: Cloud Proof should maintain the performance, scalability, and availability of cloud services despite adding security.

The overhead should be acceptable compared to the cloud service without security, and concurrency should be maintained.

The system should scale to large amounts of data, many users per group, since this is demanded by large enterprise data owners.

VII. CONCLUSION

In this discussion we found various techniques provide the security for data stored on cloud. In this paper we demonstrate how we can achieve confidentiality and integrity security by using EFS and TPM techniques. Kerberos proofs the authentication of users on network. SLAs with Cloud Proof build confidentiality, integrity, write-serializability and read freshness (denoted by C, I, W, F). Providing privacy to customer and his data on cloud is very complex and cost effective system but it can be achieved by different technologies we have discussed in this paper.

REFERENCES

[1] Abha Sachdev, Mohit Bhansali "Enhancing cloud computing security using AES Algorithm" International Journal of Computer Applications(0975-8887) Volume 67-No.9,April 2013

[2] H. Hacigumus, B.R.Iyer, C.Li and S. Mehrotra, "Executing SQL over encrypted data in the database service provider model," in proc of the ACM SIGMOD Conf., 2002.

[3] B.Hore, S.Mehrotra, and G.Tsudik," A privacy preserving index for range queries,"in Proc. Of the VLDB Conf., 2004,Pp. 720-731.

[4] R.Agrawal, J.kiernan, R.Srikant, and Y.Xu,"Order preserving index for range queries," in Proc. Of the ACM SIGMOD Conf.,2004,pp.563-574.

[5] Chor, B. Goldreich, O., Kushilevitz, E., Sudan, M.:Private information retrieval In: Journal of the ACM,vol.45,no.6,PP.965-982(1998).

[6]Shamir,A.: How to share a secret.In:Commun.ACM,vol.22,no.11,PP.612-613(1979)

[7] Rabin,M.O.:Efficient dispersal of information for security, load balancing, and fault tolerance. In: journal of the ACM 36(2),PP.335-348(1989)

[8] http://www.tar.hu/wininternals/ch12lev1sec8.html

[9] Mehdi Hojabri,' Ensuring data storage security in cloud computing with effect of Kerberos',Vol. 1 Issue 5 , July - 2012 ISSN: 2278- 01 81

[10]Raluca Ada Popa, Jacob R.Lorch, David Molnar, Helen.J.Wang,Li .Jhuang :Enabling Security in Cloud Storage SLAs with cloudProof.