Information Security in Cloud

Divisha manral[1], Jasmine Dalal[1], Kavya Goel[1]

[1]Department of Information Technology, Guru Gobind Singh Indraprastha University

E-Mail- divishamanral@gmail.com

ABSTRACT-With the advent of the internet, security became a major concern where every piece of information was vulnerable to a number of threats. Cloud is kind of centralized database where many clients store, retrieve and possibly modify data. Cloud computing is environment which enables convenient and efficient access to a shared pool of configurable computing resources. However the data stored and retrieved in such a way may not be fully trustworthy. The range of study encompasses an intricate research on various information security technologies and proposal of an efficient system for ensuring information security in cloud computing platforms. Information security has become critical to not only personal computers but also corporate organizations and government agencies, given organizations these days rely extensively on cloud for collaboration. Aim is to develop a secure system by encryption mechanisms that allow a client's data to be transformed into unintelligible data for transmission.

Keywords – Cloud, Symmetric Key, Data storage, Data retrieval, Decryption, Encryption, security

I. INTRODUCTION

Information Security is nothing but to protect the database from destructive forces, actions of unauthorized users and to guard the information from malicious modification, leakage, loss or disruption. The world is becoming more interconnected with the advent of the Internet and new networking technology. Information security [1] is becoming of great importance because of intellectual property that can be easily acquired. There have been numerous cases of breaches in security resulting in the leakage or unauthorized access of information worth a fortune. In order to keep the information system free from threats, analysts employ both network and data security technologies.

Cloud computing is a model which provides a wide range of applications under different topologies and every topology derives some new specialized protocols. This promising technology is literally called Cloud Data Security. It is the next generation computing platforms that provide dynamic resource pools, virtualization and high availability.

II. INFORMATION SECURITY TECHNOLOGY

A. ENCRYPTION

In cryptography [2] encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key, which adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys. There are two basic types of encryption schemes: Symmetric-key and public-key encryption [3].

B. SYMMETRIC-KEY CRYPTOGRAPHY

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption

avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.

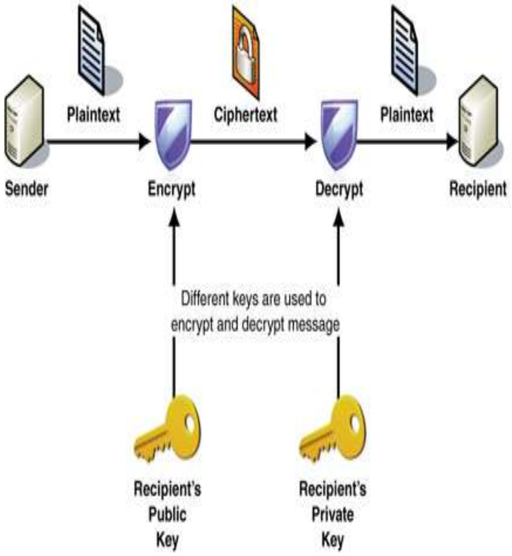

Figure 1: Cryptography Model using Symmetric Key

C. HARDWARE BASED MECHANISM

Hardware based or assisted computer security offers an alternative to software-only computer security. Devices such as dongles may be considered more secure due to the physical access required in order to be compromised. Working of hardware based security: A hardware device allows a user to login, logout and to set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read both by a computer and controllers in peripheral devices such as hard disks.

D. DATA ERASURE

Data erasure is the process of permanently erasing data from disk media. It is not the same as file deletion. File deletion and removal of the Volume Table of Contents (VTOC) simply erases the “pointers” to the data stored on the media so the data is not viewable in directories. It does not physically erase the data from the media. Many firms physically destroy hard drives or use various software utilities to “erase” data using these methodologies. However, these solutions are inadequate and can potentially lead to data breaches, public disclosure and, ultimately, unplanned expenses as described above.

E. DATA MASKING

Data masking technology provides data security by replacing sensitive information with a non-sensitive proxy, but doing so in such a way that the copy looks – and acts – like the original. This means non-sensitive data can be used in business processes without changing the supporting applications or data storage facilities. You remove the risk without breaking the business! In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis. In other cases, masking will dynamically provide masked content if a user's request for sensitive information is deemed 'risky'.

III. CLOUD

For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in hard drives. Others prefer external storage devices like pen drives or compact discs. Desperate computer owners might delete entire folders worth of old files in order to make space for new information. But some are choosing to rely on a growing trend: cloud storage. Cloud computing encompasses a large number of computers connected through a real-time communication network such as the Internet. It is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access.

A. CLOUD STORAGE

A basic cloud storage system needs just one data server connected to the Internet. A client sends copies of files over the Internet to the data server, which then records the information. When the client wishes to retrieve the information, he accesses the data server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself. Cloud storage systems generally rely on hundreds of data servers. Because computers occasionally require maintenance or repair, it's important to store the same information on multiple machines. This is called redundancy. Without redundancy, a cloud storage system couldn't ensure clients that they could access their information at any given time. Most systems store the same data on servers that use different power supplies. That way, clients can access their data even if one power supply fails. [4]

B. ADVANTAGES

Efficient storage and collaboration

Easy Information Sharing

Highly reliable and redundant

Widespread availability

Inexpensive

C. DISADVANTAGES

Possible downtime

Security issues Internet [5]

Compatibility
Unpredicted costs
Internet Dependency

IV.PROPOSED SYSTEM

Information security is the most important criterion for any data owner, as the data stored on the cloud will be accessible not only to him but to many other cloud users. The following proposed system provides a secure yet flexible information security mechanism which can be implemented easily at the time of data storage as well as data retrieval over the cloud. The concept of symmetric key is being used where only the data owner, the data retriever and the third party auditor will be having the access to the keys. Also double encryption will be used to make the system more secure.

A. DATA STORAGE

The proposed system for data storage is flexible as the encryption algorithms used will be of the choice of the user. The model constitutes two major stages.

The first stage starts when the data owner uploads the data to the center. The owner will be asked to choose from a list of available algorithms (Encryption Algorithm 1) or upload his own algorithm to encrypt the data. This will lead to the creation of cipher text along with the primary key (Key 1). The final step of the first stage will be the transferring of the cipher text on to the cloud.

The second stage starts with the encryption of the Key 1, where again the data owner is asked to choose from list t of available algorithms (Encryption Algorithm 2) or upload his own algorithm to encrypt the key and create the secondary key (Key 2). Then the center shares the Key 2 with the third party auditor for future verification. The auditor can verify the data, and keep track of the shared keys only. [6]

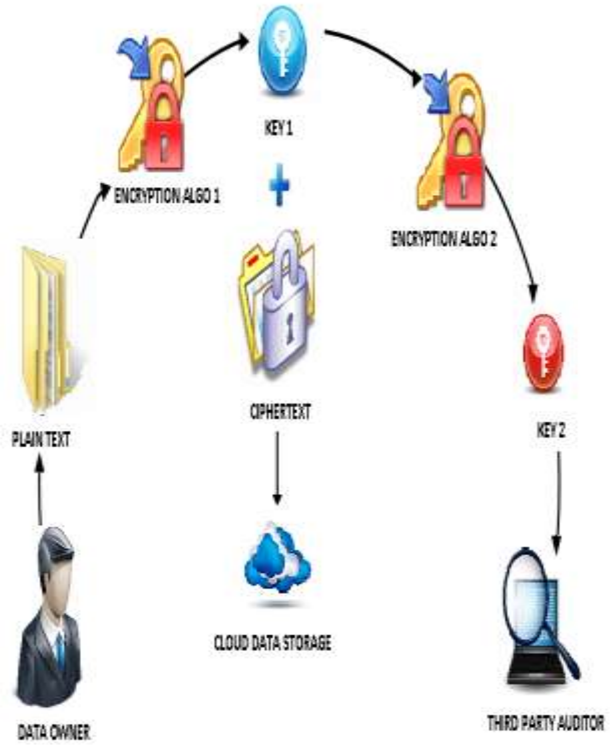

Figure 2: Proposed Data Storage Model

B. *DATA RETRIVAL*

The data retrieval poses a bigger problem than the data storage in cloud computing.

In this proposed model the data retriever has to take data access permission from the data owner by sending in a data access request. If the request is accepted by the data owner, he sends the secondary key (Key 2) and the information for further decryption i.e. which all decryption algorithms are to be used for further decrypting and retrieving the final plain text.

The data retriever sends a data request to the Third party auditor. The Auditor verifies the key send by the retriever with the database present with him, if the keys match it will allow to take the cipher text from the cloud data storage.

The information given by the data owner to the retriever helps in decrypting key 2 into key 1 using the decryption algorithm 2. With key 1 in hand the cipher text can be decrypted using decryption algorithm 1 into the final plain text, which can be used by the retriever.

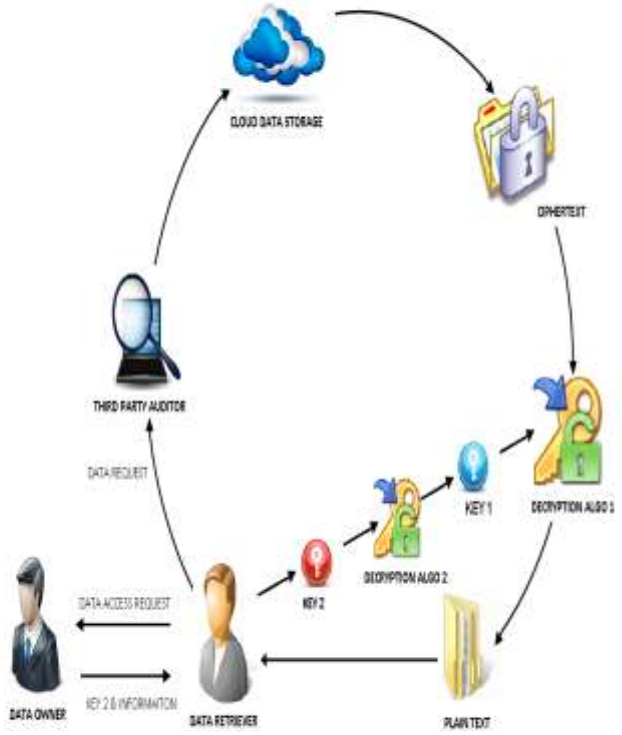

Figure 3: Proposed Data Retrieval Model

B. BENEFITS

The proposed model in this paper is highly secured because of the use of double encryption technique. The secondary key can be accessed by data owner, data retriever and the third party auditor, but this only gives access to the cipher text and hence even the third party auditor also doesn't have direct access to the data. No one can use the data unless he has been given the information by the data owner about decrypting the secondary key into the primary key and further using it to again access to the plain text.

The proposed model is flexible since the model does not hold any constraints on the use of cryptography algorithms; the data owner will be allowed to choose from a list of algorithms or given a choice to use his own algorithm for the encryption process.

The proposed model uses symmetric key cryptography technique; symmetric key is faster than asymmetric encryption algorithm. The model encrypts plain text easily and produces cipher text with less time.

The data is stored as cipher text in the cloud. So even if the attacker hacks into the cloud system and gains access to the data stored there, he cannot decrypt it and use it further. Hence making data stored in the cloud more secure and less vulnerable to threats.

V. CONCLUSION

Cloud computing is one of the most booming technology in

world right now. But this technology is facing many data security threats and challenges. With the help of the proposed system which incorporates the use of Double key encryption technique and symmetric cryptography algorithm, one can manage to keep their data securely in the cloud. It would provide high level speed and security in cloud environment. The proposed system aims to achieve goals like confidentiality, data integrity and authentication in a simple manner without compromising on security issues.

REFERENCES:

[1] Aceituno, V, Information Security Paradigms, ISSA Journal, September, 2005.

[2] Gold Reich, Oded, Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.

[3] Bellare Mihir, Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements, Springer Berlin Heidelberg, 2000, Page 1.

[4] Herminder Singh & Babul Bansal, Analysis of Security Issues And Performance Enhancement In Cloud Computing" International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 345-349, July-December 2010

[5] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility

[6] Snsha Vijayaraghavan, K.Kiruthiga, B.Pattatharasi and S.Sathiskumar, Map-Reduce Function For Cloud Data Storage and Data Integrity Auditing By Trusted TPA, International Journal of Communications and Engineering, Vol 05,No 5,Issues 03,pp 26-32,March 2012