Vol. 6, Issue. 1, 2019, ISSN 2349-0780

Enhanced Data Security Approach for Cloud Computing

Pankaj Gehaloach, Rohit Mahajan
Department of Computer Science and Engineering, Golden College of Engineering and Technology, Gurdaspur, Punjab, India

Abstract: In the innovation of technologies, cloud computing plays a vital part as an architecture of IT Enterprise. As compared to traditional computing services, Cloud computing has been moved the application software and databases to the large data centres. Multiple advantages of cloud computing has attracted the individual as well as IT to adopt it but there are some issues which degrades the user services. Sometimes, users are not able to fearlessly upload their confidential data to cloud due to some security flaws like data security, leakage, privacy, confidentiality and integrity.

To solve this problem, we proposed a highly-secured model which provide security before uploading and during downloading the data. Data is encrypted, dual authenticated and access management techniques has been applied in first phase of proposed model i.e. data uploading. While in second phase i.e. during data downloading, HMAC algorithm and decryption has been applied which makes the proposed model more reliable and secure.

Index Terms: *Cloud Computing, Data Security, Encryption, Decryption, HMAC*

Introduction

Cloud based storage is the emerging trend in the area of computing because it provides ubiquitous, appropriate, and on-demand accesses to bulky data shared over the Internet. An individual as well as IT has attracted to cloud based storage due to its several benefits, including lower cost, greater agility, and better resource utilization. Even though cloud storage has lot of benefits cloud users, providers and third party associated with cloud are always concerned about the security of their confidential data

In this paper, we focus on major issue of security of data in cloud and as a solution we proposed a model which provide the solution to this issue. When user upload their confidential data in cloud, the cloud service provider doesn't provide full control on it. Sometimes the replicate the data into another server to avoid the loss of data during server failure. Thus, it leads to fear of losing and stealing of data in user's mind which stops user for adopting of cloud storage.

To make data more secure and trustworthy upload in cloud, we proposed a highly-secured model. The main purpose of this model to provide security of data from individual aspects i.e. before uploading and during downloading the data to cloud.

The rest of this paper is organised as follow: section 2 represents the related work in the field of cloud security. Section 3 represents the architecture of the proposed model. Conclusion and future work are drawn in section4.

Related Work

A lot of work has been done already in the area of cloud security. Numerous models and techniques are proposed for cloud security.

Jingwei [1] studied the problem of integrity auditing and secure deduplication on cloud data. Their work aimed at achieving both data integrity and deduplication in cloud and proposed two secure systems i.e. SecCloud and SecCloud+An auditing entity with a maintenance of a MapReduce cloud was introduced in SecCloud which helps clients to generate data tags before uploading. SecCloud+ was designed to motivate by the fact that customers always want to encrypt their data before uploading, and enabled integrity auditing and secure deduplication on encrypted data.

Hong Liu et al [2] proposed a shared authority based privacy-preserving authentication protocol i.e. SAPA to address privacy issue for cloud storage. In this technique, shared access authority was achieved by anonymous access request matching mechanism with security and privacy parameters. Attribute based access control was

adopted to realize that the user can only access its own data fields and at last proxy re-encryption was applied by the cloud server to provide data sharing among the multiple users.

Chang Liu et al[3] presented a novel public auditing scheme named MuR-DPA. The proposed scheme incorporated a novel authenticated data structure based on the Merkle hash tree (MHT). Rank and level values in computation of MHT nodes was included to support full dynamic data updates and authentication of block indices

Louai A. Maghrabi[4] reviewed the literature that focuses on the expert's findings and interpretations of data security issues and threats over the Cloud. Author points out seven security threats: abuse and nefarious use of Cloud Computing, insecure Application Programming Interfaces (APIs), malicious insiders, shared technology vulnerabilities, data loss or leakage, account or service hijacking, and unknown risk profile.

M. Sugumaran et. al. [5] discussed about some of the techniques that were implemented to protect data and proposed an architecture to protect data in cloud. The proposed architecture was developed to store data in cloud in encrypted data format using cryptography technique which is based on block cipher.

Baojiang et. al.[6] proposed the novel concept of key aggregate searchable encryption i.e. KASE and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents.

Cong Wang et. al.[7] proposed a privacy-preserving public auditing system for data storage security in Cloud Computing. They utilized the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content that is stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage.

XiaoChun et. al. [8], proposed a scheme to securely store and access of data via internet. They used ECC based PKI for certificate procedure because the use of ECC significantly reduces the computation cost, message size and transmission overhead over RSA based PKI as 160-bit key size in ECC provides comparable security with 024-bit key in RSA. They designed Secured Cloud Storage Framework (SCSF) in which users not only can securely store and access data in cloud but also can share data with multiple users through the unsecure internet in a secured way.

Zhongma et. al.[9], proposed a secure way for key distribution without any secure communication channels and the users can surely obtain their private keys from group manager. Proposed scheme achieved fine-grained access control, any user in the group can use the source in cloud and revoked user cannot access the cloud again after they are revoked. The proposed scheme also protect the cloud data from collision attack.

III. PROPOSED MODEL

Proposed model is highly based on Key management policies which further divided into two parts i.e. key generation and key Storage. The outcome of model is extremely productive in terms of security of data i.e. data remains private even if it is outsourced. To maintain data

- Phase I (Encryption & Uploading)
- Phase II (Downloading & Decryption)

3.1 Phase I- Encryption & Uploading: - It is also known as data storage and uploading phase. In this phase, third party is responsible for generation of keys and further keys are divided into key pieces. Owner keeps his key piece for encryption and decryption.

Before uploading the data to cloud, data is encrypted to maintain the data privacy. In proposed model, encryption on data is performed by owner with its key piece and he further give the encrypted data to third party and after that third party perform re-encryption of data with its own key pieces and uploading to cloud.

Once the data encryption is done, HMAC i.e. hash-based message authentication code is calculated to avoid data tempering. Owner will encrypt HMAC and re-encrypted HMAC, by third party, will uploaded along with data to cloud. HMAC is one of the components in a protocol that provides integrity.

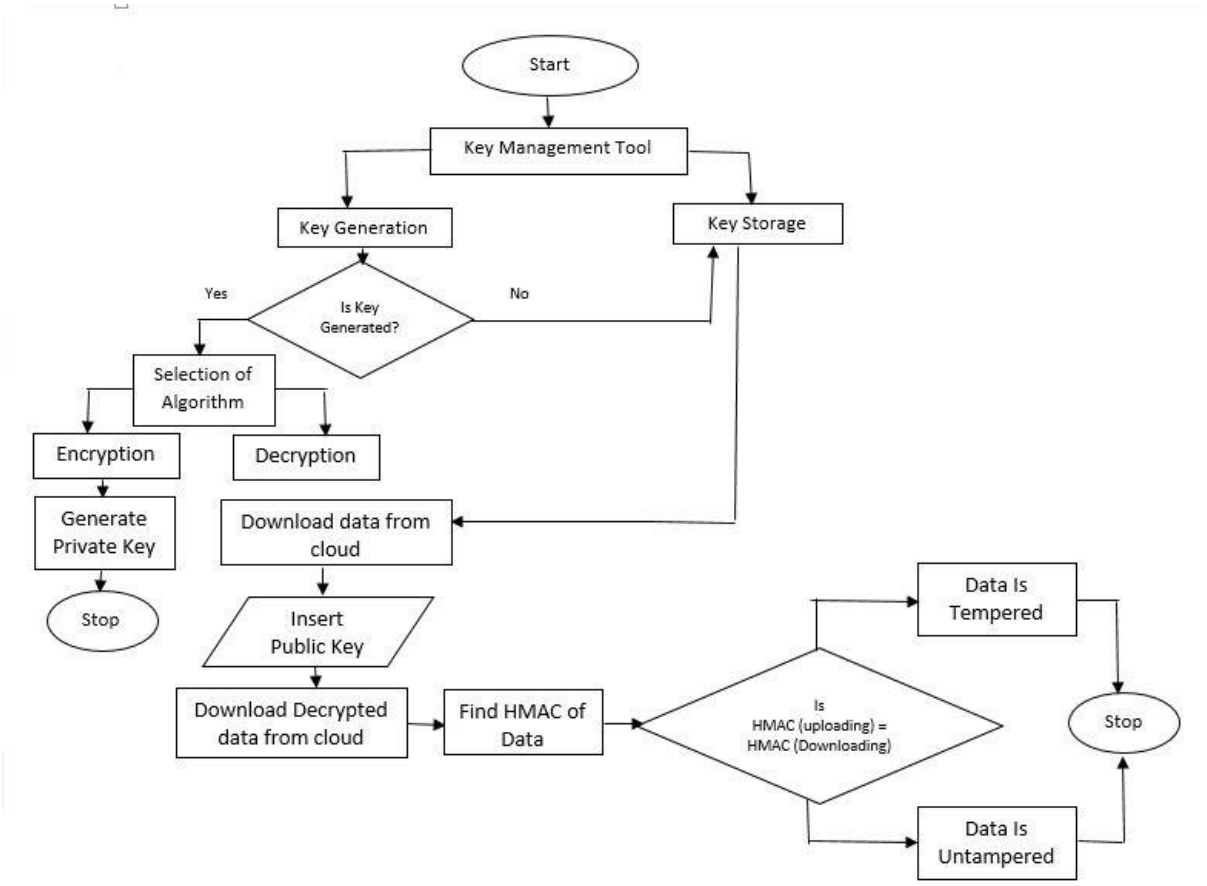

Figure 1.Phases of Data Encryption & Uploading to Cloud

.

3.2 Phase II-Downloading & Decryption

3.2.1 User Level Authentication & Data Integrity: -

In proposed model, only authorised users will have privileges to download data from cloud. User will get identity-based access to encrypted data on successful login to cloud.

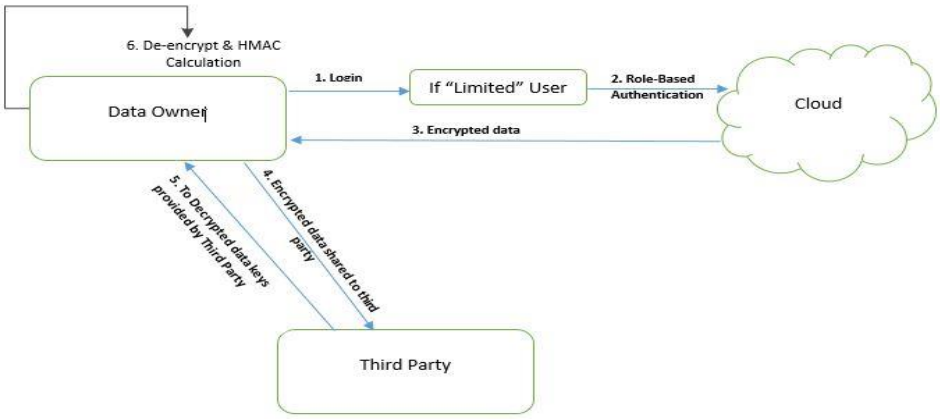

Figure 2: Phases and check Data Integrity

Once the encrypted data is downloaded from cloud, third party will decrypt the same with its key piece. Now the encrypted data will be passed to user. Then user or data owner will decrypt the data & generate the HMAC of data to check the data integrity. Data integrity holds only if HMAC before uploading the data to cloud equals HMAC after downloading data.

$$\text{HMAC(uploading)} = \text{HMAC(Downloading)} \longrightarrow \text{Data is un-tampered}$$

Figure 3: Data Integrity.

IV. SECURITY ANALYSIS

Proposed model is secure from all threats like unauthorized access, tampering of data, confidentiality, privacy which can prevail and harm the data. It provides security when data at rest as well as during transmission. Security analysis of model has been performed on below mentioned parameters.

- Data Confidentiality: In the proposed model, re-encryption technique has been designed for data secrecy. Data encryption is done by two authorities i.e. data owner & third party.
- Data Privacy: data privacy has been maintained in whole methodology as only the authorised users will have aces to upload/download of data
- Overhead: As the proposed model is owner centric so all the overhead will on data owner but this model has been proposed such that data owner overhead should be less because of use of third party.
- Data Integrity: Hash Based Message Authentication Code is used to maintain the data integrity.
- User Authentication: to prevent data from unauthorised access, identity-based user authentication is used in proposed model.
- Availability: According to SLA certification of cloud service provider the data will be available 24*7. The data can be access anytime from anywhere.
- External Attack: External Attack can be from untrusted parties like third party or cloud service provider or network intruder. The data is safe as it is in encrypted format throughout different the phases of model.

IV. EXPERIMENTAL RESULTS

The proposed model has been assessed with execution. This model has been verified using OpenSSL tool [17] in red hat Linux and own Cloud [18]. Figure 4 illustrates that after execution various security parameters i.e. Key Management, HMAC and dual user authentication. HMAC provides less data security than user roles and this User roles provide less security than Key Management technique. Basically, if we combine all security parameters i.e. HMAC, user roles, key management, dual user authentication, it results in highly secured data owner centric approach for uploading data to cloud. It results in highly secured proposed model used in various cloud environment which is designated as peak value as shown in figure.

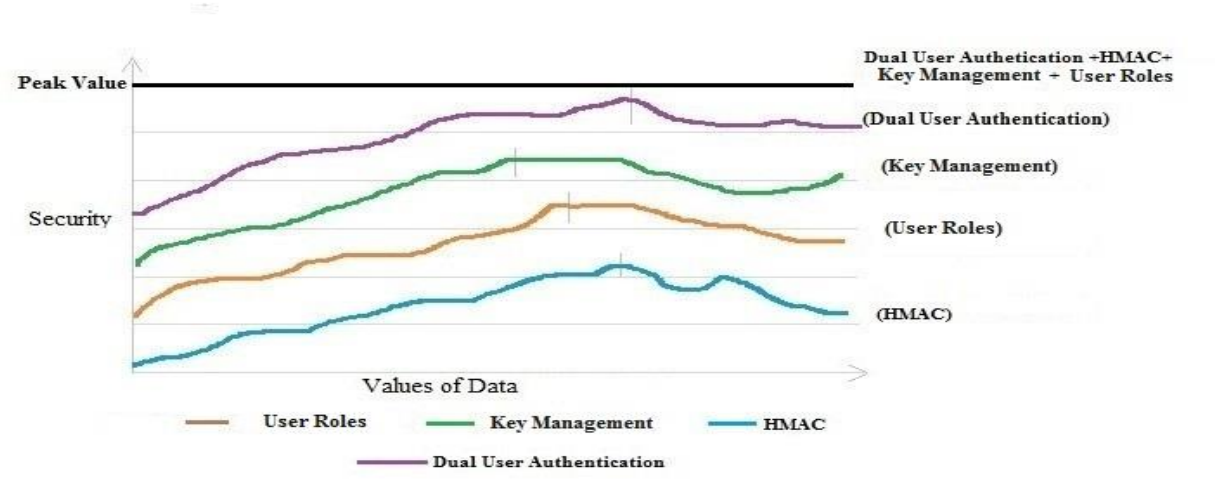

Figure 4. Security Evaluation

V. CONCLUSION & FUTURE SCOPE

Recent trend in cloud computing illustrations that data security is main issue which has been obstacle for adopting the cloud. To resolve this issue, security model has been proposed which is secure enough to use in cloud for storing data. Proposed model is divided into two phases i.e. Encryption & uploading and downloading & decryption. Data remains private and not disclose to unauthorized access during these two phases. The proposed model is data owner centric and highly secure to adopt in real life.

Although the model is tenable but in imminent we will try to enhance on more security parameter in order to make model more secure and efficient. We will authenticate the model by applying it to higher and realistic projects.

REFERNCES

1. Jingwei Li et al "Secure Auditing and Deduplicating Data in Cloud", IEEE Transactions on Computers, DOI 10.1109/TC.2015.2389960.
2. Hong Liu et al, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, DOI 10.1109/TPDS.2014.2308218
3. Chang Liu et al, " MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud", IEEE Transactions on Computers, DOI 10.1109/TC.2014.2375190
4. Louai A. Maghrabi, "The Threats of Data Security over the Cloud as Perceived by Experts and University Students", IEEE 2014
5. M. Sugumaran et. al., "An Architecture for Data Security in Cloud Computing", 2014 World Congress on Computing and Communication Technologies.
6. Baojiang et. al.," Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE transactions on computers, VOL. 6, NO. 1, JANUARY 2014
7. Cong Wang et. al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM 2010

8. XiaoChun et. al., "An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI",ICACT 2014.

9. Zhongma et. al.," A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems,2015