DATA SECURITY APPROACH BASED ON HMAC ALGORITHM FOR CLOUD ENVIRONMENT

Supreet  
Department of Computer Science and Engineering  
Global Institute of Management & Emerging Technologies, Amritsar, India

Dr. Vinay Chopra  
Assistant Professor  
Department of Computer Science  
D.A.V.I.E.T, Jallandhar, India

ABSTRACT

Cloud Computing looks as a computational hypothesis as well as dissemination architecture. Cloud security is a multi-layered and highly problematic issue. In cloud computing stages, resources need to be dynamically re-configured and accumulated over virtualization and customers’ desires can hypothetically vary over time and improvements need to be accommodated. The Major issues are data security, data confidentiality, data leakage, data privacy, and data integrity. According to security issues users are not able to confidently upload their data to cloud. To solve this problem we proposed a model which is highly secure and is based on data owner centric model i.e. data is under control of data owner. Encryption, Obfuscation, HMAC and Dual authentication and access management technique has been used which make the proposed model more reliable and effective to use it in real world.

INDEX TERMS—Cloud Computing, Data Security, Encryption, Obfuscation, HMAC.

I. INTRODUCTION

Cloud is a computing environment based on network, where the users get various resources as per requirement and repealed after the completion of user task. Cloud is used for saving clients data to a storage system also called remote database, where connection is provided by the internet between user computer and the remote database. The Cloud provides unlimited and configurable resources to end user which may be in the form of storage space, memory, processing time, application software, processing power, etc. Cloud computing can be used by various users of multifaceted scales ranging from a single user to big organizations.

A number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, Virtualization and other technologies with reliance to the Internet are used to satisfy the computing needs of users and common business applications through web browsers are provided, while the server stores their data and software. There are three types of Cloud Environments: Public, Private and Hybrid Clouds. In Public cloud, applications are run externally by large service providers and various benefits are offered over private clouds. Private cloud is an architecture that provides hosted services to various users behind a firewall. Hybrid cloud is an environment which is provided by a company or large organizations. The combination of private and public clouds is also known as Hybrid cloud.

Cloud provides large storage for data and high computing speed to customers over the Internet. It shifts the data and application software to the big data stores i.e. cloud, where data is managed and services cannot be fully trustworthy. This is the main reason that many companies avoid using cloud even cloud computing provides a large range of facilities and luxuries. Security in cloud is a scalable and highly complex issue.

In cloud computing model, there are three functional units which revolves around it. They are as follows:

1.) Cloud Service Provider: Cloud Service Provider manages Cloud Storage Server (CSS) and it has significant storage space to store the user’s data and has high computation power.

2.) Client/Owner: Client is an entity with large data files which has to stores in the cloud and depends on cloud for the maintenance of data and computation of data. Client or owner can be an individual or organizations.

3.) User: User is a unit in which the owner is being registered and uses the owner’s data which is stored on the cloud. The user can be the owner itself.

When user store their data at cloud they have no direct control over data, even they don’t know where data is residing even could service provider untrusted sometime. So fear of losing and stealing of data remain in user mind which stops user for adoption of cloud. To make users comfortable with cloud model
has been proposed. The main role in this model is data owner. As data owner can take care of data better than anyone else. With the adoption of this model user can fearlessly keep data at cloud.

Section II discusses the related work done in the field of data security in cloud. Section III desirable the proposed model Section IV and V provides the security analysis and experimental results respectively. Section VI we conclude with our work.

II. RELATED WORK

There are many research work carried on related to data security in cloud computing. Numerous model, techniques and schemes are proposed for fearlessly uploading the data to cloud.

Sandeep K. Sood et al. [3] proposed framework is divided into two phases in which one phase deals with mechanisms and methods to store and secure the data from beginning and transmitting insecurely to the cloud in encrypted form. It is further divided into subsections (Classification, Index Building and encryption, Message Authentication Code (MAC) and another phase Firstly the retrieval of data requires the user to register him with the owner/organization by getting a username and a password. The user will register to get its username and password at organization, which will further forward the username to cloud to let it store the username into its directory. Thus, his proposed technique provides a way to protect the data, check the integrity and authentication by following the best possible industry mechanisms. Unfortunately, there will be high overhead on data owner and hence time consuming is too. Danan Thilakanatha et al. [4] proposed scheme using proxy re-encryption for security of data. In this scheme data owner encrypt the data using his key piece then proxy encrypt the data using his key piece. Decryption is also carried in similar fashion. However, if proxy is fake then data becomes in secure. P. vara lakshmi et al. [5] represent of three entities cloud broker, client and cloud storage. Broker handles encryption, hash key, decryption and local data base management. According to cloud space available the client files are partitioned in to segment and hash values of segments has been generated. When the client need sits file its ends request to broker then broker download the file, partition the file in to segments and then calculate the hash values. For checking the data integrity hash values before uploading to the after downloading are matched. If this matches data is un-tampered. Sandeep k. sood et al. [6] they provided improved data security by using concept of hybrid cloud. In this scheme the sensitive data i.e., about 3%-5% is stored at private cloud and rest of the data at public cloud. This model is applicable to organizations whose sensitive data is about 3%-5%. If the sensitive data increases then this model will prove to be expensive. His paper proposes a hybrid cloud computing model which handles both external as well as internal data security threats and using both private as well as public cloud in its architecture. A dual layer of security is used in his model, one is authentication based on username and password and the other, the condition that the user should possess the key to decrypt a password stored at the cloud, without which the password filled by the user and the password stored cannot be compared.

In this Proposed model data is protected against all threats i.e. internal and external, threat during, transits as well as when data at rest.

III. PROPOSED MODEL

Proposed model is based on main responsibility of data owner towards data protection at cloud. For data security, encryption and obfuscation technique is used which protect the data during transits as well as at rest. During transit of data, Data integrity plays vital role so for data integrity hash based message authentication. Code is calculated on encrypted data in order to have minimum overhead over data owner. So third party is involved.

The proposed model is divided into two categories i.e.

*Phase-1 (uploading)*

*Phase-2 (downloading)*

And involved four entities that is - data owner, CSP, third party and user.

3.1 Phase-1 (Uploading)

3.1.1 Key Generation and maintenance

In this model third party acts as key management infrastructure for key generation and storage. The third party generates the symmetric key and gives the key to data owner for further process. Data owner divide the key into key pieces. Owner keeps its one key piece for encryption and other key piece for corresponding user id for future use. Data owner encrypt these two keys by passcode and then sends to the third party. These key pieces are kept with third party and taken when needed.
3.1.2 Classification of data

The data can be of two types i.e. type 0 and type 1:
- Type 1: when the data is of alpha numeric type
- Type 0: when the data is of numeric type

3.1.3 Encipher and Indexing

Based on classification of data, corresponding encipher technique is used. Data owner identifies the type of data. If data is of type 1 then encryption is used otherwise obfuscation is used. Before these techniques, indexing is performed. After indexing as well as data applied according to technique are uploaded to cloud.

3.2.4 Data Integrity

Before data is uploaded to cloud, hash based message authentication code HMAC is generated in order to check data privacy during transit of data to cloud. After generation of HMAC, it is also in the same way encrypted as that of data and uploaded to cloud.

Figure 3.3. HMAC Generation for Data Integrity

3.2 Phase 2: Downloading

3.2.1 Dual Authentication and Access Management:

In this proposed model, data is secured against unauthorized user. For authentication, data owner shares its user database with cloud. Authenticated user login to cloud and get role based access to data. To decrypt the data user goes to data owner. First data owner verify the user using digital signature and pass user id detail to third party. Now, user is redirected to third party. Third party verifies the user id and gives corresponding key piece to user for data decryption.

Figure 3.4 Dual User Authentication

3.2.2 HMAC verification

For data integrity, the HMAC is regenerated by user and matched with HMAC before data uploaded to cloud i.e.

HMAC (Uploading) = HMAC (downloading)

If both HMAC are same then data is not tempered but if not same user report to data owner.

40
IV. SECURITY ANALYSIS

An enhanced data security model has been proposed so as to use in various cloud environment for uploading data without the fear of being lost or theft. This model has been designed in a manner that data remain private and secured throughout the entire process of cloud computing. There have been many models proposed in this field but they lack in some way for providing security. The comparison has been made between existing model and proposed model as shown in the table below.

Table 1 Functionality comparison

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Generation and Maintenance</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Division Of Key Into Two Parts</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrity/ Block Code</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Identifying Data</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Obliteration</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual User Authentication</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Digital Signature Verification</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Stored User Data Security And Password</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Identity Type Of Data</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Role Based Access</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The comparison shows that proposed model tries to deal with all the possible data security issues of cloud computing. The table represents that all the security issues in cloud computing are overcome by the proposed model. The proposed model is highly based on data owner centric approach i.e. data owner has full control on data irrespective of location. In this model data is protected against all the parties involved in cloud computing process i.e. third party, cloud service provider, user and network intruder.

V. EXPERIMENTAL RESULTS

The proposed model has been evaluated with implementation. This model has been verified using OpenSSL tool [17] in red hat Linux and ownCloud[18]. Figure 5 shows that after implementation various security parameters i.e. Encryption/Decryption Complexity, classification of data, HMAC and dual user authentication, Key Management and User Role. The graphs shows that Role of the user in security increases with increase in values of data but it has less security then key management. While Key management also provides less data security than User Roles and dual user Authentication. In dual user authentication perform good role in has less impact on security as compare to key management. securing the data, security of data increases with respect to values of data, but after some point it started degrading. But classification of data plays better role in security of data, as classification of data can depict that which data should be more secured.

HMAC has better performance in securing the data, but it is less secure than the encryption and decryption complexity.

In other hand Encryption/decryption complexity makes data more secure than any other technique and factor. It is highly secure than key management, dual user authentication, classification of data and HMAC. Basically if we combine all security parameters i.e Encryption/Decryption Complexity, classification of data, HMAC and dual user authentication, Key Management and User Role, 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 denoted as peak value as shown in figure.

Figure 5 Security Evaluation

VI. CONCLUSION & FUTURE SCOPE

Recent trend in cloud computing shows that data security is major issue which has been an obstacle for adopting the cloud. To overcome this issue, model has been proposed. The model is highly secure and protects the data during transit as well as data at rest. It also secures the data against all threats i.e. insight as well as out sight. It helps the user to fearlessly upload the data at cloud without any hesitation of data being lost or steeled.

Although the model is secured but in future we will try to add on more security parameter so as to make model more secure and efficient. We will validate the model by implementing it to larger and realistic projects.
REFERENCES


[18]https://www.openssl.org/

[19]https://owncloud.org/