Secure Online Data Encryption in Cloud Computing

Nipa Sarkar[1], Sheeba P[2]
Department of Computer Science[1,2], New Horizon College of Engineering[1,2]
Bangalore-560103, Karnataka, India
Email: nipas94@gmail.*com*[1], sheebaravindra87@gmail.com[2]

Abstract- Step by step it is getting to be vital and achievable to utilize distributed cloud storage because of its secure, adaptable administrations. As the total number of clients who are embracing cloud information administrations is increasing rapidly various security issues are arising. In such situation accessible security of the Providers providing Cloud Service administrations can appear to be lacking to guard client's information. Client level security component improves safety and security for accessing the cloud and gains client's belief in embracing the cloud information administrations. Our proposed framework deals with the execution of encryption related to online information component utilized at client level. This framework handles the data and encrypts selected data during uploading it to cloud storage environment. During the period of transferring of data, mixing-up of the information takes place and then it is transferred it to distributed storage. The process of secure online encryption of data and information fastens the procedure and spares client's opportunity. A data security procedure is utilized in which client's ID and login information is used. For data decryption process a cipher key, is introduced to cloud. With the assistance of salt and one-time secret keyword Decryption method is performed. Client is not involved in storing the key and administration responsibility. Progressed and strongly secured innovation of storing information in cloud system are offered to the Holders. This paper discusses about various encryption techniques and their implementation involved in online data storage in cloud computing and also the investigation of results acquired.

Index Terms- Cloud data security; online data encryption; decryption; distributed storage.

1. INTRODUCTION

Now a days cloud computing is widely used emerging techniques which is mainly used to enable convenient, efficient, on-demand network admission to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) [6]. Cloud computing can be launched with minimal management effort of carrier issuer interaction and unexpectedly provisioned. Five most important fundamental points of Cloud structure are- i) self-service on request, ii) rapid access of network, iii) resource pooling, iv) fast elasticity, v) measured amenity. According to the official National Institute of Standards and Technology (NIST) models of cloud service are of three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [1]. Cloud proposes four types of models involved with the deployment process. These are: i) private, ii) public, iii) hybrid and iv) community. Cloud computing architecture consist of five most important parts: i) cloud consumer, ii) cloud provider, iii) cloud carrier, iv) cloud auditor and v) cloud broker. Each part is an entity. Each part can be a person or an organization that participates in the cloud computing or performs various tasks in cloud computing. Five main Actors in NIST cloud computing reference architecture is described below:

Cloud consumer- A person or organization that manages a business relationship and also maintains users service from cloud providers.

Cloud provider- A person, organization, or an entity who has the authority for making a service accessible to interested parties.

Cloud auditor- A party which is eligible to conduct independent valuation of cloud services, performance and security of the cloud application.

Cloud broker- An entity that manages the usage, overall performance and distribution of a various number of cloud services, and exchanges relationship between cloud provider companies and cloud customers.

Cloud carrier- An intermediate party that delivers connectivity and conveyance of cloud services from cloud providers to cloud customers.

The total number of Users involved in accessing cloud facilities have progressively increased and it has triggered new types of security challenges and complex security issues. These threats are to be glimpsed immediately to achieve a best result in accessing the cloud. “Treacherous 12” was published by Cloud Security Alliance (CSA) in January 2016. This report reveals the top 12 threats involved in cloud computing that the organizations are going to face from 2016.

Too many security complications are arising day by day. So, various essential solutions have to be performed to solve these issues. Moreover, user must have their own security technique along with the amenities of Cloud Service Provider's (CSP's) security mechanism to endure against susceptible circumstances which is arising from period to period in cloud computing technology.

2. LITERATURE SURVEY

Security threats and challenges in cloud computing environment is changing very hastily. Various companies like Amazon, Google, IBM, Microsoft have boosted up their growth in cloud computing technology field. They have introduced various reliable structures which are widely used to enlighten offered services to provide user friendly storage features to users under cloud computing technique. Still the users are not convinced enough to implement cloud computing system as there is no assurance of guaranteed security and privacy techniques to handle sensitive data. Because it is incapable of assuring durable security when data privacy and data integrity is taken into consideration. Cloud security service features such as AWS, CipherCloud, CSA is discussed below with literature.

Amazon Web Services (AWS) was officially launched on March, 2006. AWS offers a secure on demand cloud computing platform. It is highly flexible and based on paid subscription method. Users can form a structure of extensive variety of applications. AWS guard the confidentiality, integrity, and individuality of the client's systems. AWS propose many security resolutions like secure log-in, identity and access controlling, data prevention and protection and so on. User can use any of AWS product on basis of pay per use which is based on hourly or monthly or yearly subscription. Users receives their own (BYOL) key options which acts as a license key. AWS key management system(KMS) delivers facilities in which encryption of data and hardware security components plays a vital role to guard safety of the encryption keys. Gemalto's SafeNet Protect V permits customers to keep a track of the generated encryption keys. It safeguards sensitive data present in EC2 and EBS volumes. SafeNet Protect V permits the client to personalize data and generated encryption keys for better security purposes. [10,11,14].

CipherCloud was introduced in 2010 to deliver security of cloud services in the form of SecaaS (Security as a Service). It helps to protect the data under cloud environment and improves the visibility of cloud data. CipherCloud offers cloud system with guaranteed security and service-control. CipherCloud offers SecaaS which is widely used for the applications in Economic Services, various Technologies, hospital systems & Life Sciences, Administration, Telecom services, and many more. CipherCloud structure includes various applications which secures multiple cloud applications, examples are Chatter, Force.com, Gmail, Office 365, Amazon AWS and various others. By using CipherCloud's framework Users can preserve their information privately on the public cloud model. CipherCloud acts as an Encryption Gateway by authorizing various companies to encrypt delicate information by using the email in the cloud. User have to choose an algorithm to encrypt data and securing the email content as per the protection is concerned. The AES-256 encryption algorithm is widely used to provide robust encryption mechanism in cloud environment. CipherCloud is the only provider which provides encryption of email under cloud system by keeping registry of the key within the user's currently working company [9]. By any chance, If the company loses user's key data, the user is not a valid member to access data form the cloud by using CipherCloud.

The Cloud Security Alliance (CSA) was started in 2008. CSA proposals includes cloud security explicitly in investigation, teaching, accreditation, actions and products of commercial and discrete associates. CSA's wide-ranging investigation package deals with industry, advanced education and administration on worldwide foundation. SecaaS and CSA associates together to form a group to distribute security facilities to cloud technology. CSA also delivers strong security to- IaaS, PaaS, SaaS cloud models. CSA consist of Cryptography tools along with key management service, commonly known as KMS. It is rapidly used to protect the sensitive data in contrast to unauthorized user's access. Encryption algorithms like AES, RSA etc are executed with the help of CSA. Identity-Based encryption practices are also done by CSA. To maintain trust and integrity Digital signature techniques plays a significant role.

Multi-tier structure of authentication process is discussed here which follows authentication based on two-tier structure. This structure offers improved security and distributes user confidentiality protection. Availability of data is a major concern than data privacy protection. Data excruciating and duplicating at various places is projected in the proposed structure. In this paper we have discussed partially and completely unidentified attribute-oriented regulator structure to introduce user confidentiality failures within cloud storing system. This structure is consisting of three layers- 1) Access control layer 2) Intrusion detection and prevention layer 3) Encryption layer. Proposed framework has combined hardware and software features in its construction. User's current location is detected and verified for encrypting the file. During decryption, the current location of the user is used as main key component to fetch the data. By using this technique, user does not need to store key with them. This method frees the system from any jeopardy of data integrity and unauthorized access.

3. ENCRYPTION MECHANISM

By following the two encryption techniques user can upload any type of data to cloud:

- Offline encryption
- Online encryption

In the Offline encryption technique, user or the client picks the files which is to be uploaded and transferred from local storage to the cloud storage. Once the selection of file is done encryption takes place. User or client takes the help of online amenities to upload encrypted file in cloud storage. Whereas in the Online encryption procedure client is allowed to complete the file encryption process and uploading the file data parallelly. In the Offline encryption technique user unreasonably becomes tangled in an extended procedure whereas Online encryption scheme manages user's data accessing time. So, we have utilized second procedure which is online encryption technique. In this encryption method Containers or buckets are utilized for data storage under cloud environment which enhances to obtain improved security.

User or client selects a particular file or data which has to get uploaded in the cloud. The authentication is carried out successfully by using knowledge factor authentication process. Once the selection of file is done by the user, the particular file gets encrypted and simultaneously gets uploaded to cloud storage. Salt and UDIC token obtained from user are combined together to form cipherkey. Obtained cipherkey is mainly formed for the entire encryption process. Usually key registry is stored in local storage of the user but no registry is maintained for the above-mentioned process. By forming this, insider attack risks arisen. In our proposed structure we have detached the necessity of keeping the key with client. Therefore, there exist no jeopardy of revealing keys and finally no risk of losing personal data.

During data retrieval process user has to login successfully into authenticated account. Only after successful authentication process user can select the file for downloading which is in the encrypted form. Once CSP receives a request of data retrieval an OTP is sent on user's registered email-id. Received OTP is entered by the user for verification and then decryption of data is carried out. Complete Decryption process takes place at user's location itself. Once file is downloaded, it is still in the encrypted format. This file gets stored in user's system and Only after providing exact OTP which is received through the email, user becomes permissible for decrypting file and gains random access to it. Therefore, OTP plays an important role to provide security to safeguard data.

Because of shared feature of cloud computing several Security Threats are arising.

To resist cloud related issues, a strong mechanism is considered at two stages which are:

• Cloud service provider level- These are the safety techniques followed by CSPs.

• User level- Security approaches and resolutions used by various individuals are categorized as user level mechanisms.

User level refers to a single individual user or a community. It may also be a company. The security mechanism at the user level is considered as an added exertion to keep user's data protected. This mechanism works with CSP's security services to provide data security and data integrity. The proposed system in this paper is a user level mechanism which offers data protection along with CSP's security system.

Various security threats considered in this system are listed below:

• Data breaches: Existence of data breaches occurs because Cloud maintains massive quantity of data and data users. Data breaches cause severe disaster as it gets exposed to user's monetary, fitness and assets data. Data breaches extract and transfer the sensitive personal information to the intruder even though various measures involving lawsuits and criminal charges are taken. It also disturbs the commercial aspects of the client and affects service provider's business- [6]. Data breaches may not be stopped entirely but a resolution can be used to safeguard user's data. Our system offers a four-layer security architecture which maintains the safety of the user's data by providing security even if data breaches happen in cloud atmosphere.

• Compromised credentials and broken authentication: In a single-tier verification structure, weak password leads to data breaches. Key management system (KMS) contains very sensitive data associated with user's authorizations. So, a poor Key management system provides open access to unauthorized users. Multiple authentication process provides solution to this risk. In our proposed system data encryption key is not stored anywhere. So, it is free from the risk of conceding credentials.

• Malicious insiders: By insider threat all information can get hacked and so, the system retrieving CSP facilities is at high risk. In our proposed scheme KMS is not essential. Hence malicious insiders threat is unsuccessful in this case.

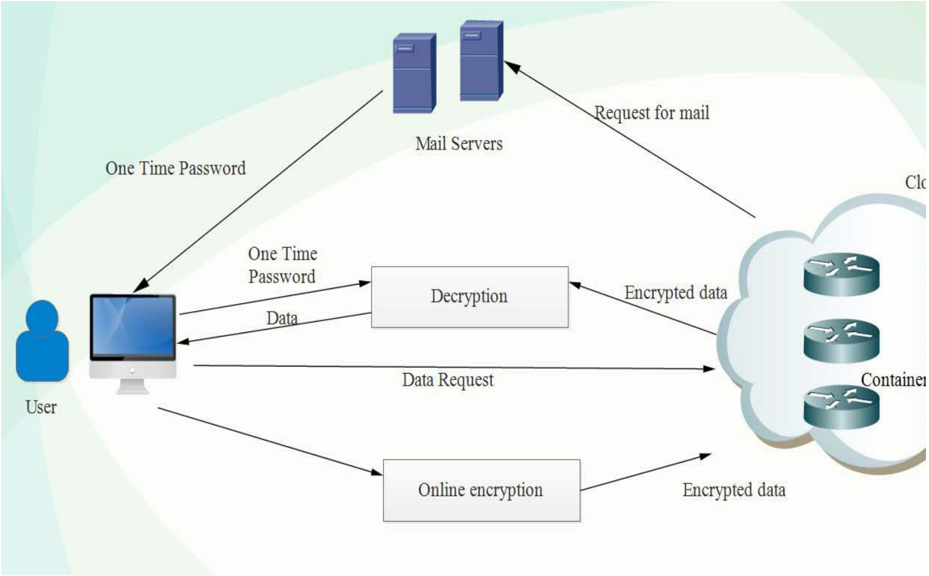


Figure. 1 General flow of online data encryption [1]

4. PROPOSED FEATURES OF THE SYSTEM

4.1. *KMS free:*

Any type of secret keys is not stored in our proposed structure during the complete execution process. Therefore, key storage system against insider attacks gets unusable here.

4.2. *Online data encryption:*

By using this method total time needed to upload data in cloud storage has reduced. User completes data uploading by following two methods: 1) Encrypting data locally by following user's encryption technique 2) Uploading encrypted data to cloud using CSP. In our proposed structure user is permitted to complete these two different methods as one single job. In this structure user just need to choose a folder for uploading and delivering the security authorizations. Remaining techniques of procedure is completed by the online encryption mechanism structure. Two dissimilar jobs are carried out at the same time for reducing the performance time of the system.

4.3. *Four-layer security of data:*

Data access controlling and privacy protection are the major significant concepts in cloud computing as data is stored within public cloud location. In our system information is protected in our proposed system by means of four-layer security architecture discussed below:

- ➢ In built security mechanism of cloud data services: It consists of various in-built security features of Microsoft Azure Emulator service.
- ➢ One Time Password (OTP): This authorizes legitimate user decrypting downloaded file by feeding into OTP received on user's mail-id. OTP performs an important role of generating the decryption key. It guarantees user for valid data authorization.
- ➢ Generation of Two-layered encryption key: This layer consists of two different sub layers to produce data encryption key.
- ➢ Salt and UDIC: Encryption key is generated by Using these two constraints. It makes system to sustain against various attacks and unauthorised access.

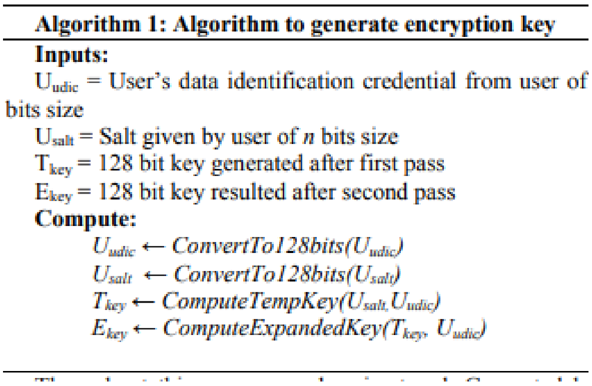
5. SYSTEM DETAILS

The system we are instigating here is secure online data encryption technique. Data is encrypted at user location and uploaded to cloud storage system during uploading. Online encryption mechanism of data fastens this procedure and saves time during data uploading by the user. A robust data security procedure is used to provide improved data access control. Here, user's data identification(UDI) credential and salt is used to carry out each step successfully.

Our proposed structure attempts to resolve various threats including breaches of data, negotiated identifications and fragmented verification, malicious insiders and offers review support. This system accomplishes several purposes like validating operator, producing secret key of encryption mechanism, connected encryption and decryption process, inspecting data and so on. Authentication is a foremost important component in any safety structure. In log-in validation process user need to input login id and secret key using previous knowledge factor. Once login is successful, user is permitted to accomplish several actions on information like data uploading, data fetching and downloading, executing inspection on data and various others. User may have several sorts of organized structured and unstructured data records. In our structure containers or data buckets are utilized to store data in the cloud system. Containers have in-build safekeeping structure offered as added security features to store information within cloud computing environment. Encryption mechanism includes two-layer key generation techniques. Generated key of first layer is the input of second layer. The finally obtained generated resultant key of the two layers is utilized as encryption process.

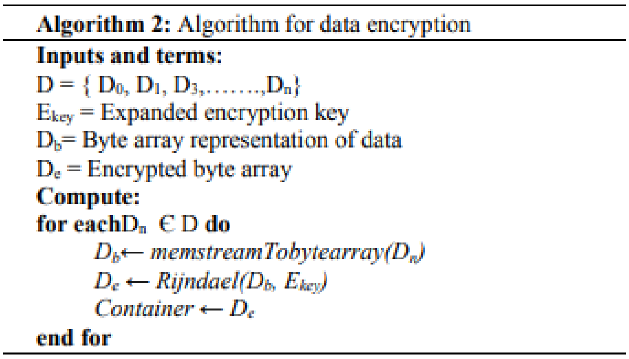
3 algorithms are used in this concept which are discussed below:

1. Algorithm to produce encryption key
2. Algorithm for data encryption
3. Algorithm for data decryption



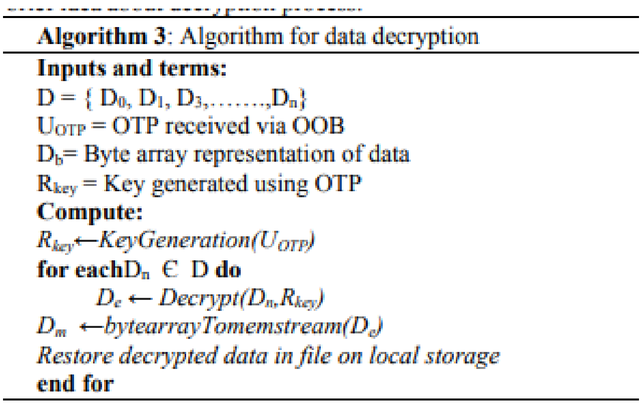
```
Algorithm 1: Algorithm to generate encryption key
Inputs:
$U_{udic}$ = User's data identification credential from user of bits size
$U_{salt}$ = Salt given by user of n bits size
$T_{key}$ = 128 bit key generated after first pass
$E_{key}$ = 128 bit key resulted after second pass
Compute:
    $U_{udic} \leftarrow ConvertTo128bits(U_{udic})$
    $U_{salt} \leftarrow ConvertTo128bits(U_{salt})$
    $T_{key} \leftarrow ComputeTempKey(U_{salt}, U_{udic})$
    $E_{key} \leftarrow ComputeExpandedKey(T_{key}, U_{udic})$
```

1. By using this algorithm an encryption key is generated during the uploading of data. This algorithm breaks the data into blocks and each block is encrypted by unique key E_{key} generated by the system [1]



```
Algorithm 2: Algorithm for data encryption
Inputs and terms:
D = { $D_0$, $D_1$, $D_3$,.......,$D_n$}
$E_{key}$ = Expanded encryption key
$D_b$= Byte array representation of data
$D_e$ = Encrypted byte array
Compute:
for each$D_n$ € D do
    $D_b \leftarrow memstreamTobytearray(D_n)$
    $D_e \leftarrow Rijndael(D_b, E_{key})$
    $Container \leftarrow D_e$
end for
```

2. This algorithm helps in encrypting data and providing security when the data is getting uploaded to the cloud [1].



```
Algorithm 3: Algorithm for data decryption
Inputs and terms:
D = { $D_0$, $D_1$, $D_3$,.......,$D_n$}
$U_{OTP}$ = OTP received via OOB
$D_b$= Byte array representation of data
$R_{key}$ = Key generated using OTP
Compute:
$R_{key} \leftarrow KeyGeneration(U_{OTP})$
for each$D_n$ € D do
    $D_e \leftarrow Decrypt(D_n, R_{key})$
$D_m \leftarrow bytearrayTomemstream(D_e)$
Restore decrypted data in file on local storage
end for
```

3. By using this algorithm user can decrypt the data whcich is to be downloaded from the cloud [1].

Specifically, these three algorithms are used because these are very secure and takes less time for encryption and decryption compared to all other algorithms.

6. CONCLUSION

The secure online encryption technique consumes less of the user's time for accessing the data stored in cloud system. The four-layer security techniques discussed above facilitates access control of data and protects data privacy which are most challenging in the cloud storage environment. By using UDIC token and salt security structure privacy of data is maintained. Data is still safe even if data breaches or broken authentication occur. Moreover, this system uses containers for data storage in cloud which is free from key storage and management. Using this technique makes this system further more secure. In case even if the user's data identification credentials is hacked it will not be useful since decryption key has to be produced by two components. The outsourcing of incomplete key enables user's information possession more translucent and intensifies user's faith in cloud storage facilities and cloud computing technologies.

REFERENCES

[1] Rajani S. Sajjan, Vijay R. Ghorpade," Inside cloudcomputing: Exploring threats and risks", second International conference on current trends and challenges in management, engineering, computer application and technology, ICCTCMECAT-2012

[2] Submitted to Asia Pacific University College of Technology and Innovation (UCTI)

[3] Submitted to University of Technology, Sydney

[4] www.vyomtech.com

[5] www.ijetae.com

[6] www.dtic.mil

[7] www.rroij.com

[8] Docker, "Modern application architecture for the enterprise", January 21, 2016

[9] "Introduction to Microsoft Azure Storage", http://azure.microsoft.com/enin/documentation/articles/storageintroduction

[10] "Protecting data and privacy in the cloud", Microsoft 2014

[11] "Secure the AWS cloud with SafeNet solutions ebook", Gemalto 2016

[12] "The 10-minute guide to securing email in the cloud", www.ciphercloud.com

[13] "Global cloud data security report Q1: The authority on how to protect data in the cloud", CipherCloud 2015

[14] Ashish Singh, Kakali Chatterji," A secure multi-tier authentication scheme in cloud computing environment", International Conference on Circuit, Power and Computing Technologies(ICCPCT) IEEE 2015