IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 58-62
www.iosrjournals.org

Secure Data Sharing Using Cryptography in Cloud Environment

Anjali Patel[1], Nimisha Patel[2], Dr. Hiren Patel[3]
[1]*PG Student, Computer Engineering Department, S.P. College of Engineering, Visnagar, Gujarat, India,*
[2]*Phd Scholar ,Rai University, Ahmadabad, Associate Professor, Computer Engineering, S.P. College of Engineering, Visnagar, Gujarat, India,*
[3]*Professor, Computer Engineering Department, S.P. College of Engineering, Visnagar, Gujarat, India,*

Abstract : *Cloud computing is rapidly growing due to the provisioning of elastic, flexible, and on-demand storage and computing services for users. In cloud based storage concept, data owner does not have full control over own data because data controlled by the third party called cloud service providers (CSP). Data security is challenging problem when data owner shares own data to another known as data sharer on cloud. Many researchers have addressed this issue by cryptography with different encryption schemes that provides secure data sharing on cloud. Here, we propose system model for secure data sharing on cloud with intension to provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption by users, support dynamically changes of users membership, owner not be always online when the user wants to access the data.*

Keywords: *Cloud Computing, Data security, Cloud Service Providers (CSP), Secure Sharing, Cryptography, Access control*

I. Introduction

The National institute of standard and technology(NIST) that defines the, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service), three service models (SaaS, PaaS, IaaS), and four deployment models (Public, Private, Hybrid, Community). [1]

Organizations use the high storage and computing services within own budget without investing in infrastructure and maintenance for required services but using that services provided by cloud users losses the control over on data and computing take place on cloud that raises data security issues for organizations, thwarting the wide adaptability of the public cloud. [2]

So, the loss of control over own data on storage platform provided by cloud motivates cloud customers to maintain the access control over own data. Security of data is more concerns when sharing (individual data or data shared among a group of users) of data is take place on cloud.

The rest of this paper is organized as follows. Section 2 presents the background theory. Section 3 presents the related work done towards secure sharing with cryptography techniques on cloud. Section 4 presents our proposed system model for secure data sharing on cloud and in section 5 conclusion is shown.

II. Background Theory

For sharing data on cloud main three entities that are involved is data owner who want to share own data to another person is known as data sharer and cloud service provider (CSP) that provides storage, computational facilities related to data. Here, CSP is untrusted third party which provides data storage facilities, computational facilities. So, it is necessary requirements of cloud users to not disclose original credentials to CSP.

For making data share securely on the Cloud, the data owner want to share data is first encrypted then store encrypted on the Cloud after owner send encryption key to sharers to whom with he want to share data. Using encryption key sharers decrypt the shared data put on cloud by owner. [9] This way of sharing data on cloud guarantees confidentiality of data, but the problem with this is that the key management between all the communicating parties to whom with share data is cumbersome. In some situation system users with poor computing capabilities devices becomes a bottleneck.

Here shows the overview of some of the dominant methods used for secure data exchange.

1. Public Key/Asymmetric encryption in public key encryption each users have own private and public key. sender encrypt the own data by the using own private key and receiver receivers that original data by decrypt received data using sender public key which provides authentication of sender on that data and for

provides data confidentiality sender encrypt the own data by the using receiver public key and receiver receivers that original data by decrypt received data using own private key.

2. Private Key/Symmetric encryption.
   In private key encryption both sender and receiver use the same key for file encryption and decryption respectively.
3. Proxy re-encryption
   Proxy re-encryption scheme that enable re-encryption of some ciphertext encrypted by one user such that another user will be able to decrypt it , which is useful when some user wants to forward some encrypted data to another user without the need of key forwarding.[3]
4. Identity Based encryption (IBE)
   IBE sender can encrypt a message using only identity without need of public key certificate. In IBE, ones publicly known identity (ex. email address) is being used as his/her public key where as corresponding private key is generated from the known identity.[7]
5. Attribute Based encryption (ABE)
   Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of a ciphertext is possible only if the set of attributes associated at receivers key are match with the attributes associated at the ciphertext.[4]

So, for secure sharing data on cloud requirements to be considered is explain below:

1. Data confidentiality: Any cloud service provides or unauthorized users not able to learn any credentials in the encrypted data files.[2]
2. Fine-grained access control: For users in the same group or different groups, each user can be associated with different access rights which will make the scheme more reliable and efficient as a real life solution. [8]
3. Scalability: The system should efficiently work even though numbers of authorized system user increases. [3]
4. User revocation: System must be able to denied access the shared data for revoked user and it should be work properly without affect other user's services or no need to change the encryption key.[3]
5. User rejoin: It refers capability that revoked user to include back in the system without affect other user's services or no need to change the encryption key.[3]

So, in this paper we will propose system model for secure data sharing on cloud with this objectives,

- Provides data confidentiality and access control on share data.
- Removes the burden of encrypt/decrypt files by users.
- Key management and exchange with sharers by owner.
- Owner online is not necessary when the sharers wants to access the share data and,
- Not disclose any original credentials of users to CSP.

III. Related Work

Md Mozammil et al.[5]: The mobile device is used for uploading, downloading and sharing of data but it has limited capacity of computation. so, when mobile user want to share own mobile device data to another on cloud by secure way can follow the proposed solution by this researchers where data owner encrypts the data using blowfish algorithm which is fast and required small amount of memory which is suitable for mobile devices and sends it to cloud storage. The data owner sends email of encrypted file to the sharer then privately provide secret key to the data sharer. Sharer decrypt the file received in mail using secret key and get the original data.

Uma et al. [6]: In Cloud computing, maintain data confidentiality, authentication and integrity is main problem when data sharing take place with another person on cloud. so, as per proposed solution by researchers message digest of plain text is signed by owner with RSA algorithm and plaintext message is encrypted by the public key of recipient. Recipient will decrypt the cipher text to plaintext with his private key, and from that compute the message digest code ,which is compare with the singed message digest code by owner if both are identical then signature is valid and data say data share securely. This technique solves the problem of data confidentiality, authentication and integrity.

Mazhar et al. [2]: For share data in group on cloud access control of user, forward and backward secrecy problem is comes which is solved by researchers. They have proposed SeDaSC methodology by introducing CS (cryptographic server), encryption/decryption operations are performed at the CS which is a trusted party in the SeDaSC. When user want to upload/ download the shared file on cloud comes along with own secret key provided by CS and CS will takes the appropriate actions on the plaintext/cipher text file. The proposed SeDaSC provides confidentiality of data, securely share data, access control of user and control the forward and backward access.

Ching-Hung et al.[10]: Using public key cryptography PKI share data in group is cumbersome and if use private key cryptography key distribution is main problem and also solve the problem of forward and backward secrecy. As per proposed model by researchers for secure data sharing on cloud Only 1 public key which is common in group using that encrypt data which want to share by any group member and another member in group can get that data using own private key which is assigned by group leader. Here, Group leader takes all responsibilities of key generation and updating it when any member leave or join/rejoin the group leader update public and private key.

Criteria based on below summary of literatures review table is constructed are, data Confidentiality for protect private data and only authenticated users can show it, data integrity checking mechanism provide on data sharer side ,data sharing model suitable is suitable for data share in group or peer-to-peer, access rights which are assigned by owner to sharer for data on cloud is only read or all (read,write,delete etc.) and owner should be always online or not when the user wants to access the data.

Table: Summary of literatures review.

Criteria	Data Confidentiality	Data integrity	Data Sharing	Access Rights	Online
Md Mozammil et al.[5]	Yes	No	Peer-to-Peer	Read	Yes
Uma et al.[6]	Yes	Yes	Peer-to-Peer	Read	Yes
Mazhar et al.[2]	Yes	No	Group	All	No
Ching-Hung Yeh.[10]	Yes	No	Group	No	Yes

IV. Proposed System Model

CSP is untrusted third party which provides data storage facilities, computational facilities. so,for secure sharing data on cloud we introduce new entity call as 'Cryptserver', which is trusted party and take responsibility of encrypt/decrypt the file, secret key management and send encrypted/decrypted file to entity(users,CSP) and removes burden of encrypt/decrypt files by users,key management and exchange key with users by owner, owner not be always online when the user wants access the data and not disclose any original credentials to CSP.

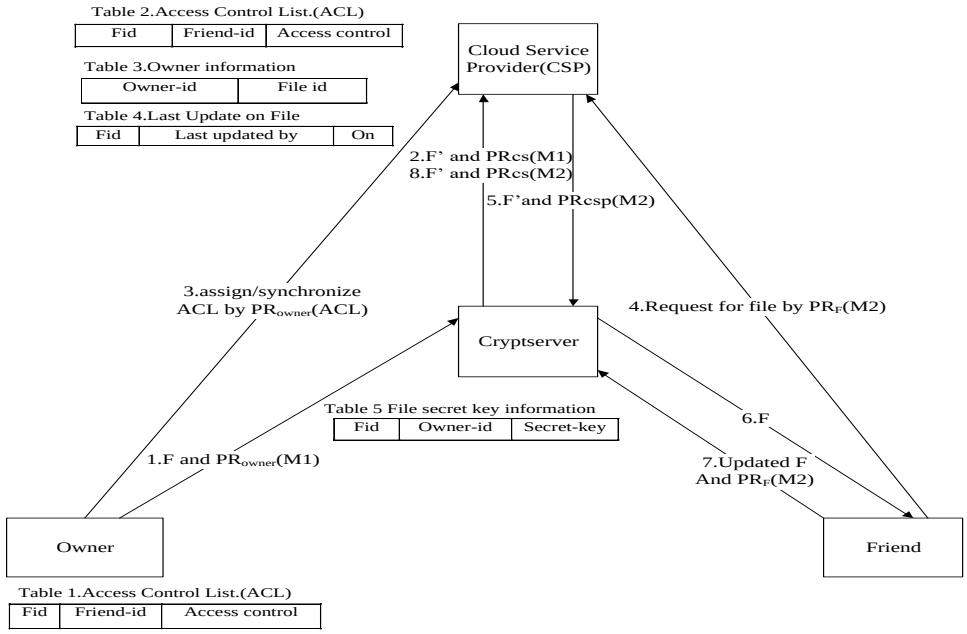

Fig.1. Proposed system model for secure data sharing on cloud

Mainly 3 entities in our proposed model:

i. Users: users of the system users is divided into two types.
- Owner: parson want to share own data to other parsons and also want to assign access rights to parsons, access control list (ACL) is assigned by owner to CSP based on CSP control access on shared data.
- Friend: access the shared file by owner based on access rights assigned by owner.

ii. Crypt-server: Trusted Party take all responsibilities encrypt, decrypt of shared files ,generation and management of the encryption key K.

iii. CSP: Untrusted party provide store facilities and for sharing data ,maintain ACL assigned by user and based on that control access of encrypted store file.

Fig.1 shows the all entities in system along with the information which entity maintains which tables. Table 1 ACL is maintained by file Owner, CSP maintain Table 2 ACL for control the access of the shared file where ACL is assigned by the file Owner,Table3 store owner information and Table 4 for last update on file. Crypt-server maintains Table 5 for File secret key information using which file is encrypted. Below Table shows the information available in message which we have use in our proposed system.

Table: Information in Message

Message-id	Information in Message
M1	fid, owner-id
M2	fid, owner-id, Friend-id

We use secure communication channel that could be Secure Sockets Layer (SSL)channels for communication between users and Crypt server. We assume there is publically available dynamic directory from that public key of any users is available.

Proposed system model in Fig 1 is explain in detail by divide into 3 phase below:

I. Uploading file and assign/synchronize ACL on cloud by owner.
II. Downloading file from cloud by users (Owner, Friend).
III. Updating file on cloud by users(owner, Friend).

Table: List of notations with description

Notation	Description
K	Secret key of symmetric encryption
Fid	File id
F	Plain text file
F’	Cipher text file
CSP	Cloud service provider
Owner-id, Friend-id	Uniquely identify users in system
ACL	Access Control list
Friend	To whom with owner has share data
M1,M2	Message
M1’,M2’	Cipher Message
PUcsp,PRcsp	Public and private key of CSP
PUuser,PRuser	Public and private key of user
PUcs,PRcs	Public and private key of Crypt-server.

I. Uploading file and assign/synchronize ACL on cloud by owner as shown in Fig.1 by Step 1 to 3is explain in detail below.

1. Owner send F and M1’=PR_{owner}(M1) to Crypt-server.
2. Crypt-server Receive information in M1 (Fid and owner-id) by M1= PU_{owner} (M1’) and store that information in Table 5, generate new K and encrypt F by K and generate F’.
3. Crypt-servers send F’ and forward M1’=PR_{cs}(M1) toCSP.
4. CSP Store F' and store fid,owner-id information in M1=PU_{cs}(M1’) into Table 2.
5. For assign/synchronize ACL with CSP ,Owner send ACL’=PR_{owner}(ACL).
6. CSP receives ACL= PU_{owner}(ACL’) and store all information in Table 1 maintain by itself.

II. Downloding file from cloud by Users as shown in Fig.1 by Step 4 to 6 is explain in detail below.

1. User send request for F by sending M2’=PR_{user}(M2) to CSP.
2. CSP receive M2=PUuser(M2’).
3. CSP check
   if owner-id and own-id in M2 are match then request send by file owner
      if owner-id and fid in M2 are match with owner-id and fid in Table 3.
      then generate M2’=PUcsp(M2) where owner-id and Friend-id are same and send M2’and F’ to Crypt-server.
   Else request send by Friend
      If Friend-id and fid in M2 are match with Friend-id and fid in Table 2 ACL maintained by own
      then generate M2’=PUcsp(M2) where owner-id and Friend-id are different and send M2’and F’ to Crypt-server.
4. Crypt-server receives K from Table 5 based on fid and owner-id specified in M2=PUcsp(M2’) and using K decrypt F’ and generate F.

5. Crypt-server forward F to user which is specified in M2 as Friend-id by CSP.

III. Updating file on cloud by Users as shown in Fig.1 by Step 7 and 8is explain in detail below.

1. User send updated F with M2'=PRuser(M2) to Crypt-server.
2. Crypt-server receives K from Table 5 based on fid and owner-id specified in M2=PUuser(M2')and using K encrypt F and generate F'.
3. Crypt-server send F' and M2'=PRcs(M2) which is send by user to CSP.
4. CSP generate M2=PUcs(M2') and check
   if Owner-id and Friend-id in M2 are match then file Owner is file updator
      if owner-id and fid in M2 are match with owner-id and fid in Table 3
      then update F' and maintain information in Table 4.
   Else file updated by Friend
      if Friend-id and fid in M2 are match with Friend-id and fid in Table 2 ACL maintained by own
      then update F' and maintain information in Table 4.

In future, we want to implement this proposed system model using blowfish symmetric encryption algorithm for file encryption and ECC(Elliptic Curve Cryptography) asymmetric encryption for user authentication on data because both algorithms gives best performance as per computational speed and security which are suitable for this proposed system model. [11-12]

V. Conclusion

Cloud computing is emerging paradigm because of rapidly assigned and released with minimal management effort or service provider interaction for required services of users with on-demand-self-services and pay-as-you-go model. Data confidentiality,access control, Scalability, user revocation and re-join in group are necessary requirements for secure sharing data on cloud. so, we proposed system model for secure data sharing on cloud which provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption by users, support dynamically changes of users membership, Owner should not be online when the Friend wants to access the data.

References

[1] Mell P. and Grane T. (September 2011), "The NIST Definition of Cloud Computing," National Institute ofStandards and Technology (NIST) [Online], Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li and Albert Y. Zomaya,SeDaSC: Secure Data Sharing in Clouds,SYSTEMS JOURNAL PP,no.99,2015,1-10.

[3] Hussain Aljafera, Zaki Malika, Mohammed Alodibb and Abdelmounaam Rezguic,A brief overview and an experimental evaluation of data confidentiality measures on the cloud,JOURNAL OF INNOVATION IN DIGITAL ECOSYSTEMS 1, no.1-2,2014,1–11.

[4] Minu George, Dr. C.Suresh Gnanadhas and Saranya.K,A Survey on Attribute Based Encryption Scheme in Cloud Computing , International Journal of Advanced Research in Computer and Communication Engineering 2, no. 11,2013,4408-4412.

[5] Md Mozammil Alam, Sourav Hati, Debashis De and Samiran Chattopadhyay,Secure Sharing of Mobile Device Data using Public Cloud,Confluence The Next Generation Information Technology Summit,2014,149 – 154.

[6] Uma Somani,Kanika Lakhani and Manish Mundra, Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing ,Parallel Distributed and Grid Computing ,2010,211-216.

[7] Raseena M , Harikrishnan G R ,Secure Sharing of Data over Cloud Computing using Different Encryption Schemes An Overview, International Journal of Computing and Technology 1,no. 2,2014,8-11.

[8] Ronald L. Krutz Russell Dean Vines, Cloud Security:A Comprehensive Guide to Secure Cloud Computing(Wiley Publishing ,2010).

[9] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, Secure Data Sharing in the Cloud, springer ,2014,45-72.

[10] Ching-Hung Yeh,A Secure Shared Group Model of Cloud Storage,Advanced Information Networking and Applications Workshops,2013,663 - 667.

[11] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi,Peformance Analysis Of Data Encryption Algorithms,Electronics Computer Technology (ICECT) 5, 2011,399-403.

[12] Kristin Lauter, Microsoft Corporation,The Advantages Of Elliptic Curve Cryptography For Wireless Security,Wireless Communications 11,no. 1 ,2004,62-67.