Overview of Cloud Computing Storage System

Vrushali Arun Patil[1]
Student of BE Information Technology
BVCOE & RI, Nasik, Maharashtra, India, University of Pune
Vrushalip30@gmail.com

Sayali Dilip Jejurkar[2]
Student of BE Information Technology
BVCOE & RI, Nasik, Maharashtra, India, University of Pune
sayalijejurkar@yahoo.in

Sushmita Sonyabapu Gadekar[3]
Student of BE Information Technology
BVCOE & RI, Nasik, Maharashtra, India, University of Pune
Sushmita.gadekar@gmail.com

Abstract **-** Now a days their is main issue related to data that the data should be safe or secure so that no one can make changes in our personal or important data .This System includes Cloud Storage System, which is a paid facility which benefits the Data Owner to outsource its data on the cloud and data owner can perform dynamic operations on the stored data. Data owner has rights to select the authorized user .The dishonest party can be easily detected and data owner will get the alerts .All the authorized user will get the modified data from the data owner. Only data owner has rights to modify, insert, delete etc, and all updated copies are given by data owner to the authorized user.

Keywords—*Cloud Service Provider, Trusted Third Party, Data possession,Provable Data Possession, Dynamic Provable Data Possession.*

*****

I. INTRODUCTION

Many organizations have important data such as finance data, Hospital data, Personal data etc. To handle and maintain this large amount of data is very expensive, so this system is used where large amount of data are handle and not so expensive. Cloud Service Provider is used to reduce the maintenance. The problem of data integrity, confidentiality, access control are solve in this system. The data owner has rights to give permission to access the data to the selected users. The data owner can revoke the permission from the user. Existing system can not detect the unauthorized user. The authorized user doesn't get the duplicate copy, if the data owner changes the uploaded data. The data owner encrypts the data and uploads the data on cloud server by their master public key and authorized user who has access control decrypt the data by its own private key. As the system encryption is done so no unauthorized user can read or make the changes in the data. This system has more advantages than the existing system such as security, performance etc. More benefits are provided in this system than the earlier system. Earlier system doesn't provide the copy of the updated document. The system doesn't get the alert when unauthorized user tries to make the changes in the document.

This all drawbacks are covered in this system as well as performance is greater than the earlier system and less expensive than earlier system. The data owner and authorized user are verified by the TTP. TTP keeps the track or status of the data owner and authorized user. Initially, the information of data owner is stored in the database. The information of authorized user is stored in database, so that Trusted Third Party can easily detect.

The TTP uses the Cheat Detection Algorithm to detect the unauthorized user. The TTP verifies the identification of the data owner and the authorized user. A data owner encrypts the block with same data keys. The data owner generates the proxy re-encryption keys so this system has low management overhead. The important advantage of the proposed system is immediate access to the wide range of application and flexibility to scale up and down Information Technology capacity, mobility. It performs the dynamic operations at the block level. It ensures that the authorized user gets the modified data. It establishes indirect mutual trust between the data owner and cloud service provider since each party resides in a different trust domain. It enforces the access control for the outsourced data. Storage capacity is very main issue in the large organization and to maintain it is very costly. Encryption is done to safe the personal data at the system level. Data owner has the all the rights to select the authorized user and grant the access control.

The system provides main objectives that are:

1. Dynamic operations are done at the block level.
2. Cloud Service Provider is protected from the unauthorized user.
3. The security is well good and good maintain.
4. The performance is fast than the earlier system.

II. LITERATURE SURVEY

The system introduce a model for provable PDP that allows a client that has stored data at an unauthorized server to verify that the server possesses the original data without retrieving it [1]. Remote DP checking protocols allows checking that a remote server can access an uncorrupted file in such a way that the verifier does not need to know before handover the entire file that is being verified. Existing system protocols allow a limited number of successive verifications. In this, system present a new remote data possession checking protocol such that 1) it allows an

 ISSN: 2321-8169
184 - 189

unlimited number of file integrity verifications and 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier [2].

The system construct a highly efficient and provably secure PDP technique based entirely on same key for encryption, which is done at the system level. PDP technique allows data owner to modify, delete, update data [3]. The original PDP scheme applies only to static files. The PDP model which support provable updates to stored data is extended by the definitional framework and efficient constructions for DPDP is represented by the system [4].

The system improve the Proof of Retrievability model to achieve efficient data dynamics [1] by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive security and analysis of system performance show that the proposed scheme is highly efficient and provably secure [5].

III. SYSTEM OVERVIEW

The data owner uploads the important data on the cloud server. Master encryption key or master public key is used by data owner to encrypt data at the system level. The TTP verifies the data owner and authorized user. The authorized user has rights to access the data. The solid lines show the trusted relationship and solid dashed lines shows the non trusted relationship. The data owner can perform full block level dynamic operations on the outsourced data.

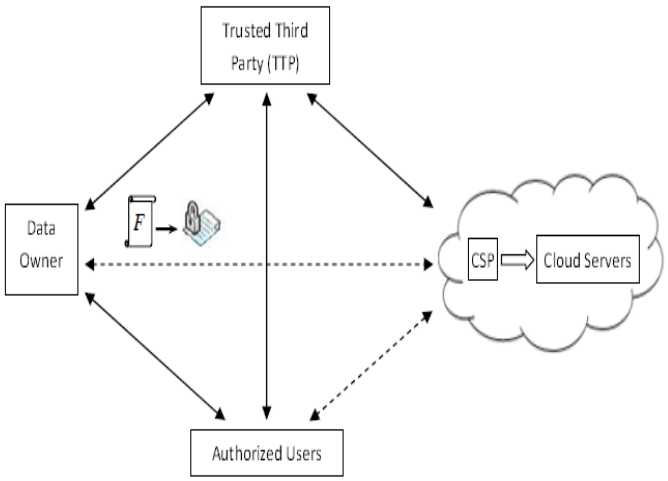

Figure 1: System Model

CRYPTOGRAPHIC TECHNIQUES

1. Lazy Revocation –
   This technique is used to remove the access rights from the authorized user. The copy of that data which is updated by the data owner is not given to that authorized user (whose access rights are removed). Every time when access is removed the next key is to encrypt the data. The cycle of changing master public key begins.

2. Key Rotation-
   This is the technique where the sequence of the key can be generated from the initial key and the master secret key. There are two types:-

2.1 The current key is used by data owner to Generate next key.
Authorized user can also generate all previous key if he knows the key.

3. bENC-
   The Broadcast Encryption is used by the data owner to upload the important data on the server in the encrypted form. Only authorized users are able to access the encrypted data.

IV. Algorithmic Strategy

Algorithmic strategy contains following algorithms:

A. MODIFICATION OF DATA

/* Modification of a block b j with b j for the outsourced file */

/* RevFlag is initialized to false */

Data Owner

1) If the access of one or more users has been revoked then

a) Rolls Kctr forward (using key rotation)

b) Increments ctr = ctr + 1, and sets RevFlag = true

c) Copies KVj from BST O to KVj (i.e., KVj = KVj)

d) Sets KV j = ctr in BST O, and generates Rot =

ctr, bENC(Kctr)

e) Sends Rot to the TTP

2) Creates an encrypted block $\tilde{b}_j$ = E DEK (BN j ||b j), where

DEK = h(K ctr)

3) Forms a block-modify entry TEntryBM = {BN j , KV j }

4) Sends a modify request BM, TEntryBM , j, KV j , h($\tilde{b}_j$), RevFlag, $\tilde{b}_j$ to both the CSP and the TTP (OSMR

 ISSN: 2321-8169
184 - 189

transmission), where h (˜ b j) is the hash of the outsourced

block to be modified. The KVj is not sent in the modify

request if RevFlag = false

5) The CSP accepts the modify request only if {BN j , KV j } sent from the owner matches {BN j , KV j } in BST C , and h(˜ b j) is equal to the hash of ˜ b j on the cloud server (to guarantee that correct values are sent to the TTP)

CSP
/* upon accepting the modify request from the owner */

1) Replaces the block b j with b j in the outsourced file F
2) If RevFlag = true then

Updates the BST C entry at index j using TEntry BM

TTP

1) Updates F H T T P = F H T T P ⊕h(˜ b j) ⊕h(˜ b j)
2) If RevFlag = true then

a) Updates the previously stored Rot with the newly received value

b) Updates T H T T P = T H T T P ⊕h(BN j ||KV j) ⊕ h(BN j ||KV j)

B. INSERTION OF DATA

/* Insertion of a block ¯b after index j in the outsourced file */

/* RevFlag is initialized to false */

Data Owner

1) If the access of one or more users has been revoked then

a) Rolls K ctr forward (using key rotation)
b) Increments ctr = ctr + 1, and sets RevFlag = true
c) Generates Rot = ctr, bENC(K ctr)
d) Sends Rot to the TTP

2) Constructs a new block-insert table entry TEntry BI = {BN j+1 , KV j+1 } = {1 + M ax{BN j } 1≤j≤m , ctr}, and inserts this entry in BST O after index j
¯ b = E DEK (BN j || ¯b), where

3) Creates an encrypted block ˜
DEK = h(K ctr)

4) Sends a request BI, TEntry BI , j, null, null, RevFlag, ˜
¯b to both the CSP and the TTP (OSMR transmission)

CSP
/* upon receiving the insert request from the owner */
¯b after index j in the outsourced file F
1) Inserts the block ˜
2) Inserts the table entry TEntry BI after index j in the BST C.

TTP
1) Updates F H T T P = F H T T P ⊕h(˜
2) Updates T H T T P = T H T T P ⊕h(BN j+1 ||KV j+1)
3) If RevFlag = true then

...Replaces Rot with the newly received value

C. DELETION OF DATA

/* Deletion of a block b j from the outsourced file */

Data Owner

1) Copies the entry at index j from BST O to a block-delete table entry TEntry BD = {BN j , KV j }
2) Deletes the entry at index j from BST O
3) Sends a request BD, TEntry BD , j, null, h(˜ b j), false, null to both the CSP and the TTP (OSMR), where h(˜ b j) is the hash of the outsourced block to be deleted
4) The CSP accepts the delete request only if TEntry BD sent from the owner matches {BN j , KV j } in BST C and h(˜ b j) is equal to the hash of the block ˜ b j on the cloud server (to guarantee that correct values are sent to the TTP).

CSP
/* upon receiving the delete request from the owner */

1) Deletes the block at index j (block ˜ b j) from the out-sourced file F
2) Deletes the entry at index j from the BST C

TTP

 ISSN: 2321-8169
184 - 189

1) Updates F H T T P = F H T T P ⊕h(˜ b j)
2) Updates T H T T P = T H T T P ⊕h(BN j ||KV j)

D. ACCESS TO DATA

1) An authorized user sends a data-access request to both the CSP and the TTP

2) The CSP responds by sending the outsourced file F = {˜ b j } 1≤j≤m associated with a signature σ F (CSP's signature on the entire file), and sending BST C associated with a signature σ T (CSP's signature on the entire table) to the authorized user

3) The authorized user verifies σ F and σ T , and accepts the data only if σ F and σ T are valid signatures

4) The TTP sends F H T T P , T H T T P , and Rot = ctr, bENC(K ctr) to the authorized user

5) Verification of the BST C entries

a) The user computes T H U = ⊕m
j=1 h(BN j ||KV j)

b) If the user claims that T H U = T H T T P then

...report "integrity violation" to the owner and

...invoke cheating detection procedure (Fig. 7)

6) Verification of the data file F
˜

a) The authorized user computes F H U = ⊕m
j=1 h(b j)

b) If the user claims that F H U = F H T T P then

...report "integrity violation" to the owner and

...invoke cheating detection procedure (Fig. 7)

7) Data access

a) The authorized user gets K ctr by decrypting bENC(K ctr) part in Rot

b) for j = 1 to m do

/* rotate backward the current K ctr to the version that

is used to decrypt the block˜ b j */

...– Set K j = K ctr

...– for i = 1 to ctr - KV j do

.....K j = (K j) e mod N /* N is the RSA modulus*/

.....end for

−1

(˜ b j), where DEK = h(K j)

...– (BN j ||b j) = E DEK

...– Get the physical position SN j of b j using BN j

..... and BST C

...– The authorized user places b j in the correct order

E. CHEATING DETECTION

The TTP is invoked to determine the dishonest party:

1) The TTP verifies σ T and σ F
2) If any signature verification fails then

...TTP reports "dishonest owner/user" and exits
3) The TTP computes T H temp = ⊕m
j=1 h(BN j ||KV j) and
˜F H temp = ⊕m
j=1 h(b j)

4) If T H temp = T H T T P or F H temp = F H T T P then
...TTP reports "dishonest CSP" and exits
...../* data is corrupted */
else
...TTP reports "dishonest owner/user" and exits
...../* data is NOT corrupted

V. IMPLEMENTATION METHOD

System flow diagram shown in figure 2 provides all details regarding different operations performed within system.

 ISSN: 2321-8169
184 - 189

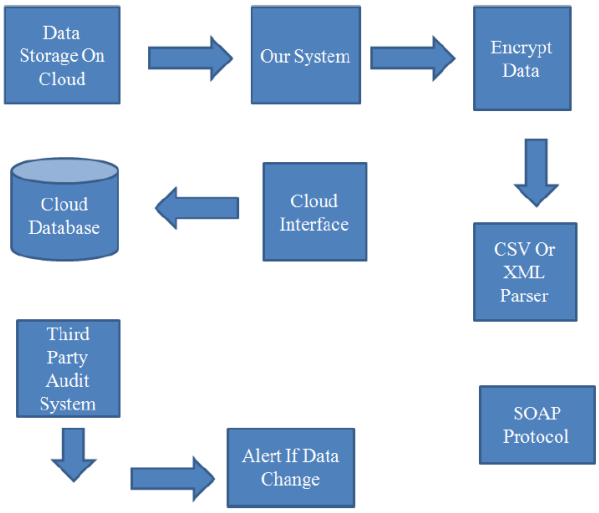

Figure 2: System Flow

The System Algorithm uses different type of method used in the system –

1. Cloud Server

In this module, cloud service provider has to get the key first than only he can store the file in this cloud server. The TTP can only check the cloud server whether cloud server is authorized or not. If it is fake trusted third party won't allow the file to store on the cloud server.

2. Data Owner

In this module, if a data owner of data has to store data on the cloud server, he or she should register the details first. These details are maintained in the database. Then he has to upload the data in a file database. The data which are stored in a database are in an encrypted form. Authorized user can only decode it.

3. Trusted Third Party

In this module, TTP monitors and verifies the data owner and checks the cloud server is authorized or not. The trusted third party uses cheat detection algorithm to detect the unauthorized user.

4. Authorized User

In this module, if the user wants to access the data then the user has to register first and if data owner have given rights then only he can access otherwise user can not access.

VI. CONCLUSION

The system proposed a cloud based storage system where the data owner uploads the data on the cloud and encrypt the data on the system level. The data owner has rights to select the authorized user and grant or revoke access rights from the user. The security issues are also well handled, the techniques such as Lazy Revocation, Key Rotation and Broadcast Encryption algorithm. Other important factor is Trusted Third Party who has the all the personal data of the data owner and the authorized user. The unauthorized user is recognized by the TTP and give alerts to authorized users. At the system level encryption is done, no one knows the secret key except the data owner.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson, and D.Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598-609.

[2] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Securityand Privacy in Communication Netowrks, 2008, pp. 1-10.

[4] C. Erway, A. Kupc u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213-222.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proceedings of the 14th European Conference on Research inComputerSecurity, 2009, pp. 355-370.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89-98.

[7] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Overencryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123-134.

[8] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multiple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[9] K. D. Bowers, A. Juels, and A. Oprea, 'HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187-198.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89-98.

 ISSN: 2321-8169
184 - 189

[11] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03: File and Storage Technologies, 2003.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT '08, 2008, pp. 90-107.

Vrushali Arun Patil she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of computer networking.

Sayali Dilip Jejurkar she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of pune. Her interest in the field of cloud computing.

Sushmita Sonyabapu Gadekar she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Instituted, Nashik Under University of Pune. Her interest is in the field of database administrator.