ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Privacy Aware Data Sharing In Cloud

[1] Tessy John. L, [2] G.Michael
P.G Student, Dept. of CSE, Bharath Institute of Higher Education and Research. Chennai
Asst. professor, Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai

Abstract: ***Cloud storage is a unified object storage that redeem organizations from secure data storage systems. Though, cloud storage gives rise to security reasons. In group-shared data, the data face cloud- oriented and insider threats. Privacy aware data sharing in a group that counts insider threats of mischievous users is an important research issue. Privacy Aware Data Sharing in Clouds methodology provides data security and integrity, access with time intervals, data sharing among the group shared data within a group, counting insider threats, and access control of the data. The file encrypts with a single encryption key. Two different key shares are generated, the user mastering one share. The dominion of a one share of a key allows the privacy aware methodology used to count the insider threats. Another key is with a cryptographic server. The privacy aware methodology is also suitable for well-established and mobile cloud computing systems. It is an implement of working ideal of this methodology and size up its performance based on the time go through during various operations. Also conventionally verify the working of privacy aware data sharing by using Petri nets, the Satisfiable Modulo Theories Library, and a Z3 solver. The results proved to be hopeful and shows privacy aware data sharing in cloud has the future to be capably used for secure group data sharing in the cloud.***

Keywords—Access control Language, cloud computing, Petri net,modeling,Satisfiable Theory.

I. INTRODUCTION

Cloud computing is acting turn up due to the apparatus computing services for clients. System with a low allocation can employ high computing and storage services without lend in frame work and upkeep .The debt of control bygone data and computing hike many security burden for organizations. Cryptography is used as a symbolic tool to provide familiarity and privacy services to the data. The data are encrypted before consume to the cloud. The access control, key management, encryption, and decryptions are controlled by the customers to establish data security. When the data are to be shared within a group, the cryptographic services need to be malleable enough to handle different users, training the access control, and maintain the keys in an efficient manner to shield data familiarity. The extant, departing, and fresh joining group members can justify to be an insider threat contravene data familiarity and privacy. Insider threats can prove to be more calamitous due to the fact that they are generally launched by trusted entities. Multiplex security controversy can crop up due to diverse users in a group. A single key shared between all crew members will result in the approach of past data to a new joining member. In group-shared data, the inside users may provoke the concern of backward access control and forward access control .The simple solution of emit does not prove to be climbable for frequent changes in the group.

A feasible key for each user is a ponderous solution. The data must be free encrypted for each user. The changes in the data depend upon the decryption of all of the copies of the clients and encryption again with the modifiable contents. The data can be decrypted, modified, and re-encrypted by a malicious user within a group. Therefore, an unlawful user in the group might access certain unauthorized files within the group.

The possession of the key also essentially proves the malicious of a user to operate on the data. The proposed methodology named Privacy aware data sharing that deals with the introductory security requirements of grope shared data within the cloud.

The Privacy aware data sharing methodology works with three entities as follows:

1) Clients
2) Cryptographic server
3) Cloud.

The owner of the data submits the data, the list of the users, and the parameters required for achieve an access control list to the Cryptographic server. The Cryptography server is a trusted third party and is responsible for key management system, encryption, decryption, and access control. The CS generates the key and encrypts the data with the generated key. Finally, for each client in the group, the CS divides the key into two parts such that a one part alone cannot recreate the key. Successively, the original one is deleted through secure overwriting. One part of the key is transmitted to the

reciprocal user in the group, The ACL is generated through the parameter. The encrypted data are frequently uploaded to the cloud.

The key is recreated by operating on the user side of the key, and the corresponding CS maintaining the precise portion for that particular user. The data can be decrypted and sent back to the client. For a newly joined client, the two key shares are generated, and the client is added to the ACL. For a departing member, the record is deleted from the ACL. Furthermore, Privacy aware data sharing can be used with the mobile cloud computing ideal in addition to typical cloud computing due to the fact that compute-in depth operations are performed by the Cryptographic server.

Existing system:

The data can be decrypted, modified, and re-encrypted by an illegal user within a group. A lawful client in the crew might access certain pirated files within the crew. CL-PRE scheme, the data proprietor encrypts the data with the commensurable key. The symmetric key is encrypted with the public key of the data proprietor. The encrypted key is reencrypted by the cloud, that turn into decryptable by the client private key.

Drawbacks of existing system:

The proxy reencryption is hinge on bilinear pairing and the bilinear Diffie–Hellman problem that makes the CL-PRE scheme computationally comprehensive. The computing cost of the bilinear pairing is high as compared with the standard operations in finite data fields.

Proposed system:

The Privacy aware data sharing methodology gives security for the data among a group without using the El-Gamal cryptosystem, the bilinear Diffie–Hellman problem, and bilinear pairing. The Privacy aware data sharing methodology is based on symmetric cryptography without Reencryption. It seems lightweight methodology for using .The encryption and decryption functions are performed at the Server that is a trusted third party in the Privacy aware data sharing methodology. The working of Privacy aware data sharing was legally analysed using HLPNs, the SMT-Lib, and a Z3 solver.

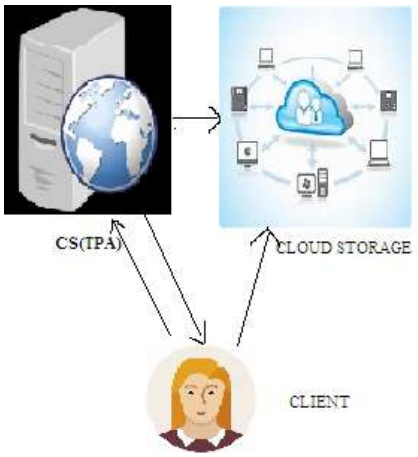
Advantages of proposed system:

The proposed methodology insures the covertness of the data on the cloud by using symmetric encryption. The crew of clients are ensured without the elliptic curve or BDH cryptographic reencryption. The custody of a section of the key ensure the data against illegal insiders within the crew. The proposed Privacy aware data sharing methodology insures the data against issues of forward and backward access control that arise due to insider menace. The performance of the Privacy aware data sharing methodology was calculated based on the time utilization during the key generation, file upload, and file download operations.

Privacy aware data sharing in cloud

Here presenting the design of proposed methodology privacy aware data sharing that gives security for sharing and forwarding of data within a group without involving reencryption in the cloud.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018



Privacy aware data sharing architecture

1. Entities

The Privacy aware data sharing in cloud methodology has the following entities.

A) Cloud: The cloud grant storage services to the client. The data on the cloud want to be secured against privacy rupture. The covertness of the data is insured by accumulate encrypted data bygone the cloud. The cloud in the Privacy aware data sharing in cloud methodology only associate basic cloud operations of file upload and download. Accordingly, no changes at the obligation or utilization level on the cloud are required.

B) CS: The CS is a trusted third party and is liable for the preservation operations, such as key administration, encryption, decryption the encryption, the administration of the ACL for providing hypnotic, and shielded data forwarding within in a group. The clients of Privacy aware data sharing in cloud are vital to be registered with the CS to seize the security services. The CS is assumed to be a secure entity in the future methodology. The CS can be retained by a system or can be bought by a third-party provider. However, the CS maintained by a system will create more trust in the system.

C) Clients: The clients are the users of the stockpile cloud. For each data directory, one client will be the proprietor of the data file, although the others in the group will be the data consumers. The owner of the file determine the access rights of the other crew members. The access rights are acknowledged and revolted based on the ruling of the owner. The access rights are handled by the CS in the form of an ACL file. A depurate ACL is cultivate for each of the directory.

2. Cryptographic Keys

The Privacy aware data sharing in cloud methodology retained a single cryptographic key for each of the directory. Yet, after encryption/ decryption, the full key is not stored and enchanted by any of the involved parties. The key is segregation into two parts and are possessed by different entities. The following are the keys that are used in Privacy aware data sharing in cloud.

3) Symmetric Key X: X is a random secret generated by the CS for every directory. The length of X in Privacy aware data sharing in cloud is 256 bits, as is endorsed by most of the standards regarding key length for symmetric key algorithms. Yet, the length of the key can be altered X is obtained in a two-step process. In the first step, a random number Z of length 256 bits is generated such that $Z = \{0, 1\}^{256}$. In the next step, Z is passed through a hash function that could be any hash function with a

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

256-bit output. Here secure hash algorithm 256. The second step completely randomizes the initial user-derived random number *Z*. The output of the hash function is termed as *X* and is used in symmetric key encryption for securing the data.

Algorithm: 1 Key generation And Encryption

Input:

A, the ACL, the SKA, the 256- bit hash function H_f **Compute**:

$Z = \{0, 1\}^{256}$

$A = H_f(Z)$

$C = \text{SKA}(A, X)$

for each user *i* in **the ACL, do**

$X_i = \{0, 1\}_{256}$

$X_i = X \oplus X_i$

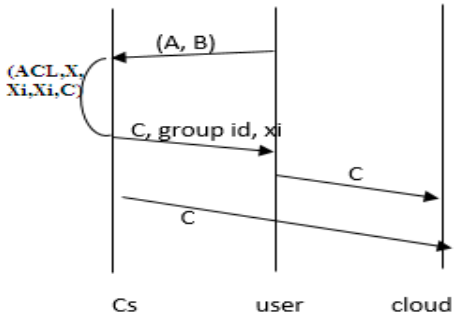
Add Xi for user *i* in the ACL

Send xi for user *i* **end for** delete (*x*) delete return *C* to the owner or upload to the cloud.

Privacy aware data sharing design

In this section, we present the design of privacy aware data sharing. In particular, we propose several cryptographic key operations that enable privacy aware data sharing to achieve security goals.

1) File Upload: Whenever a need to share data among a group, the file proprietor sends the request to the CS *B* is used to access rights for each of the users. *B* is used to create the ACL for the data. *B* is sent to the CS. The CS, after receiving the encryption request for the file, creates the ACL from the list and creates a group of the users. Subsequently, the CS generates xi, xi for every user and deletes *X* by secure overwriting. The *xi* for each user is inserted into the ACL for later use. To secure the integrity of the file, the group, and the xi for the owner are sent to the requesting data owner. The group ID and the xi for the rest of the group clients are directly sent to them over a secure communication list.



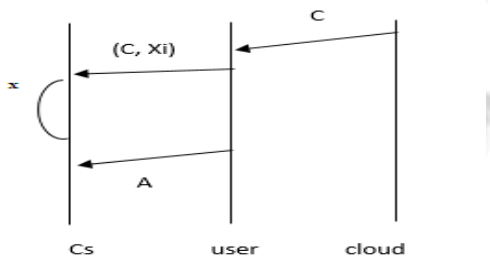
File upload.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

In this section. In the second option, the CS can be delegated the authority to upload the file to the cloud on behalf of the user

Algorithm 2: Decryption algorithm

Input: C, the ACL, the SKA **Compute**:
GeT Xifrom the requesting user
Get C from the requesting user or download from the cloud
Retrieve xi from the ACL
If xi does not exist in the ACL, then return the access denied message to the user else
X=xi+xi'
A= SKA(C, X) send A
to the user
end if
delete (X) delete
xi'



File download.

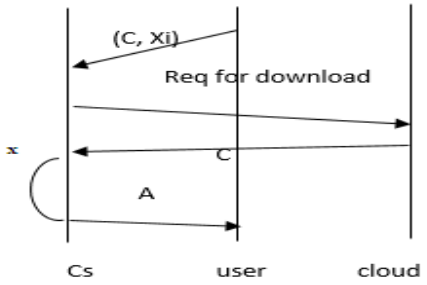


Fig. 4. File download: A special case.

The CS, after authenticating the user, sends the download request to the cloud for the specified file. The cloud sends the encrypted file (C) to the CS.

II. CONCLUSION

The Privacy aware data sharing methodology provides guaranteed deletion by deleting the parameters vital to decrypt a file. The encryption and decryption functionalities are execute at the CS that is a trusted third party in the Privacy aware data sharing methodology. Based on the time expenditure during the key generation, file upload, and file download operations. The results graveled that the Privacy aware data sharing methodology can be practically used in the cloud for secure data sharing among the group.

III. REFERENCES

[1] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 1431–1441, Jul. 2014.

[2] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Future Gen. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, Jul. 2013.

[3] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, Feb. 2014.

[4] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.

[5] D. Chen et al., "Fast and scalable multi-way analysis of massive neural data," IEEE Trans. Comput., DOI: 10.1109/TC.2013.2295806, 2014, to be published.

[6] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in Proc. 6th USENIX Security Symp. Focusing Appl. Cryptography, 1996, p. 8.

[7] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud," in Proc. 7th ACM Symp. Inf. , Comput. Commun. Security, 2012, pp. 87–88.

[8] Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in Proc. IEEE 11th Int. Conf. TrustCom, 2012, pp. 295–302.

[9] K. Alhamazani et al., "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," Computing, DOI: 10.1007/s00607-014-0398-5, 2014, to be published

[10] L. Moura and N. Bjrner, "Satisfiability modulo theories: An appetizer," in Proc. Formal Methods, Found. Appl., vol. 5902, Lecture Notes in Computer Science, 2009, pp. 23–36.