Secure Encrypted Scheme Over Outsourcing Data for Query on MultiCloud Platform

Ms. Gayatri Patil
Computer Department, Dr.Babasaheb Ambedkar University,Lonare, India
Email: patilgayatrib12@gmail.com

***Abstract*— A secure knowledge cluster sharing and conditional dissemination theme with multi-owner in cloud computing, within which data owner will share non-public information with a group of users via the cloud in an exceedingly secure manner, and knowledge communicator will publicize the info to a brand new cluster of users if the attributes satisfy the access policies within the ciphertext. We have a tendency to additional gift a multiparty access management mechanism over the disseminated ciphertext, within which the info co-owners will append new access policies to the ciphertext thanks to their privacy preferences. Moreover, 3 policy aggregation ways, together with full permit, owner priority and majority permit, are provided to solve the privacy conflicts downside caused by completely different access policies. Many schemes are recently advanced for storing information on multiple clouds. Distributing data over completely different cloud storage suppliers (CSPs) mechanically provides users with a definite degree of data run management, for no single purpose of attack will leak all the knowledge. However, unplanned distribution of data chunks will cause high information revealing even whereas exploitation multiple clouds. An efficient storage plan generation algorithmic rule supported cluster for distributing information chunks with least data escape across multiple clouds. So to provide more security to users data we will divide our data into blocks and upload each block to different cloud providers.**

Keywords*— *Data Sharing, Conditional Proxy re-encryption, Attribute-based encryptionn , Privacy Conflict, System Attackability, Remote Synchronization, Distribution and Optimization

INTRODUCTION

The popularity of cloud computing is obtained from the benefits of rich storage resources and instant access. It aggregates the resources of computing infrastructure, and then provides on-demand services over the Internet. Many famous companies are
now providing public cloud services, such as Amazon, Google, and Alibaba. These services allow individual users and enterprise users to upload data (e.g. photos, videos and documents) to cloud service provider (CSP), for the purpose of accessing the data at any time anywhere and sharing the data with others.

With the more and more fast uptake of devices like laptops, cellphones and tablets, users need associate degree present and massive network storage to handle their ever-growing digital lives. To fulfill these demands, several cloud-based storage and file sharing services like Dropbox, Google Drive and Amazon S3, have gained quality because of the easy-to-use interface and low storage price. However, these centralized cloud storage services are criticized for grabbing the management of users' knowledge that permits storage suppliers to run analytics for promoting and advertising

Prof. Mr. Rahul Gaikwad
Associate Professor, Computer Department,
Dr.Babasaheb Ambedkar University,Lonare,
India

[1]. One possible resolution to scale back the chance of data leak is to use multicloud storage systems [2], [3], [4], [5] in which no single purpose of attack will leak all the data. A malicious entity, like the one disclosed in recent attacks on privacy [6], would be needed to oblige all the various CSPs on that a user would possibly place her knowledge, so as to induce a complete image of her knowledge. Put simply, as the saying goes, do not put all the eggs in one basket.

CSPs such as Dropbox, among many others, employ rsync-like protocols [7] to synchronize the local file to remote file in their centralized clouds [8]. Every local file is partitioned into small chunks and these chunks are hashed with fingerprinting algorithms such as SHA-1, MD5. Thus, a file's contents can be uniquely identified by this list of hashes. For each update of local file, only chunks with changed hashes will be uploaded to the cloud. In order to protect the privacy of users, most cloud services achieve access control by maintaining access control list (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owner's control.

I. LITERATURE SURVEY

A. Introduction

Series of unaddressed security and privacy issues emerge as important research topics in cloud computing. To deal with these threats, appropriate encryption techniques should be utilized to guarantee data confidentiality. In private information sharing schemes, information owner outsources encrypted information to the CSP by shaping a listing of receivers, therefore solely the supposed users within the list will get the cryptography key and further decode the non-public information. ABE is another promising one-to-many science technique to understand information encryption and fine-grained access management in cloud computing.

B. Literature Survey

Secure data dissemination is another important security requirement for data storage in cloud computing. The identity-based PRE [33] is a basic encryption algorithm to reach secure data dissemination in cloud computing, with which the data disseminators could send their reencrypting keys to the semi-

trusted proxy to transform data owner's ciphertext for new users

Sr. No	Paper Title	Author	Name of Journal/ Conference	Summary / Gains
1	Ciphertext-Policy Attribute-Based Encryption	J. Bethencourt, A. Sahai, and B. Waters	IEEE Symposium on Security and Privacy	provides a replacement kind of encrypted access management .
2	NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds	H. Chen, Y. Hu, P. Lee, and Y. Tang	IEEE TRANSACTIONS ON COMPUTERS	It provides us a cost-effective repair for a permanent single-cloud failure
3	Achieving Scalable Access Control Over Encrypted Data for Edge Computing Networks	B. Lang, J. Wang, and Y. Liu	IEEE Access, vol. 5, pp. 1510-1523, 2017.	It proposes such a scheme in which key distribution does not require any secure channels
4	Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage	K. Xue, W. Chen, W. Li, J. Hong, and P. Hong	IEEE Transactions on Information Forensics and Security, vol. 13	Provides a solution to secure encrypted cloud storages from EDoS attacks and supply resource consumption answerableness
5	Identity-based broadcast encryption with constant size ciphertexts and private keys	C. Delerabl´e e	Proc. International Conf. on the Theory and Application of Cryptology and Information Security	IBBE system with constant size ciphertexts and private keys

II. PROPOSED METHODOLOGY

More use of cloud storage enforces people to store their data on cloud, which creates problem of confidentiality of user's data. Due to some malicious users, data can be leaked in multi cloud storage environment, to avoid this problem an information leakage aware storage system is proposed. To provide multiparty access control mechanism over the disseminated data.

A. Architecture

Our system model consist of data owner, data co-owner, data user, multiple clouds and trusted authority. The data owner will divide the data into different blocks encrypt those blocks and upload them on different clouds. At the same time data owner will choose a policy aggregation strategy. The strategies are of three type full permit, owner priority and majority permit. In Full Permit all owners (including data owner and data co-owners) have the same right to decide the dissemination conditions of data. The data disseminator should satisfy all the access policies defined by these owners. In Owner Priority the data owner's decision has high priority, though he tags the co-owners. The data disseminator can disseminate the data only when he satisfies the access policy of data owner or all the access policies of data co-owners. In majority permit the data owner firstly chooses a threshold value, and the data can be disseminated if and only if the sum of access policies satisfied by disseminator's attributes is greater than or equal to this fixed threshold. We require these policy aggregation strategies to fulfill the authorization requirements from multi-owner i.e. data owner and data co-owners.

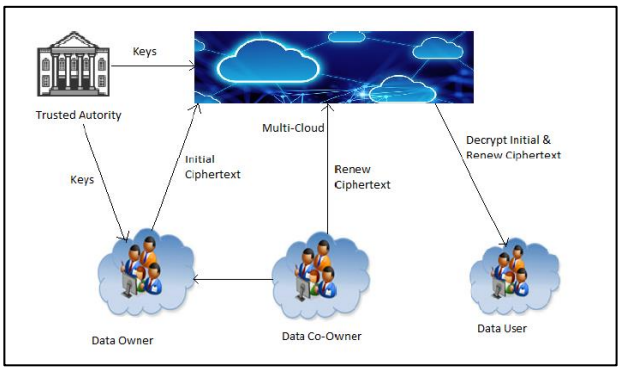

Fig: System Architecture

System Analysis:

A. Algorithms

Algorithm 1: File Splitting and Encryption:

Input: Text file, secret key
Output**:** Encrypted Files E (F.1), E (F.2)... E (F.N)

Step 1: Uploads a file (F) and secret key (SK)

Step 2: Divide the file into blocks.

Step 3: Index based files (F.1, F.2...F.N) are created with the same file name.

Step 4: Encrypt each part of the divided file E (F.1), E (F.2)...E

(F.N) and upload it to
the Cloud server.

Step 5: Data user will request for keys to Data Owner and once have them can decrypt
and download the file.

Step 6: End

Algorithm 2: File Decryption

Input: File Name, Secret key (SK)
Output: Decrypted File parts

Step 1: Get the File Name (FN) and Secret Key (SK) from the data owner or File owner
by making request

Step 2: Enter or Pass that File Name (FN) and secret Key (SK)

Step 3: Pass the secret key (SK) to the data user

Step 4: Data user can download the original file F.

Step 5: End

B. Mathematical model

Let S be a System such that,

S = {I, P, O}

I = Input

P = Process

O = Output

I = {I1, I2, I3, I4}

I1=File (Text/Doc/PDF)

I2=Public Key

I3=Private Key

I4=Tags

P = {P1, P2}

P1 = Encryption of File(S [EF])

S [EF] =TSB+TEB+TUD+TUC+TGK

Where,

TSB=Time required to split file into blocks.

TEB=Time required to encrypt block of file.

TUD=Time required to upload block of file to database.

TUC= Time required to upload block of file on cloud.

TGK= Time required to generate keys.

P2 = Decryption of File(S [DF])

S [DF] = TGK+TDBF+TDF+TAB+TDB

Where,

TGK= Time required to get the keys from data owner.

TDBF= Time required to decrypt block of file.

TDF= Time required to decrypt file.

TAB= Time required to add block of file.

TDB= Time required to delete block of file.

O = {O1, O2}

O1 = Original Content of file

O2 = Check the status of file (Changed/Original)

C. Software requirement specification:

Hardware requirements:

Processor Type	Pentium IV
Speed	2.4 GHZ
RAM	3 GB
Hard disk	20 GB
Keyboard	101/102 Standard Keys
Mouse	Scroll Mouse

Software requirements:

Operating System	Windows 7/8
Programming Package	Net Beans IDE 8.2
Coding Language	JDK 1.8
Database	MySQL

D. Some Common Mistakes

According to review we have done, in existing papers, the proposed system assures more security as compared to existing system. As we are dividing file into number of blocks and to each block we are assigning a tag, after this the re-encryption of the file is done using two different algorithms. To upload file on cloud the time taken by proposed system is less than the existing system.

III. RESULT AND DISCUSSIONS

The expected results are the user's data will get more security as we are going to divide the data into multiple blocks and these blocks are stored on multiple clouds so if an attacker gets access to any of the block then the next block will be stored on different cloud so the attacker will not get access to it. By all this we assure more security and integrity of the user's data.

IV. CONCLUSIONS

Distributing knowledge on multiple clouds provides users with a certain degree of data run management there in no single

cloud supplier are aware of the entire user's knowledge. However, unplanned distribution of information chunks will cause avoidable information run. The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the
data confidentiality becomes a challenge. Here, we are providing information leakage aware storage system and confidentiality of the data in an multi cloud environment.

REFERENCES

[1]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," Proc. IEEE Symposium on Security and Privacy (SP '07), pp. 321-334, 2007.

[2]. H. Chen, Y. Hu, P. Lee, and Y. Tang, "Nccloud: A network-coding-based storage system in a cloud-of-clouds," 2013.

[3]. H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.

[4]. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[5]. C. Delerabl´ee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT '2007), pp. 200-215, 2007.

[6]. B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," IEEE Access, vol. 5, pp. 1510- 1523, 2017.

[7]. L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," IEEE Transactions on Cloud Computing, 2018,
https://ieeexplore.ieee.org/document/8458136.

[8]. N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[9].T. G. Papaioannou, N. Bonvin, and K. Aberer, "Scalia: an adaptive scheme for efficient multi-cloud storage," in Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE Computer Society Press, 2012, p. 20.

[10]. Z. Yan, X. Li, M.Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[11]. H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and fine-grained data access control mechanism for P2P storage cloud," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.

[12]. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/docu ment/7448446.

[13]. J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," Proc. of 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 541–546, 2014

[14]. S. Choy, B. Wong, G. Simon, and C. Rosenberg, "A hybrid edge-cloud architecture for reducing on-demand gaming latency," Multimedia Systems, pp. 1–17, 2014.

[15]. L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[16]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.

[17.] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing
and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[18]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. on Computer and Communications Security (CCS '06), pp.89- 98, 2006.

[19]. S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based
data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[20]. L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social assisted mobile content dissemination scheme in DTNs," Proc. 32nd IEEE International Conf. on Computer Communications (INFOCOM '2013), pp. 2301-2309, 2013.