WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Access and Sharing of Data in Cloud with Time Condition Decryption

Mr. C. A.Kandasamy[1], Mr.C.Kirubakaran[2], Mr.S.Kavin[3], Ms.T.Karpaga Lakshmi[4], Mr. S. Kamesh[5]

[1] Assistant Professor, Department of MCA, K.S.R. College of Engineering, Tiruchengode, kandamca86@gmail.com
[2 ,3, 4, 5] Student, Department of MCA, K.S.R. College of Engineering, Tiruchengode, cemcakirubakaran22@gmail.com, kavinsmiley12345@gmail.com, kkarpagalakshmi2001@gmail.com, cemcakamesh19@gmail.com

ABSTRACT

Cloud has been utilized by everyone widely due to its various usages such as storing and sharing of huge volume of data. To ensure secure data transaction, encryption is a well known approach for it. Currently storing a data in cloud with security by encrypting the particular file and disseminating it to other person is available. In single file transaction issues are not faced a lot because it gets acknowledgement from the owner of the file before dissemination. The issue faced here is while sharing a file to multiple person or group with multi owner concept. Because when a file has been shared by a single person to multiple persons then these persons will also be the owner of that particular file. Based on these users need file may be shared to n number of persons or groups hence this affects original owner policy. To overcome this issue attribute based condition dissemination has been implemented with time based keyword search. In our proposed system a file could be shared among different users with condition through Attribute Based Encryption (ABE). To secure against data leakage while searching a file from cloud Time based keyword search has been proposed in addition. This shows our proposed method attains better performance in secure sharing and storing of data in cloud compared to other existing methods.

Keywords: Attribute based encryption, secure data transaction, cloud, data leakage and multi owner.

I. INTRODUCTION

Cloud computing is considered to be a figuring worldwide through its resources facility in the computing environment are available as services over the Internet. The cloud computing benefits singular clients and ventures with helpful access, expanded operational efficiencies and rich storage resources by combining existing works and new generating approaches for studying, for example, service oriented designs and virtualization. Although the benefits brought by cloud computing are exciting for users, security problems may somehow impede its quick development. At present, to an ever increasing extent clients would outsource their information to cloud service provider (CSP) for sharing. However, the CSP which denies data owners immediate power over their information is accepted to be straightforward however inquisitive, that may provoke security concerns. These security matters existing in open cloud encourage the necessity to appropriately keep information confidential. Several approaches generating cryptographic systems to settle the security issues have been proposed. In our proposed work ABE is used to secure data in cloud.

In general, the encryption techniques can protect data from unauthorized entities accessing but it does not focus on data dissemination in cloud computing. Through the above techniques data has been encrypted and information disseminators are definitely not able to modify the cipher text uploaded by information owner. Proxy re-encryption (PRE) scheme is utilized to accomplish secure information scattering in cloud computing by designating a re-encryption key related with the new recipients to the CSP. However, the information disseminator can spread the majority of the information owner's data to other people with this re-encryption key, which may not meet the practical requirement since the information owner may just allow the information disseminator to scatter a particular file. However, combining data owner and multiple co-owner privacy preferences is not a simple task because in multiparty authorization enforcement privacy conflict occurrence is expected. When the data owner has conflicting privacy policies then privacy issue will happen and it results in ensuring data is not being accessed by anyone. To overcome this issue multiparty access control mechanism has been implemented. However all of them are based on plaintext data. Here fine-grained conditional dissemination over the ciphertext in cloud computing with attribute based CPRE is proposed. The cipher text is initially deployed with the access policy appended by data owner. In our propose scheme, each owner of data can add their own preferences to their encrypted data according to their need in multiparty access control mechanism. Hence the data disseminator can re-encrypt the ciphertext when the attributes are satisfied with respect to access policies.

Goal of our work:

- To ensure data owner preferences based on access permit and data should shared among various group with security.

- ❖ At any cost data owner attributes should not fail.
- ❖ To reduce the data leakage while searching the file.
- ❖ Multi owner concept by satisfying every user priority.

II.LITERATURE SURVEY

Flexible data access in cloud based on trust and reputation

Cloud computing offers another method for administrations and has turned into a prominent assistance stage. Putting away client information at a cloud server farm significantly discharges stockpiling weight of client gadgets also, brings get to comfort. Because of doubt in cloud administration suppliers, clients by and large store their essential information in an encoded structure. Different application situations demand adaptable control on cloud information access dependent on information proprietor strategies and application requests. Either information proprietors or some confided in outsiders or both ought to deftly take an interest in this control. Be that as it may, existing work hasn't yet examined a successful and adaptable answer for fulfill this interest. Then again, trust plays a significant job in information sharing. It aides defeating vulnerability and staying away from potential dangers. In this paper, we propose a plan to control information access in distributed computing dependent on trust assessed by the information proprietor as well as notorieties produced by various notoriety focuses in an adaptable way by applying Attribute-Based Encryption and Proxy Re-Encryption. We coordinate the idea of setting mindful trust and notoriety assessment into a cryptographic framework so as to help different control situations and methodologies.

Scalable access control of encrypted data in edge computing

Edge processing has been acquainted with stretch out the distributed computing engineering to the edge of the system, which dissects a large portion of the IoT information close to the gadgets that produce and follow up on that information. Despite the fact that edge figuring takes care of the dormancy issue of information preparing, it additionally carries issues to the information security and protection conservation. One system which is potential to give versatile access control to bolster information security and protection in edge registering is quality based encryption (ABE). In this paper, we propose a crude named intermediary helped ciphertext-arrangement ABE (PA-CPABE), which redistributes the greater part of the decoding calculations to edge gadgets. Contrasted with the current ABE with redistributed unscrambling plans, PA-CPABE has a bit of leeway where the key conveyance doesn't require any protected channels. It presents a conventional development of PA-CPABE and afterward officially demonstrates its security.

SDN security

The brief overview of SDN security survey specifically investigate the potential it heats of man-in-the-middle attacks on the Open Flow control channel and also describe a feasible attack model in the open flow channel, and then implement attack demonstrations to show the severe consequences of such attacks. Additionally, to propose a lightweight countermeasure using Bloom filters. Implement a prototype for this method to monitor stealthy packet modifications. The successful attacks can effectively poison the Virtual Machine information, a fundamental building block for core SDN components and topology-aware SDN applications. With the poisoned network visibility, the upper-layer Open Flow controller services/apps may be totally misled, leading to serious hijacking, denial of service or man-in-the-middle attacks. The result of our evaluation shows that our Bloom filter monitoring system is efficient and consumes few resources.

Cloud-based outsourced storage

It describes Cloud-based outsourced storage relieves the client's burden for storage management and maintenance by providing a comparably low-cost, scalable, location independent platform. The Cloud Storage Service (CSS) relieves the burden of storage management and maintenance. To avoid the securityrisks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable Data Possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services.

III.SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

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. Unfortunately, the CSP is usually a semi-trusted server which honestly follows the designated protocol, but might collect the users' data and even use them for benefits without users' consents. On the other hand, the data has tremendous usages by various data consumers to learn the behavior of users. It is essential to adopt access control mechanisms to achieve secure data sharing in cloud computing.

DRAWBACKS OF EXISTING SYSTEM

- Data in cloud environment is not secured completely.
- Group sharing of data need more attention and access policy in cloud environment.

- Chance for leakage of user private information.

PROPOSED SYSTEM

In our proposed system, the issue discussed in multi group sharing of data in cloud has been eradicated. This concentrates on preserving co-owner privacy preferences as well as original data owner preferences and sharing a file to various groups with multi owner concept is a main objective of our work. ABE based encryption has been used to encrypt user data and stored in cloud with access control list. This access control privileges will prevent our data unauthorized user access. However once an user share their data with other users with set of attributes if any privilege modification is done by co-user then data should be re-encrypted according to his/her attributes. This is processed by proxy re-encryption scheme and it is employed to achieve secure data dissemination in cloud computing by delegating a re-encryption key associated with the new receivers to the CSP. The issue behind this existing system is once user attains particular key of the specific document there is a chance of re-accessing the file without user knowledge. Hence in our proposed RC4 encryption is implemented to encrypt the data. Once file is encrypted and stored in cloud with keyword. If user wants particular document he/she will search it using keyword. To enhance security the searched data will be available for a particular time otherwise it will be expired therefore it should be searched again. Similarly once a key is used then the same key generated using RC4 is not used to access the same file. If the file does not decrypt within the particular time it will be expired then again the user wants to send request to the data owner and new key will be generated. Hence it will ensure user privacy of data without any leakage.

ADVANTAGES OF THE PROPOSED SYSTEM

- Enhances security of user data in cloud.
- Time based decryption avoids data loss.
- Misbehaving activities does not take place through access policy.

The implementation process of our work has been described in step by step process as below,

User phase:

In this phase, we divide the user role into the following categories: data owner, data co-owner, data disseminator and data accessor. Data owner has the rights to define access policy where the disseminator verifies the condition and disseminate data by aggregating user policy needs. Then he encrypts data for a set of receivers, and outsources the cipher text to CSP for sharing and dissemination. Data owner can share to other users by tagging which states those users are co owner of the data and they have the rights to add their own policies to the file and can generate renewed cipher text. This condition has been checked and respective re encryption key is generated if and only if the user satisfies data owner access policy and these works are carried by data disseminator. The data accessor can decrypt the initial, renewed and re-encrypted cipher text with her or his private key.

Encrypting the file with timing:

In this module, data owners upload the data to cloud. Here data owner assigns access rights for file and assign co owners of data and upload it. RC4 is used to encrypt the data; once file is encrypted it is uploading with particular time interval for decrypt. This timing condition will secure data from information leakage, such as if more number of user uploads data with same keyword when new user enters and search with particular keyword it will retrieve all cipher text data and it leads to privacy issues. Therefore in this module data is encrypted with RC4 and uploaded with specific timing.

The RC4 cipher consists of two parts:

1. The Key Scheduling Algorithm (KSA), and

2. The Pseudo Random (Byte) Generation Algorithm (PRGA).

An array of 256 elements has been taken in arranged format in KSA and then uses a variable length of private key to convert the array into a pseudo random order. Once the process has been completed the array should look in a randomly arranged format. The completion of KSA is sequentially followed by PRGA and this part generates the output of one byte at a time.

Temporary keyword search :

The information proprietor creates an accessible figure content identified with a watchword and the hour of encoding as indicated by an expected access control arrangement, and redistributes it to the cloud. From that point forward, each approved information client chooses a discretionary time interim and produces a quest token for the expected catchphrase to discover the figure content. At that point, he/she sends the produced token to the cloud to run the inquiry activity. By getting the token, the cloud searches for the archives contain the planned catchphrase. On the off chance that an information client's traits set fulfills the entrance tree of the information proprietor, at that point he/she can create a legitimate hunt token. The cloud applies the created pursuit token to locate the relating cipher texts which have been scrambled in a period interim determined by the information client.

Result extraction :

In this phase, search results have been extracted based on keyword and result are retrieved to users. Even the user may authorized one he/she is permitted to decrypt the file with in particular time limit. Otherwise file time will be expired and user should request it again once generated key is expired again a new key will be generated again. The same key is not used again for decrypting files each and every key is valid for particular time limit only.

IV.SYSTEM DESIGN ARCHITECTURE

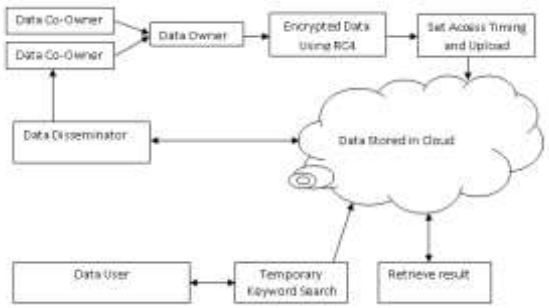

Fig 1: proposed system architecture

In our proposed work, user will select a file and store it in cloud and share the data to single or a group of users. While sharing a file the owner can assign privacy preferences and share it on cloud with it. The uploaded data will be encrypted through ABE to ensure security here attributes of owner preferences has been done through it. If co-owner of particular data wants to share he/she should satisfies the attributes policy generated by owner of data. in addition to reduce the leakage of data while searching a particular file was obtained through Temporary keyword search process here, a particular time limit will be added to the file while uploading in cloud. In case, if a user search a data in cloud it will retrieve the content that are related to that particular keyword hence there is a chance for leakage or data. So this particular time period retrieval will add much more security and protect our file from leakage because within the time it should be retrieved otherwise the file could not be accessed by the user. Similarly, once generated key could be used again to access the same file without any knowledge of that particular data owner. Therefore, random key generator has been implemented in our work to ensure that each time if a user wants to access the file he should get proper permission from that file owner.

Hence data disseminator can access the data and also generate the re-encryption key to disseminate data owner's data to others if he satisfies enough access policies in the cipher text. The data accessor can decrypt the initial, renewed and re-encrypted cipher text with her or his private key. Therefore our proposed method attains maximum performance in securing as well as group sharing of data in cloud in efficient way.

Result and discussion:

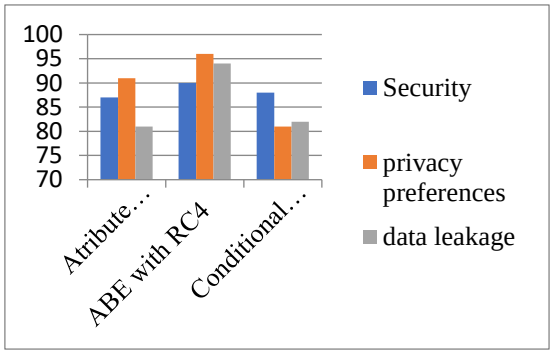

Fig 2: Performance analysis

In the above graph it shows that our proposed work attains better performance compared to other existing work. The comparison has been done based on parameters such as security, privacy preferences and data leakage based on the result our system attains better performance.

CONCLUSION

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. In this paper, we present a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the data owner could encrypt her or his private data and share it with a group of data accessors. To enhance data security in our work RC4 encryption has been deployed and it reduces the chance of accessing a file again and again using a same file key. To avoid leakage of data while searching a file from cloud temporary keyword search has been implemented. Hence it attains better performance compared to existing methods in case of privacy preferences, security and data leakage.

REFERENCES

[1] Q. Huang, Y. Yang, and J. Fu, “Secure data group sharing and conditional dissemination with multi-owner in cloud computing,”,IEEE Transactions on services computing, DOI 10.11.09/TCC.2019.2908163,2020.

[2] V. Senthilkumar, “providing security against Ip crowdsourced spoofing attacks on cloud using topoguard algorithm,” Volume 7, Issue 1, 2020.

[3] T. Poongothai, “Secure and Efficient Audit Service for Data Integrity in Cloud Storage,” International Journal of Engineering Research and Technology (IJERT), Volume 7, Issue 01, April 2019.

[4] 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.

[5] B. Lang, J. Wang, and Y. Liu, “Achieving flexible and self-contained data protection in cloud computing,” IEEE Access, vol. 5, pp. 1510- 1523, 2019.