Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Enhanced Security for Data Sharing in Clouds through Policy and Access Control Management

Dhasaratham Meghavath
Department of Computer Science and Engineering
SSSUTMS, Sehore, Madhya Pradesh - 466001, India.

Dr RP Singh
Department of Computer Science and Engineering
SSSUTMS, Sehore, Madhya Pradesh - 466001, India.

Abstract
Cloud records sharing protection, presents a better computing, with the traits of intrinsic utilization of assets. In cloud computing, cloud service carriers provide an abstraction of endless garage area for clients to host information. It can assist customers reduce their economic overhead of facts managements through migrating the neighborhood managements gadget into cloud servers. Propose a secure statistics sharing scheme, which could reap secure key distribution and data sharing for dynamic group. In this assignment, existing scheme is capable of assist dynamic organizations efficaciously, while a new user joins inside the organization or a consumer is revoked from the organization, the personal keys of the opposite customers do now not need to be recomputed and up to date. Moreover, scheme can gain comfortable consumer revocation; the revoked customers cannot be able to get the original information files once they're revoked although they conspire with the untrusted cloud. To avoid these hazards, Data Anti collusion is a way for removing reproduction copies of statistics, and has been extensively used in cloud garage to reduce storage space and upload bandwidth and at ease cloud information stored. The proposed convergent encryption model has been considerably followed for comfortable Anti collusion and to correctly and reliably control a large variety of convergent keys.

Keywords—Access Control, Privacy Preserving, Key Distribution.

Introduction

The next generation computing is Cloud computing, where we have centralized computing resources (both hardware and software) and the centralized resources are delivered as service over a network i.e. Internet, Intranet or Extranet. Cloud Computing provides huge storage, processing, applications, Operating systems, Network and various other infrastructures, all the specified features are centralized in big server called cloud server.

These features can be accessed in various shapes required by the surfer, they can access in Systems, Mobiles, Tabs and other media required. Briefly discussing the common use of cloud is a symbol of abstraction in a complex infrastructure in centralized location. Cloud computing provides trust to remote services with a user's data, software, applications, security and computations accessed in any media. Central Cloud computing consists of hardware, Software and Application resources made available on the Internet and Mobile wireless technology as managed by third party services, all the cloud servers are accessed to third party and from third party users or surfers take access to use the resources in their required form. These services typically provide access to advanced software applications and high-end networks of server computers. The next generation of computing in Internet will be cloud computing, through cloud computing we can reduce the infrastructure, maintenance of huge systems and provide green computing with one centralized system providing resources services to a wide range of users. To overcome the drawbacks of investment,

Cite this article as: Dhasaratham Meghavath & Dr RP Singh, "Enhanced Security for Data Sharing in Clouds through Policy and Access Control Management", International Journal of Research in Advanced Computer Science Engineering, Volume 3 Issue 6, 2017, Page 18-24.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

maintenance and over rid of attackers the proposed architecture is cloud architecture. The following figure shows the structure of cloud computing. The main aim and goal of cloud computing is to use the traditional supercomputingSs procedures, In supercomputing or Local Networking we place server and use all the server facilities through a connected networks. In Local networking server has a high-performance computing power and other main resources centralized, Generally it perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The same above technology is implemented to cloud computing extending the uses networks of large groups of servers typically connected various medias Internet, Wireless, These servers running at very low cost to the consumer PC or Mobile technology with specialized connections, security and resources to spread data processing and data access. This shared Cloud server and IT infrastructure contains large pools of systems and resources that are linked together for providing sharing in wide area of media. The virtualization and sharing techniques in the cloud servers are used to utilize the resources and power of cloud computing by wide area users or surfers

LITERATURE SURVEY

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data [1]. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers.

However, safety concerns grow to be the primary constraint as we now outsource the garage of information, that's possibly sensitive, to cloud vendors. To keep statistics privateness, a not unusual approach is to encrypt information documents before the customers upload the encrypted facts into the cloud [2]. Unfortunately, it's miles tough to design a cozy and efficient information sharing scheme, specially for dynamic companies in the cloud. Kallahalla et al [3] provided a cryptographic storage system that permits secure statistics sharing on untrustworthy servers primarily based on the strategies that dividing files into filegroups and encrypting every file_group with a document-block key. However, the record-block keys want to be up to date and disbursed for a user revocation, consequently, the device had a heavy key distribution overhead. Other schemes for records sharing on untrusted servers were proposed in [4],[5]. However, the complexities of user participation and revocation in those schemes are linearly increasing with the number of data proprietors and the revoked users. Yu et al [6] exploited and combined strategies of key policy characteristic-based totally encryption [7], proxy re-encryption and lazy re-encryption to attain fine-grained records get entry to control without disclosing facts contents. However, the single-owner way might also hinder the implementation of programs, in which any member within the organization can use the cloud provider to save and proportion data documents with others.Liu et al [10] provided a relaxed multi-owner information sharing scheme, named Mona. It is claimed that the scheme can obtain great-grained get right of entry to manipulate and revoked users will no longer be capable of get admission to the sharing statistics again as soon as they're revoked. However, the scheme will easily suffer from the collusion attack via the revoked consumer and the cloud [13]. The revoked user can use his personal key to decrypt the encrypted information record and get the name of the game statistics after his revocation through conspiring with the cloud. In the phase of document access, initially, the revoked consumer sends his request to the cloud, then the cloud responds the corresponding encrypted information document and revocation list to the revoked person with out verifications. Next, the revoked user can compute the decryption key with the help of the assault set of rules. Finally, this assault can cause the revoked customers getting the sharing statistics and disclosing different secrets of valid members. Zhou et al [14] provided a

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

comfy get admission to manipulate scheme on encrypted information in cloud garage via invoking function-primarily based encryption method. It is claimed that the scheme can acquire green person revocation that combines function-based totally get admission to manage policies with encryption to comfy huge information storage inside the cloud. Unfortunately, the verifications between entities aren't involved, the scheme without difficulty suffer from attacks, for instance, collusion assault. Finally, this assault can lead to disclosing sensitive statistics. Files Zou et al. [15] offered a practical and bendy key control mechanism for depended on collaborative computing. By leveraging get right of entry to manage polynomial, it is designed to reap green get right of entry to manage for dynamic businesses. Unfortunately, the comfortable manner for sharing the private everlasting portable mystery between the person and the server isn't always supported and the non-public key may be disclosed as soon as the private permanent portable secret is received via the attackers. Nabeel et al. [16] proposed a privateness retaining policy-based totally content sharing scheme in public clouds. However, this scheme is not relaxed due to the susceptible safety of commitment in the section of identity token issuance.

OVERVIEW OF PROPOSED SYSTEM

We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access control and efficiency as follows:

Key Distribution: The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.

Data confidentiality: To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

Efficiency: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the others, which means that the remaining users do not need to update their private keys

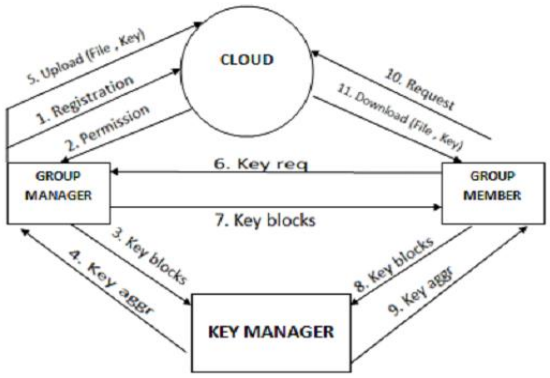


Fig 1: Cloud Based Architecture with Key Exchange

The proposed cloud based architecture provides provides various policies between data owner, user and cloud administrator. Cloud admin allots different policies to data owner based on policy key owner can share, upload and download files. The Group Key aggregation cryptosystem includes Group Key Aggregate Cryptosystem algorithm [17]. The information owner installation most people parameter using Setup and creates a public/non-public key and combines the usage of KeyGen. The mystery document is encrypted making use of algorithm. The statistics owner will make use the master-mystery to come up with combination decipherment key for a group of facts documents. The generated keys can be handed to delegates securely (through relaxed e-mails or comfy gadgets). Finally, any user with mixture key will decrypt the statistics report and down load it Fig. 1 shows the structural behaviour of gadget. In this structure, the state of affairs of users is taken for example, wherein the person-1 wants to upload the facts onto the cloud, whereas the consumer-2 wants to down load the information from the cloud. When the user-1 is importing the information or the files, the information is first encrypted the usage of the DES set of rules [14] and the record receives uploaded onto the cloud. The generated respective personal key for each

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

document is displayed as an acknowledgement to the user-1. When the person-2 desires to view or get admission to a few files of user-1, he requests the person-1 to percentage the combination key of those particular files, the use of which after downloading the encrypted documents is deciphered the use of that constant length combination key. The consumer-2 can now down load and look at all those files using the mixture key. An Group Key mixture cryptosystem produce constant length cipher texts such that efficient delegation of decryption rights for any set of cipher textual content are possible. During registration we must create the general public key and then login to the specific page. Here we will upload the documents and additionally down load the equal documents, if we're the legitimate consumer. If other character wants to get entry to the records then they must get the legitimate public key from the specific user and then they can access the decrypted records. System parameter thru Setup and generates a public/private key and integrate via KeyGen [13]. The secret file is encrypted by using the usage of information encryption general (DES). The information proprietor will use the grasp-secret to provide you with mixture decipherment key for a set of data documents. The generated keys may be passed to delegates securely (thru cozy e-mails or cozy devices). Finally, any users with mixture key will decrypted the facts record and download the record. It has the organization key aggregation method which has the importing, key aggregate generator and downloading capability. In upload module, the sender can add number of files with non-public key.

The green institution key aggregation approach is used to combine the non-public key and generate the constant sized key referred to as, the mixture key. In the down load module, the receiver can down load the record through the usage of the mixture key which is mailed with the aid of the sender. If the mixture key is legitimate, then the download for documents is authorized. While the receiver is downloading the file, the mixture key's proven or extraction of the keys is accomplished in conjunction with the ones non-public keys

IMPLEMENTATION

In this application installation is performed by means of deploying rar documents on cloud server and extracting it. The information owner executes the setup segment for an account on server which is not trusted. The setup set of rules most effective takes implicit protection parameter. This segment is done by records proprietor to generate the public or master key Pair. This segment is performed by way of any person who wants to send the encrypted information. Encrypt, the encryption algorithm takes enter as public parameters pk, a message m, and that i denoting cipher text magnificence. The set of rules encrypts message m and produces a cipher text C such that most effective a consumer that has access or permission to decrypt the message. This phase is finished through the data owner for delegating the decrypting power for a certain set of cipher text lessons to a delegate. This is executed by means of the candidate who has the decryption authorities. KAC is straightforward and at ease manner to transfer the Delegation authority.

Algorithm for Encryption

Now here comes an addition in keyagreegation. In keyagreegate, check that Qa is not equal to the identity element O and its coordinates are otherwise valid ,cipher text e=HASH(m), where hash is the same function used in the signature. To encrypt a message M having i as cipher text through key agreegate

Algorithm to generate Aggregate Key

Say S is the set of cipher text indices of those files whose aggregate-key is to be Generated. Following is the code to generate aggregate-key.

```
Extract Aggregate_key (d,S)
aggr_key = d
s <- S. size ()
i <- 1
While (i<=s)
aggr_key <- aggr_ key * S[i]
Return aggr_key
```

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Algorithm for decryption

Here comes another modification and addition in algorithm.

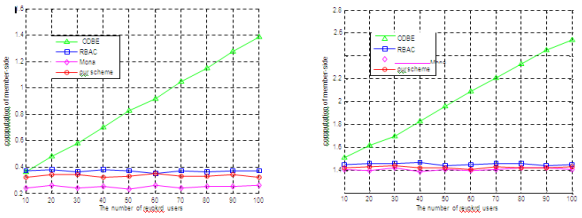
In keyagreegate, check that Qa is not equal to the identity element O and its coordinates are otherwise valid ,cipher text e=HASH(m), where hash is the same function used in the signature. To encrypt a message M having i as cipher text through key agreegate In our approach, to decrypt a set of files whose cipher te xt indices are kept in set S, following is the pseudo code of our approach.

```
Decryption(C,aggr , key,S)
S <- S.size()
i <- 1
while(S!=empty)
temp = temp * S[i]
dd = aggr_ key/temp i <- 1
while  S!=empty
derypt(key,document)
```

PERFORMANCE EVALUATION

We make the performance simulation with NS2 and compare with Mona in [10] and the original dynamic broadcast encryption (ODBE) scheme in [12]. Without loss of generality, assume the size of the data identity is 16 bits, which yield a group capacity of data files. Similarly, the size of user and group identity are also set 16 bits. Both group members and group managers processes are conducted on a laptop with Core 2 T5800 2.0 GHz, DDR2 800 2G, Ubuntu 12.04 X86. The cloud process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order.

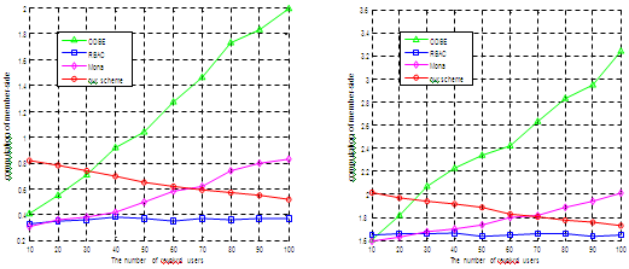
Member Computation Cost



(a) enerating a 10 MB file (b) Generating a 100 MB file

Figure 2 Comparison of various algorithms in file upload

As illustrated in figure 2, we list the comparison on computation cost of members for file upload among ODBE, RBAC, Mona and our scheme. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users. The reason is that in our scheme, we move the operation of user revocation to the group manager so that the legal clients can encrypt the data files alone without involving information of other clients, including both legal and revoked clients. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that several operations including point multiplications and exponentiations have to be performed by clients to compute the parameters in ODBE. The computation cost of members for file download operations with the size of 10 and 100Mbytes are illustrated in figure 3.



(a) Downloading a 10 MB file (b) Downloading a 100 MB file

Figure 3 Comparison of various computation cost of our scheme

CONCLUSION

In this paper, we design a protected anti-collusion facts sharing scheme for dynamic companies in the cloud. In our scheme, the customers can securely attain their non-public keys from group manager Certificate Authorities and comfy communication channels. Also, our scheme is capable of assist dynamic organizations efficiently, when a new user joins inside the organization or a user is revoked from the institution, the private keys of the other users do no longer want to be recomputed and up to date. Moreover, our scheme can gain comfy person revocation, the revoked users can't be capable of get the original information documents as soon as they're revoked although they conspire with the untrusted cloud.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Comm. ACM, vol. Fifty three, no. 4, pp. 50-58, Apr.2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-one hundred forty five, 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-forty three, 2005.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in 23 Public Key Cryptography Conf. Public Key Cryptography, http://eprint.Iacr.Org/2008/290.Pdf, 2008.

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[11] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[13] Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups within the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.

[14] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. Eight, no. 12, pp. 1947-1960, December 2013.

[15] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for relied on collaborative computing," INFOCOM 2008, pp. 1211-1219.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[16] M. Nabeel, N. Shang, and E. Bertino, "Privacy keeping coverage based content sharing in public clouds," IEEE Trans. On Know. And Data Eng., vol. 25, no. Eleven, pp. 2602-2614, 2013.

[17] B. Den Boer, Diffie–Hellman is as sturdy as discrete log for certain primes in Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science 403, Springer, p. 530, 1988.

[18] D. Boneh, X. Boyen, H. Shacham, "Short organization signature," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp.Forty one-fifty five, 2004.