ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Secure Key Distribution Using Tree Based Group Diffie-Hellman Protocol and Data Sharing for Dynamic Group

Rakesh H[1], Renukaradhya P.C [2], Priyanka H V[3]

PG Student, Department of Computer Science & Engineering, VTU, India[1]

Assistant Professor, Department of Computer Science & Engineering, VTU, India[2]

PG Student, Department of Computer Science & Engineering, VTU, India[3]

ABSTRACT: As the area of cloud computing was emerged, the systems developed for the cloud were quickly divided into three main categories of systems: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With the help of cloud computing users can achieve an efficient and cost benefit approach for data sharing among dynamic group members in the cloud with the benefit of low maintenance and little management cost. Mean while we must provide security for the exchange of group keys in a dynamic peer group with more than multiple members, we make use of tree-based Diffie-Hellman (TGDP) protocol. Each member of the group maintains a set of keys, which are arranged in a hierarchical binary tree. We assign a node id V to every tree node. For a given node, V we associate a secret (or private) key Kv and a blinded (or public) key BKv. All arithmetic operations are performed in a cyclic group of prime order with the generator. In our approach we provide a security for the exchange of keys. Second our scheme achieves fine grained access control and revoked users cannot access the cloud again and they will not be able to get the original data and manipulate the original data in the cloud. Finally our scheme can achieve fine efficiency and previous users need not update their private keys and burden for the previous users is reduced.

KEYWORDS: Cloud Computing, Tree –based Diffie Hellman, Data Sharing, Tree Node

I. INTRODUCTION

Basically cloud means data center's hardware and software's. Cloud computing provides on demand service and processing resources to the Users or devices [1]. Using cloud computing one can store, share his/ her data to other trusted parties in cloud. To protect data privacy in the cloud, sensitive data, for example, e-mails, personal health records, photo albums, tax documents, financial transactions, and so on, may have to be encrypted by data owners before they are getting to outsourcing to the commercial public cloud [2]. One of the most significant difficulties is identity privacy for the wide deployment of cloud computing. To safeguard information security, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud.

There are some problem related to secure and efficient data sharing for dynamics groups in cloud are as: Now a day's user's identity privacy is major concern. Without guarantee of identity privacy, user may not confident to store data in cloud storage. If we see on other side unconditional users identity privacy leads to snap up to privacy. In [4], [5], [6] many security scheme are proposed. In their approaches, data owners store his/her data in cloud and distribute corresponding decryption keys to authorised users but these schemes had some drawbacks related to user registration and revocation.

Secure provenance scheme [7] based on bilinear mapping technique to provide trusted evidence data forensics. [8] Proposed cipher text policy attribute based encryption technique allowing any member in group to share data with other members but revocation problem is not solved in above scheme. Fine grained access control achieving through key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

policy attribute based encryption [7].In this paper we proposed secure, efficient data sharing scheme which allow user to securely share his/her data to other by untrusted cloud server.

Secure Key Distribution using Tree Based Group Diffie –Hellman Protocol is achieved. Our scheme has some advantages includes, it provides dynamic group sharing, user revocation is made easy, computation overhead of encryption does not corresponds to number of revoked users. Any user in group can anonymously share data files to other. But any dispute will occur; data manager can reveal his/her identity by group signature. The remainder of this paper is organized as follows: Section 2 overviews the related work. In Section 3, some elementary terms are reviewed. In Section 4, the proposed scheme is presented in detail, followed by the results in section 6. Finally, we conclude the paper in Section 7

II. RELATED WORK

[1] Defines cloud refers to data centre's hardware and software. They describes obstacles and opportunities in cloud computing. S.Kamara [2] focuses on encrypting sensitive information before it is outsourced to untrusted cloud storage. They also lights on various architecture of cryptographic storage services like a consumer of cryptographic storage architecture, an enterprise architecture.[4] Kallahalla et al. proposed cryptographic cloud storage system that enables secure file sharing on untrusted cloud server and that system named as "Plutus". File get divided into file-groups and encrypting each file group with unique file block key and then data owner can share the file groups with others through lockbox key, this lockbox key generally used for encrypting file-block keys. But it has some drawbacks includes file-block keys need to be updated and distributed again for user revocation.[5] Proposed a security mechanism that improves the security of a network file system without making any changes to the file system or network server. In Sirius, files have two parts: File metadata and file data, stored on untrusted server. The file metadata has the access control information including a series of encrypted key blocks and these key blocks are encrypted under the public key of authorized users. But the size of metadata increased with number of authorized users. [10]("Revocation and tracing") solved the problem of efficient key revocation by NNL construction. But it didn't support for dynamics groups in clouds besides that computation overhead of encryption increases linearly with the sharing scale.

Proxy Re-Encryption [6] allows a proxy to transform a cipher text computed under Alice's public key into one that can be open by Bob's secret key. Using Proxy Re-Encryption scenario data owner encrypts block of content with unique and symmetric keys and further these symmetric content keys are encrypted under a master public key. For providing access control, cloud server uses Proxy Re-Encryption for directly re-encrypt appropriate contents key from master public key to allowing users public key. Due to this method malicious revoked user can read decryption keys of encrypted content blocks. In an ABE[9] system, a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. A secure, scalable and fine-grained data access control scheme [3] is based on the combination of KP-ABE, Proxy Re-Encryption, and Lazy Re-Encryption technique. KP-ABE allows data owner to delegate computation tasks for providing access control to untrusted cloud servers without disclosing actual data contents. Also user secret key updating process delegated to cloud server by group manager. So it is somewhat advantageous regarding computation overhead on server not on client side. But KP-ABE scenario did not provide multiple owner data sharing.

III. PROPOSED SYSTEM

To efficiently maintain the group key in a dynamic peer group with more than two members, we use the tree-based group Diffie–Hellman (TGDH) protocol .Each member maintains a set of keys, which are arranged in a hierarchical binary tree. We assign a node id **V** to every tree node. For a given node, **V** we associate a secret (or private) key **Kv** and a blinded (or public) key **BKv**. All arithmetic operations are performed in a cyclic group of prime order with the generator. Therefore, the blinded key of node can be generated by

$$\mathbf{BKv} = \alpha\ \mathbf{Kv} \bmod p$$

Where p is any large prime number and _ is a primitive root of p. Each leaf node in the tree corresponds to the individual secret and blinded keys of a group member Mi. Every member holds all the secret keys along its key path

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

starting from its associated leaf node up to the root node. Therefore, the secret key held by the root node is shared by all the members and is regarded as the group key. The figure below illustrates a possible key tree with six members M1 to M6. For example, member M1 holds the keys at nodes 7, 3, 1, and 0. The secret key at node 0 is the group key of this peer group

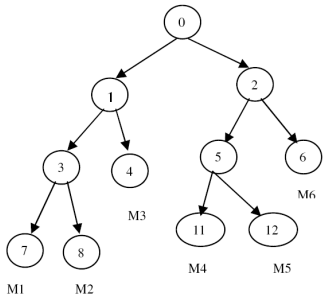


Fig 1: Tree Structure

The node ID of the root node is set to 0. Each non leaf node consists of two child nodes whose node ID's are given by 2v+1 and 2v+2 . Based on the Diffie–Hellman protocol, the secret key of a nonleaf node can be generated by the secret key of one child node of **v** and the blinded key of another child node of v. Mathematically, we have

KV = (BK2V+1)K2V+2 mod P
= (BK2V+2)K2V+1 mod P
= _ K2V+1 K2V+2 mod P

Unlike the keys at non leaf nodes, the secret key at a leaf node is selected by its corresponding group member through a secure pseudo random number generator. Since the blinded keys are publicly known, every member can compute the keys along its key path to the root node based on its individual secret key.

IV. ADVANTAGES OF PROPOSED SYSTEM

- In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
- We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
- Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
- We propose a secure data sharing scheme which can be protected from collusion attack.
- The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.

V. ARCHITECTURE

The system model consists of three different entities:

- The cloud
- A group manager
- A large number of group members

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

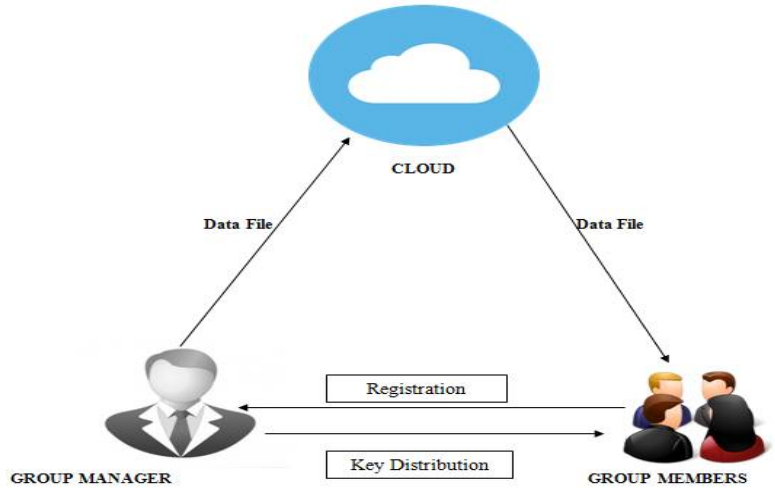


Fig 2: The System Model

- The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data.
- Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties.
- Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

It Consists of 4 Modules:

- Create cloud server Account
- CSP(Cloud Server provider) Account permission
- Manager Creating Group
- Communicate Group Without Collusion

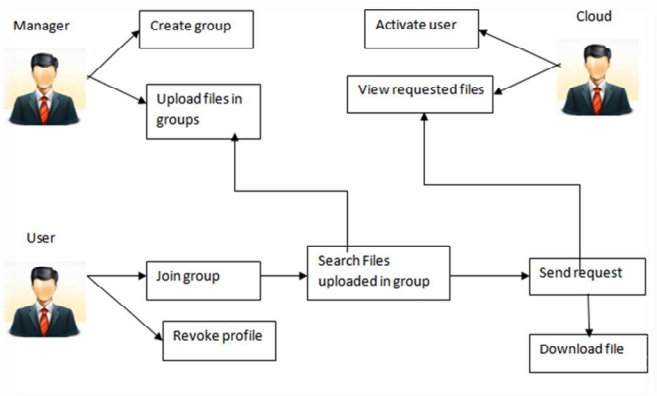


Fig 3:General Structure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

1. **Create Cloud Server Account**

- Registration:
  In this module, a user has to register first, and then only he/she has to access the data.
- Login:
  In this module, any one of the above mentioned person have to login, they should login by giving their email and password.

2. **CSP (cloud server provider) Account Permission:**

- In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers.
- To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud.

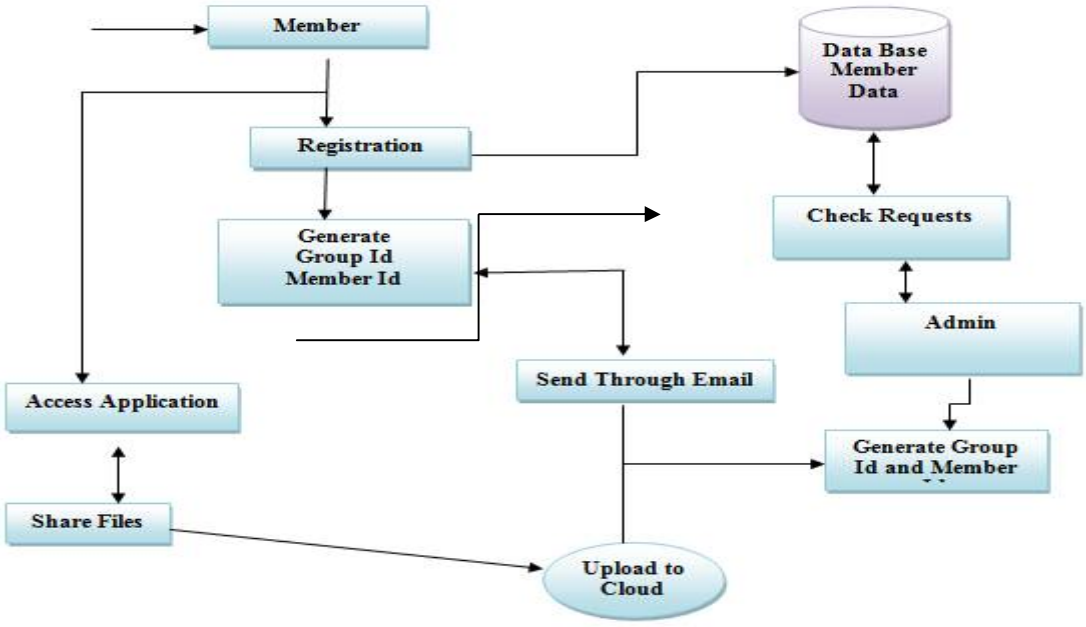
3. **Manager Creating Group**

- In this Module Manager (Owner), uploads the files (along with Meta data) into databases, with the help of this metadata and its contents, the end user has to download the file.
- The Uploaded file was in Encrypted form, only registered user can decrypt it. Even CSP can only view the encrypted file form.

4. **Communicate Group Without Collusion**

- We must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack.
- Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice.

System Architecture



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

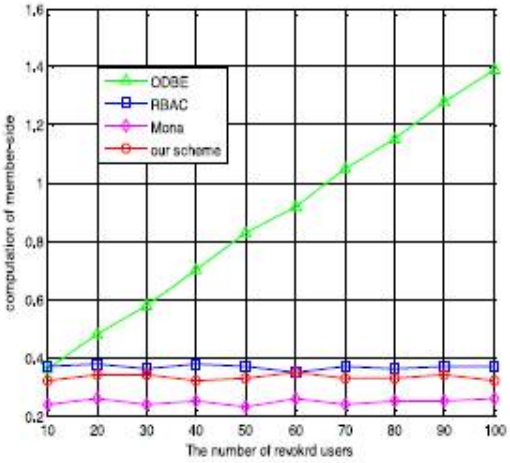
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

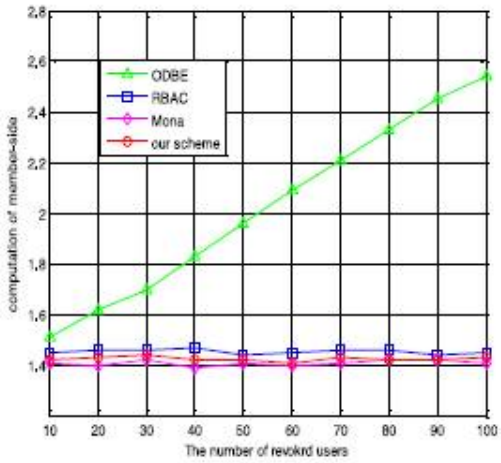
Vol. 5, Issue 3, March 2017

VI SIMULATION RESULTS

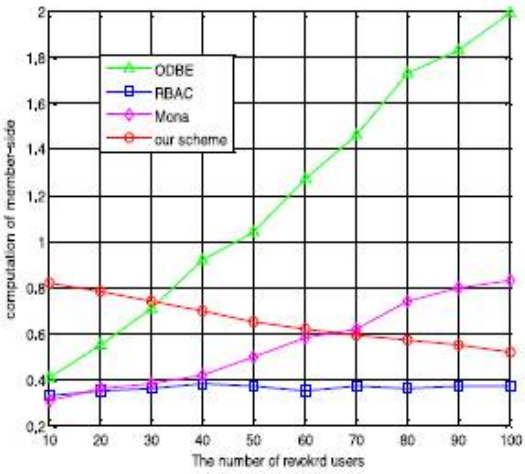
We make the performance simulation with NS2 and compare with Mona and the original dynamic broadcast encryption (ODBE) scheme . Without loss of generality, we set p ¼ 160 and the elements in G1 and G2 to be 161 and 1,024 bits, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 216 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 2 G, Ubuntu 12.04 X86. The cloud process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8 G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order.



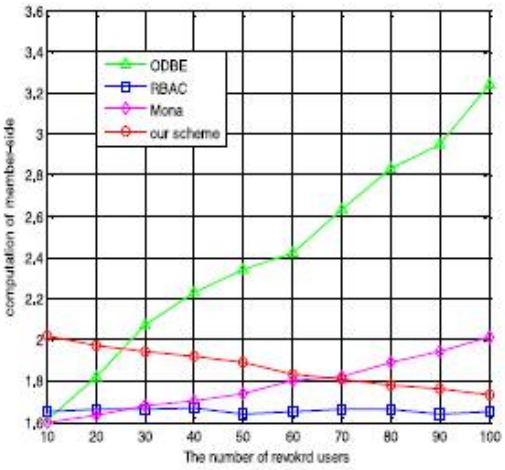
(a) Generating a 10 MB file



(b) Generating a 100 MB file



(a) Downloading a 10 MB file



(b) Downloading a 100 MB file

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

VII CONCLUSION AND FUTURE WORK

This system is design for secure data sharing scheme, for dynamic groups in an untruth cloud. A new type authentication system, which is highly secure, has been proposed in this system. User is able to share data with others in the group without disclose identity privacy to the cloud. It also supports efficient user revocation and new user joining. User revocation can be done through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. System also provides the new double encryption technique for data security. New role based encryption provides tight authentication. In our discussion , we used Tree Based Group Diffie-Hellman Protocol for security purposes. In future it can be solved with by doing research and implement with higher upcoming encryption and decryption techniques.

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," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.
[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,
pp. 29–43.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

BIOGRAPHY

Rakesh H is a final year M.Tech Student in the Computer Science and Engineering Department, Shri Devi Institute of Engineering and Technology (S.I.E.T), Tumakuru, Karnataka, India affiliated to Visvesvaraya Technological University (VTU). He received Bachelor of Engineering (B.E) degree in 2014 from Siddaganga Institute of Technology, Tumakuru, Karnataka, India. His research interests are Cloud Computing.