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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Secure Data sharing for groups dynamically in Public Cloud

Vinupriya R, Caroline kayalvizhi M, SheelaMalarvizhi M

M.Tech Student, Dept. of I.T, Muthayammal Engineering College, Rasipuram, Namakkal, Tamilnadu, India

Assistant Professor, Dept. of C.S.E, Muthayammal Engineering College, Rasipuram, Namakkal, Tamilnadu, India

Assistant Professor, Dept. of C.S.E, Muthayammal Engineering College, Rasipuram, Namakkal, Tamilnadu, India

ABSTRACT: Data security and privacy becomes more important when using cloud computing. Data owners outsource their data to the cloud for the reasons of economy, scalability and efficient accessibility. The cloud usually managed and maintained by cloud provider who considered as semi-trusted third party. So, Data owners will be a need to encrypt the data stored at cloud. With the popularity of group sharing in public cloud, the security and privacy of data at group sharing have become issues. In this paper, we propose a secure group sharing framework for public cloud. It combines GDH and TGDH together into a protocol. The Combined GDH and TGDH group sharing in which group divided into subgroups, each maintain its subgroup using Group Diffie-Hellman (GDH) and links with other subgroups using Tree-based Group Diffie-Hellman (TGDH). So Computation load is distributed among many hosts. And also support forward and backward secrecy. The theoretical and experimental analysis shows that our proposed scheme is highly secure and performs better key establishment for secure group sharing.

KEYWORDS: Group sharing, Group key agreement, Group Diffie-Hellman, Tree-based Group Diffie-Hellman

I. INTRODUCTION

In the recent years the technology has been growing and there may be tremendous changes in applications and services for various domains. Cloud Computing refers the applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services. It provide efficient access to personal files and data from any computer with internet access. This technology allows much more efficient computation by centralizing storage, memory and processing. Data security and privacy becomes more important when using cloud computing. Data owners outsource their data to the cloud for the reasons of economy, scalability and efficient accessibility. To satisfy the need for data storage and high performance computation, many cloud computing service providers have appeared, such as Amazon Simple Storage Service (Amazon S3), Google App Engine, Microsoft Azure, Dropbox and so on. There are two obvious advantages to store data in Cloud Servers: 1) The data owners save themselves out from the trouble of buying extra storage servers and hiring server management engineers 2) It is easy to data owner to share their data with intended recipients when the data is stored in the cloud. The cloud usually managed and maintained by cloud provider who considered as semi-trusted third party. So, Data owners will be a need to encrypt the data stored at cloud. Only authorized members can download it and decrypt them with given keys. Several security schemes for data sharing an untrusted servers have been proposed [4], [5]. In these approaches, data owners can store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only available to authorized users. Thus, the unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. Here the problem is how to update and distribute session keys among group members and also support to forward and backward secrecy. Group Key Agreement means that multiple parties want to create a common secret key to be used to exchange information securely. Furthermore, group key agreement also needs to address the security issue related to membership changes (join or leave the group). The membership changes requires frequent changes of group key. This can be done either periodically or updating every membership changes. The changed group key ensures backward and forward secrecy. With frequent changes in group membership, the recent researches began to pay more attention on the efficiency of group key update. Here Diffie-Hellman key agreement protocol is used which based on the difficulty of computing discrete logarithms of large numbers.it is a real time over untrusted network requires no prior secrets. In cloud, there is not possible to use a single

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

group key for the entire network because of the enormous cost of computation and communication in rekeying. So, we divide the group into several subgroups[7]; let each subgroup has its subgroup key shared by all members of the subgroup. Each group has sub group controller node and gateway node, in which the sub group controller node is controller of subgroup and gateway node is controller among subgroups. Let each gateway member contribute a partial key to agree with a common Outer group key among the subgroups. In our proposed scheme, it enables the group to update the group key pairs even though not all of the group members are online together. From the security and performance analysis, the proposed scheme can achieve the design goal, and keep a lower computational complexity and communication overhead in each group members' side.

II. RELATED WORK

Group key agreement technique which supports dynamic group membership and handles network failures. And also secure against hostile eavesdroppers [6]. The decentralized group key distribution where an existing group member is dynamically selected to act as a key server. This scheme is more robust because, if there is any partition, then a new key server can be selected by the existing members in that group. But the scalability of such scheme will still be a concern because the existing node will be additionally overloaded with the key management for all group members. To overcome the disadvantages of the existing schemes, contributory group key management scheme was proposed. The idea here is that each group member contributes an equal share to the common group key thereby avoiding the single point of failure. Steiner et al. [8], [9], [10] proposed CLIQUES protocol suite that consist of group key agreement protocols for dynamic groups called Group Diffie-Hellman (GDH). It consists of three protocols GDH.1, GDH.2 and GDH.3. These protocols are similar since they achieve the same group key but the difference arises out of the computation and communication costs. There are several works for privacy preserving data sharing issue in cloud based on various tools such as attribute based encryption (*ABE*)[11], Hybrid encryption[3].Yongdae Kim et al. [4, 8] proposed Tree-Based Group Diffie-Hellman (TGDH) protocol, wherein each member maintains a set of keys arranged in a hierarchical binary tree[2]. TGDH is scalable and require a few rounds (O (log (n)) for key computation but their major drawback is that they require a group structure and member serialization for group formation. Group has many subgroups which are connected together in tree structure [7], So Computation load is distributed among many hosts [11]. The key trees are used to efficiently compute and update the group keys and the Diffie-Hellman key exchange is used to achieve secure and distributed protocol. In this paper, we propose a combination of two protocols which uses the GDH.2 and TGDH protocols. The GDH.2 protocols are attractive because these do not involve simultaneous broadcast and round synchronization. The costs in TGDH are moderate, when the key tree is fully balanced. Therefore, these are well suited for dynamic membership in group sharing.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- Group leader (GL) create the group.
- Leader promote group member as admin
- GL Outsource Encrypted files to cloud
- Implement GDH-TGDH Protocol
- Support forward and backward secrecy
- Dynamic membership
- Manage subgroups
- Distribute computation load
- Generate Subgroup key usingGDH Protocol
- Generate Group key using TGDH Protocol
- Members decrypt the files with given keys

B. *Description of the Proposed Algorithm:*

The aim of proposed algorithm which distribute the computation load among groups. Here we use combined GDH and TGDH for secure group sharing. It divides the group divided into subgroups, each maintain its subgroup using Group Diffie-Hellman (GDH) and links with other subgroups using Tree-based Group Diffie-Hellman (TGDH). So

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Computation load is distributed among many subgroups. And also support forward and backward secrecy.A group key shared by all group members is required. Whenever a member leaves or joins the group, the group key should be updated to provide forward and backward secrecy.

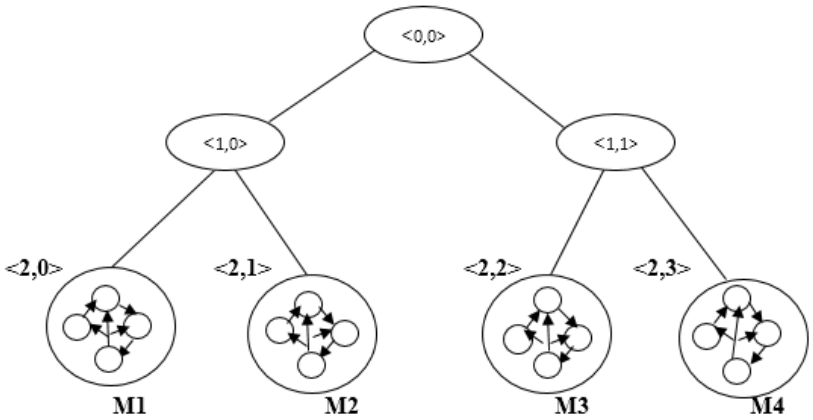

Fig.1.Combined GDH and TGDH

Forward secrecy should be guaranteed when a group member leaves, which ensure he cannot learn the new group key. Backward secrecy should be guaranteed when a newly joined members cannot learn previous group keys. GDH strongly depends on the number of current group members, since the last member in the current group becomes the sponsor or admin. The sub group controlled by sub group controller. TGDH is a distributed protocol, itrequires no centralized entity to transport secret keys.Allblinded keys in TGDH are public. Therefore, no secure channels are required in TGDH.TGDH provides key adjustment protocols to cope with the membership changes in any dynamic peer group. The TGDH provides protocols for members join, leave, merge, partition and key refresh. In combined GDH and TGDH, the binary tree used to organize the group members. Let $N(n_1,n_2,\ldots n_s)$ be the total number of group members, and $M(M_1,M_2,\ldots M_s)$ be the number of subgroup, then there will be N/M subgroups.

There are two shared keys in this group key agreement scheme. The subgroup key (SK) is used to encrypt and decrypt the messages broadcast with in subgroup members. The group key (GK) is used to encrypt and decrypt the messages broadcast among subgroup admin.

IV. SYSTEM ORGANIZATION

The main focus of this framework is secure group sharing among dynamic group and also reduce the computation load.Data owners (Group Leader) outsource their data to the cloud for the reasons of economy, scalability and efficient accessibility. To satisfy the need for data storage and high performance computation, many cloud computing service providers have appeared, such as Amazon Simple Storage Service (Amazon S3), Google App Engine, Microsoft Azure, Dropbox and so on.Data is usually encrypted before sending to the group. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. Only Authorized users (group members) can download the encrypted files and decrypt them with the given keys. The group leader can effectively grant the access of group management to one or more chosen group members.Whenever a member leaves or joins the group, the group key should be updated to provide forward and backward secrecy.

The group leader (GL) create the group and make available the data to his Group members (GM). The group leader can effectively grant the access of group management to one or more chosen group members. GL promote the group member as a Group Admin (GA).The group has many subgroups. Each subgroup maintained by using Group Diffie-Hellman (GDH) and links with other subgroups using Tree-based Group Diffie-Hellman (TGDH). In combined GDH and TGDH, generate Subgroup key (SK) using GDH and generate Group key (GK) using TGDH Protocol. The binary

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

tree used to organize the subgroups. Let $N(n_1,n_2,\ldots n_s)$ be the total number of group members, and $M(M_1,M_2,\ldots M_s)$ be the number of subgroup, then there will be N/M subgroups.

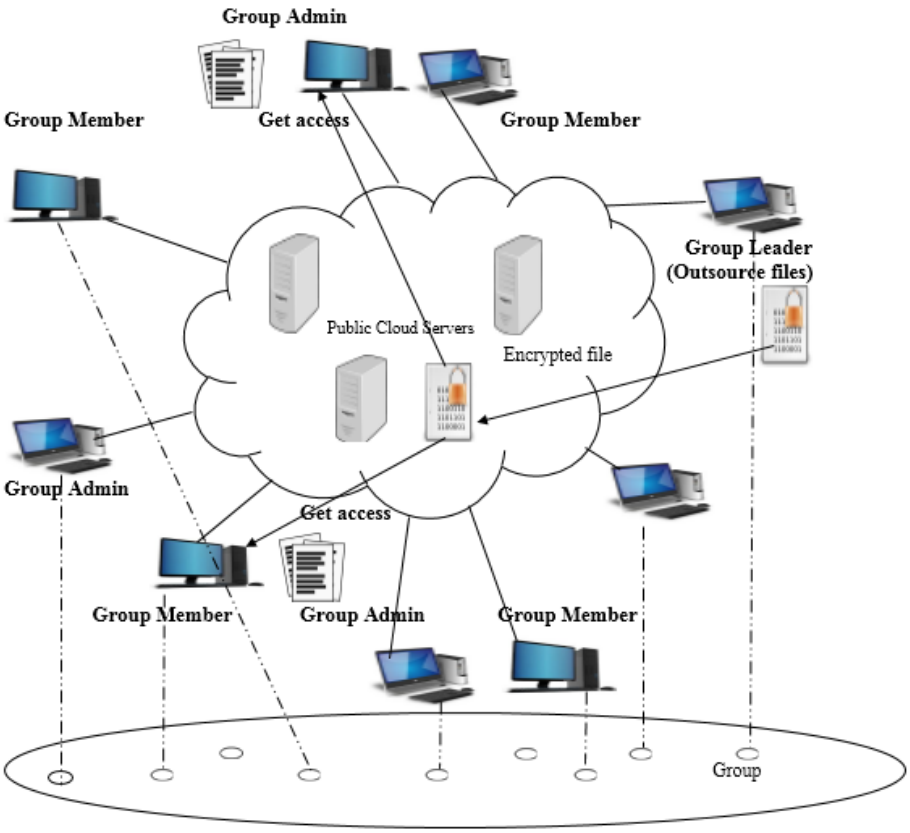

Fig.2.System Model

A. *Algorithm for combined GDH and TGDH*

1. Group formation
   N members in the group $(N=n_1, n_2,\ldots n_s)$
   Subgroup formation
   The number of membersin subgroup
   $N/M < 100$ Where, M– number of subgroup $(M= M_1, M_2, \ldots M_s)$
2. The Key Agreement Protocol (Combined GDH and TGDH) is implemented among the group members.
   It consists of three levels.
   a. Assign admin of subgroup.
   b. Using GDH to generate one common Subgroup key (SK)
   c. Using TGDH to generate one common Group Key (GK)
3. Sub group controller and Admin distribute SK,GK to its group members.
4. Key refreshed when membership changes occurs.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. RESULTS AND DISCUSSION

The experiment conducted on 10 systems running on 2.4 GHz Pentium CPU with 2GB of memory. To test this project in more realistic environment, the implementation is done by using Netbeans IDE 8.0 in network where users can securely share their data. The following figures describes the proposed algorithm shows GDH subgroups organized in TGDH.

Fig.3. GDH subgroup

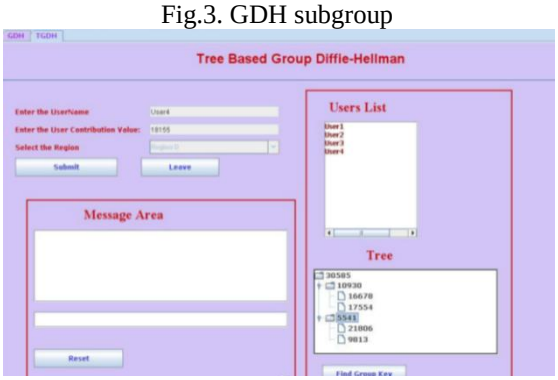

Fig.4. TGDH group

The Computational cost depends on the Serialexponentiations and the number of members joining and leaving the group. So, when the member and group size increase, the computation cost also increases significantly,When the number of subgroup increases, O (n) steps is really time consuming to build a tree.

VI. CONCLUSION AND FUTURE WORK

The Combined GDH and TGDH has been proposed which can enhance the secure group sharing using secret keys among group members. In existing scheme [1] using single key for group sharing. The proposed scheme use multiple keys which exploits asymmetric keys. Using group key agreement scheme which effectively distribute the secret key to multiple subgroups. The computation load is distributed among many subgroups and also support forward and backward secrecy. The group key updated when subgroup membership changes(join, leave) occurs. When the number of subgroup increases, O(n) steps is really time consuming to build a tree.The proposed scheme can achieve the design goal, and keep a lower computationalcomplexity and communication overhead in each groupmember's side.Compared with other schemes, the new proposed Region-Based scheme can significantly reduce thestorage and communication overheads in the rekeying process,with acceptable computational overhead.In future work, propose a new key agreement protocol which will support for subgroup increases. And construct a tree in log(n) steps using effective group key agreement algorithm in future.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

1. KaipingXue, Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing", IEEE Transactions on Cloud Computing , vol. 2, no.4, pp. 459–470,2014.
2. I. L'm, S. Szebeni, and L. Butty'n, "Invitation-oriented TGDH: Key management for dynamic groups in an asynchronous communication model," pp. 269–276,IEEE, 2012.
3. P. Tysowski and M. Hasan, "Hybrid attribute-and re-encryption based key management for secure and scalable mobile applications in clouds,"IEEE Transactions on Cloud Computing, vol. 1 no. 2, pp. 172–186, 2013.
4. 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.
5. K. D. Bowers, A. Juels, and A. Oprea,"Hail: A high-availability and integrity layer for cloud storage," in Proc. Of CCS"09, 2009, pp. 187-198.
6. Y. Kim, A. Perrig, and G. Tsudik, "Group key agreement efficient in communication," IEEE Transactions on Computers, vol. 53, no. 7, pp. 905–921, 2004.
7. K.Kumar, Dr.V.Sumathy and J.Nafeesa Begum "Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication,"IEEE, 2008.
8. Steiner.M, Tsudik.G, and Waidner.M, " Diffie-Hellman key distributionextended to group communication",Inproc of 3rd ACM conference on
9. Computer and communication security, page 31-3, May 1996.
10. Steiner.M, Tsudik.G, and Waidner.M, "Cliques: A new approach togroup key agreement",Inproc of the 18th International conference onDistributed computing systems, pages 380-387, May 1998.
11. Steiner.M, Tsudik.G, and Waidner.M, "Key Agreement in Dynamic PeerGroups", IEEE Trans. Parallel and Distributed Systems, vol. 11, no.8 Aug.2000.
12. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in CCS2006: Proc. 13th ACM Conference on Computer and CommunicationsSecurity, ser. Proceedings of the ACM Conference on Computerand Communications Security, pp. 89–98,ACM 2006.