A Novel Approach for Secure Group Sharing in Public Cloud Computing

Preeti Gulab Sonar
Student, InformationTechnology
BVCOE & RI, Nasik
Savitribai Phule Pune University

Pratibha Dattu Shinde
Student ,Information Technology
BVCOE & RI, Nasik.
Savitribai Phule Pune University

Vishakha Ashok Patil
Student, Information Technology
BVCOE & RI, Nasik.
Savitribai Phule Pune University

Rashmi Deepak Joshi
Student,Information Technology BVCOE & RI, Nasik.
Savitribai Phule Pune University

Madhuri Bhausaheb Patil
Assistant Professor,
BVCOE & RI, Nasik
Savitribai Phule Pune University

ABSTRACT
In world of Internet, the concept of group data sharing is gaining very high popularity. The privacy and security of group data sharing are the main issues which are to be considered while using this concept. Due to the semi-trust nature of the third party, it cannot be trusted and hence, security models used traditionally cannot be directly applied to the framework of cloud based group sharing. In this paper, implemented framework for a secure group sharing for public cloud, which can take the advantages of Cloud Server's help very effectively. Only difference is that the chances of data insecurity would be reduced and the threat of data being exposed to attackers and cloud provider would be reduced simultaneously. Framework is formed by combining Proxy signature, enhanced TGDH and proxy re-encryption together into protocol. The use of proxy signature technique is that the group leader can grant the privilege of group management to one or more chosen group members. With the help of cloud servers, the enhanced TGDH scheme enables the group to update and negotiate group key pairs thus all group members need not to be online all the time. By using proxy re-encryption most of intensive operations which are to be performed computationally can be handed over to the cloud servers without the threat of disclosure of any private information. The security requirements for public cloud based secure group sharing are fulfilled by our proposed scheme with high efficiency and it can be proved by the extensive security and performance analysis.

Keywords
TGDH(Tree-based Group Diffie-Hellman),PRL(Privileged revocation List), GL(Groupleader), GM(Groupmembers), GA (Groupadmin), PUDs (Personal Domains), PHR (Personal health records).

1. INTRODUCTION
In the last decade, the demand of outsourcing data is greatly increased. Data storage and high performance computation are the main needs which have to be fulfilled. These services are provided by many cloud computing service providers like Drop box, Google App Engine, Amazon Simple Storage Service (AmazonS3),etc. The advantage of storing data in cloud servers is that the data owners can reduce the overhead of buying extra strong servers and also avoid hiring of server management engineers. The technology used for internet based development is nothing but cloud computing. Cloud provider offers one of the most fundamental services that is data storage. Data encryption is a basic solution to maintain security of data and the encrypted data is uploaded into the cloud. Depending on the possibility to identify privacy and security users cannot join the cloud computing systems. As the cloud providers and attackers can easily find the real identity. Nowadays, the cloud storage has become common factor in the data storage technology. Cloud server provider can deliver the different types of services to the users such as Amazon, in cloud computing. The data storage can be provided in minimum cost at any time over the internet at the cloud computing platform. For maintaining trust between service provider and data owner, data integrity plays an important role. Cloud computing saves the cost required for implementation of different types of project in Information technology field. For providing privacy to data files Encryption is the best method and then these encrypted data is uploaded on the data servers. The data integrity can be verified of third party users is the important part of cloud data storage. The other benefit of storing data in cloud server is that it becomes easy to share the data with the intended recipients for the data owners. However, the challenges before the cloud storage cannot be overlooked. The main challenges before cloud storage are privacy and security of user's data. As known, the data owner stores his/her data in the trusted servers. These servers are controlled and managed by administrators which can be trusted fully. But the cloud is managed and maintained by Cloud providers which are also called as semi trusted third party. As a result, technologies used for traditional security storage cannot be used in cloud storage scenario. The data of data owner is desired to be shared only with intended recipients and hence it becomes more challenging to ensure that the data is shared by data owners cannot be obtained by anyone, including Cloud service providers. So that it reaches the intended recipients in a secured way.

2. LITERATURE SURVEY
Data privacy can be preserved by two solutions such as encryption of data and then upload the data that is encrypted. It is somehow difficult to design an efficient and secure data sharing between the groups. The existing system stores the encrypted data files by the data owners and the decryption keys are distributed only to authorized users. As an unauthorized users are not having any idea about the decryption keys so it cannot learn the content of data files. The complexities goes on increasing various data owners and revoked users to participate and revoke users.

As per [1] RFC2315, privacy and security of data can be provided with the encryption of data. As stated that non-adoption of end-to- end encryption may not due to the use of the issues identified by the Whitten and Tygar in their seminal paper. As investigated various issues like incomplete threat models, misaligned incentives. In our research literature as investigated evidence of a number of potential explanations for the low uptake of end-to-end encryption. Which gives us the suggestion that the availability and usability of the encrypted functions in email clients does not automatically force to increase the deployment by email users? Focus should be on building comprehensive models related to email, and email security.

As per [2] Y. Tang, P. Lee, J. Lui, and R. Perlman, has been developed the data backups for third party cloud storage services to minimize the data management costs. Also to provide the security that guarantees the data which is maintained by the third party users. Also the design and implementation of FADE, provides a security to the cloud storage system which gives the policy based access control. The another outsourced files are generated with the file accessibility terms and policies and assures to delete the files which try to make them not as recoverable to file access policies. FADE is developed using a set of cryptographic key operations which are maintained or managed by themselves such a key managers are independent of third-party clouds servers. As implemented to prove the concept of prototype of FADE such as Amazon S3, and many other cloud storage services.

As per[3] K. Ren, C. Wang, and Q. Wang developed model which allows various user to enjoy services which provided by cloud services and also providing facilities to user to store their data . It is a scalable, on demand and also easily available on internet as needed. On remote machine data is sorted by cloud. Hence it's necessary to provide more security to user from unauthorized person. For achieve this sharing they distributed storage, generated various keys and distributed secure data to user. And also performing strong cloud storage security for data and also fast data error localization.

As per[4]S. Yu, C. Wang, K. Ren, and W. Lou, developed secure, scalable, and fine-grained data access control in cloud computing. In cloud computing resources of computing infrastructure is provided services over the internet. This paradigm also provided forth challenges when user handled sensitive data for data security and access control which is not on same domain as data owners. To keep sensitive data security against untrusted servers, this solution use cryptographic methods by providing keys to the authorized users. This solution introduces key distribution and data management when data access control is desired. This goal is achieve by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption. This proposed system also has features of user access confidentiality and secret key distribution. Analysis shows that our proposed system is highly secure under existing security models.

As per [5] D.H.Tran, H.-L.Nguyen,W.Zha , and W.K.Ng, public is giving attention to some of the privacy issues online social networks (OSNs) when the users and the OSN providers are not agree when the data privacy is caused. The providers use the users' data for the commercial purposes to make the growth of their profit while the users feel that their privacy and security has been decreased by this type of the behavior. As implemented that a privacy preserving protocol for users' to share the data in online social networks in which the OSN service providers cannot get the users content while users can add or remove the social contact and it becomes more efficient to access the data. As proved that users may give permission that the OSN providers may perform the keyword search over the encrypted data for the profit and marketing purpose.

As per [6] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, "SDSM, the data and applications can be accessed by the mobile devices by using the mobile cloud computing technology. The main problems that occurs in mobile cloud computing is how to overcome the confidentiality and integrity of the users data. As implemented the framework which consists of the three main components as the Mobile Client, the Data Storage Provider and the Cloud Service Provider. The confidentiality and integrity of the mobile user's data can be ensured by this framework which minimizes the overhead processing on mobile devices.

As per ref[7]P.Tysowski and M.Hasan, developed a model of Hybrid attribute and reencryption which based on key management.which is used for secure mobile application in clouds.For economy resons outsourcing of data to cloud is good and also beneficial and also beneficial for scalability and accessibility. but technical challenges remain same in the system. One thing is curious any type of sensitive data which is stored in the cloud is protected from read in the clear by provider or cloud provider.for the processing and communication cost is minimized by resource constrained mobile devices for accessing cloud based data.

3. SYSTEM OVERVIEW

System overview contains all the description regarding system as shown in figure 1:

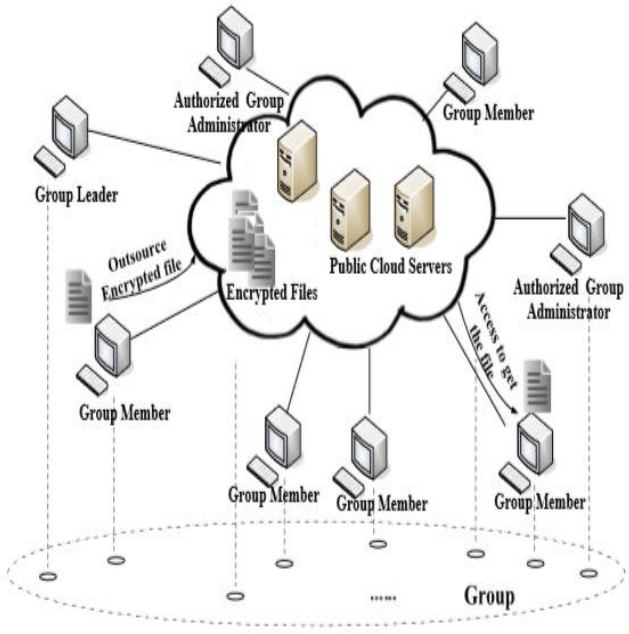

Fig 1:System Specification

Fig.1 shows that 1) The introduced scheme always supports the updating keys of the group key pair whenever the group members are living or joining takes place, without leaking the privacy of the system the computational complexity and the communication is overhead.

2) The group management can be granted by the privilege to

any of the specified group member, through which they can be revoked at any of the time.

3)TGDH can be enhanced at the original ,with the help of the cloud servers, the introduced scheme enable the group to the negotiated and the updates the group key pair even through the all of the group member are together online. Any of the offline group member can be able to launch the group key synchronization when he/she becomes online together same as the another i.e., online again at the same time.

The remaining of this paper is an organized as shown follows. In the section 2, as discussed the all system modules of our system scheme: the security model and network model. The section 3 reviews some of the related techniques preliminaries. Section 4 shows the presentation of our dynamic secure group sharing framework in the public cloud. In the section 5, As given the performance analysis an the security. Finally related work is discussed in the Section 6, and the concluded this paper in the Section7.

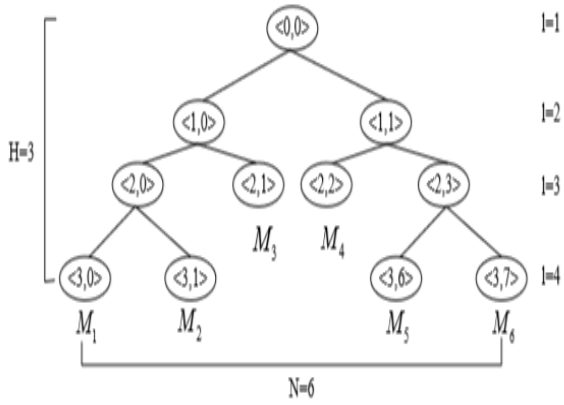

Fig 2: System Description tree

As per Fig.2 the protocol of TDGH in they uses an adaptation of the binary trees key in the following context of the fully distributed agreement of the group keys which are based on the Decisional Diffie-Hellman problem. Let the *p* and *q* be the two prime number which is satisfy the condition of q|p -1. Let the *g* would be able to generate from *G*. In TGDH protocol the binary key tree is organized a in the following system manner: the secrete key *K(l,v)* is associated with each of node(l,v) and the blinded corresponding key BK(l,v) = g^k(l,v) mod p. The internal node (l,v) of the each secret key K(l,v) is the Diffie-Hellman are exchanged the key between its own two child nodes.

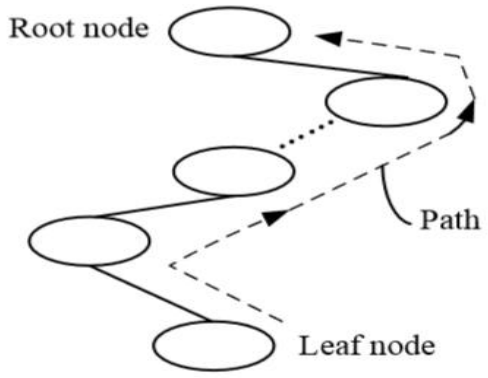

Fig 3: Path from leaf node to root node

As shown in fig.3 the data of our framework flows in the form of bottom to up format. Same as there is the leaf node and the root node present in the form of system. The system data flows from leaf node to root node and any of the node gets failed in between the framework that will affect our system immediately and because of this data can be lost.

4. ALGORITHMS

Storage and computing resources obtaining from cloud provider, for group initialization to initialize a binary tree and some related security information of the group, the group leader GL implements the phase. Private Key of each leaf node can be unicast by GL which associated with group members under encryption. Group private key can be computed by each group members and by the help of server storage. Leaving members and joining members are divided into sub-phases like member joining, member leaving and group admin leaving. To update security information of group group members, group admin, new joining group members interact with each other.

Key part of enhanced TGDH is key synchronizing in our frame. How to securely upload and download file in the group is describes by the

Data Sharing Management.

Steps:

Encryption:
Converting original plain text into cipher text is called process of Encryption.
Steps:
1.The user who want to store the data with anyone then cloud service provider give or transmit the public-key (n,e) to that user.
2. Then data is mapped by using an agreed upon reversible protocol in to the integer, that process known as padding scheme.
3. Data is encrypted and the cipher text c is c = me (mod n).

4. By the cloud service provider cipher text or encrypted data is stored.

Decryption:

Process of converting cipher text to the plain text is known as Decryption.

Steps:

1. For the data cloud user request the cloud service provider.

2. Authenticity of the user verify by cloud service provider and providing encrypted data.

3. The data is decrypts by the cloud user and also by computing, m= Cd (mod n).

4. After obtaining, user obtaining the original data by reversing the padding scheme.

Key Generation:

Key generation is done before the data is encrypted.

Steps:

1. Select two distinct prime numbers a and b.

2. Compute n = a * b.

3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).

4. Select an integer e, like that 1 < e < Ø (n) and greatest

Common divisor of e, Ø (n) is 1. Now e is as Public-Key exponent.

5. Now determine d as: d = e-1(mod Ø (n)) i.e., d is multiplicate inverse of e mod Ø (n).

6. d is take as Private-Key component, d * e = 1mod Ø (n).

7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).

8. The Private-Key having of modulus n and the private exponent d, this must be kept secret i.e., (d, n).

5. MATHEMATICAL MODULE

Formulas Used In System:

K (l;v) =BK (l+1;2v+1) ^K (l+1;2v) mod p
=BK (l+1;2v) ^k (l+1;2v+1) mod p
=g^K (l+1;2v) K (l+1;2v+1) mod p

p=any prime number

k=key

(l,v)=Is the Diffie-Hellman exchanged key between its two child nodes and can be computed recursively

G=infeasible computational and subgroup with order q of finite field Z.

Formulas used for finding secrete keys (l;v) of the internal nodes(l,v)

Let S be a system that sharing the Data or Files in groups with privileges and special permissions with encryption where S {O, K, A, P}.

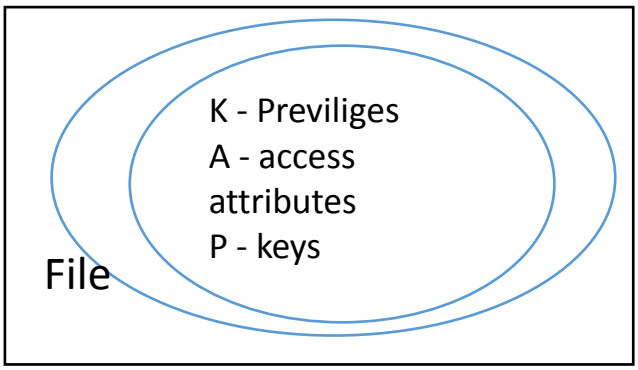

Fig 4: Mathematical Description of dynamic secure group sharing

S {O, K, A, P}

O {01, 02, • • •, 0m} objects ; data, **Files**, programs, subjects

K {K1, K2, • • •, Kr} categories: special access privileges

A {r, w, e, a, c} access attributes ; read, write, append, execute, and control

P {P1, P2, • • •, Pr} Private Key (PKi) used for encryption & description mechanism.

6. CONCLUSION

In this paper, a secure data sharing scheme is designed. The management of secure group sharing can be given to various group members. All the data or files to share are securely stored and protected in the cloud servers.TGDH scheme is used for the group members for leaving or joining the group. As all the group members are online at different time still the system works well. It also supports efficient user revocation and new user joining. . A new type authentication system, which is highly secure, has been stated in this paper. The system provides a secure channel of communication between communicating entites.To achieve the design of the goal the system the security and performance analysis of the system do well, it becomes less complex and communication becomes easy.

7. REFERENCES

[1] RFC2315, "PKCS #7: Cryptographic message syntax(version 1.5)," http://www.ietf.org/rfc/rfc2315.txt, Mar 1998.

[2] Y. Tang, P. Lee, J. Lui, and R. Perlman, "Secure overlay cloud stor- age with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903–916, 2012.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," Ieee Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM 2010: Proc. The 29th Conference on Computer Communications. IEEE, 2010.

[5] D.H.Tran,H.L.Nguyen,W.Zha,andW.K.Ng,"Towardssec uri- ty in sharing data on cloud-based social networks," in ICICS 2011: Proc. 8th International Conference on Information, Communications and Signal Processing. IEEE CS, 2011.

[6] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing," in WKSHPS 2011: Proc. 2011 IEEE Conference on Computer Communications Workshops. IEEE CS, 2011, pp. 1060–1065.

[7] P. Tysowski and M. Hasan, "Hybrid attribute-and re-encryption- based key management for secure and scalable mobile applica- tions in clouds," IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172–186, 2013.

8. AUTHOR'S PROFILE

Preeti Gulab Sonar she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of Computer Security

Pratibha Dattu Shinde she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of Cloud Computing.

Vishakha Ashok Patil she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of Cloud Computing.

Rashmi Deepak Joshi she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of Computer Security.

Madhuri Bhausaheb Patil she is Master student in the RTU, Kota. Currently working as an Assistant Professor in Brahma Valley College of Engineering And Research Institute, Nasik. Her research focuses on Data mining.