ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

GROUP KEY MANAGEMENT AND SHARING PROTOCAL IN CLOUD COMPUTING ENVIRONMENT

Dr. NAVEEN REDDY NEMILI [1], GUDISE MANASA [2], SINGAM VAISHNAVI [3], KOLLU NAVEEN REDDY [4], BATTINENI ESWAR [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The large-scale sharing needs of many enterprises promote the development of cloud storage. While the cloud computing stores the shared files outside the trust domain of the owner, the demands and concerns for file security is arising. In this project, a Group Key Management Protocol for file sharing on cloud storage (GKMP) is proposed. Faced with network attacks from public channel, a group key generation scheme based on mixed encryption technology is proposed. And a verification scheme is used to prevent shared files from being attacked by the collusion attack of cloud providers' and group members'. Security and performance analyses indicate that the proposed protocol is both secure and efficient for data sharing in cloud computing. The secured group communication is vital for protecting shared resources and ensuring authorized access. Group key management and sharing protocols play a critical role in maintaining the data security by enabling efficient and secure key distribution among group members. Cloud computing is a model where in resources on the Internet establish a resource pool and may be dynamically assigned to diverse applications as well as services.

Index Terms – Cloud storage, group key management, file sharing, cloud computing, group key management protocol (GKMP), mixed encryption, secure file sharing, key distribution, collusion attack prevention,

access control, data security, cloud security, cryptography.

I. INTRODUCTION

FACED with today's innovative blow-up of cloud technologies, rebuilding services in terms of cloud have become more popular. In a shared-tenancy cloud computing environment, data from different clients which can be hosted on separate virtual machines may reside on a single physical machine [1]. Recent news shows that Google provided the FBI all the documents of one of its users after receiving a search warrant, but the users have not been aware of the search until they are arrested. Because cloud provider has the full access to the data, the privacy of data could be violated if user's data is intercepted or modified by the cloud provider. A common way to guarantee privacy is encrypting and authenticating the shared files [2].

There is a series of cryptographic schemes [3] under such circumstance that a third-party auditor is able to check the availability of files while nothing about the file leaks. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. The cloud users are motivated to encrypt their files with their own keys before uploading them to the cloud server.

The challenge is how to share and manage the cryptographic keys among valid users without the participant of the cloud provider. These group permissions are typically used to secure the keys of data encryption. We can observe that how to securely share data files in a multiple-owner manner for groups while preserving identity privacy from a distrust cloud remains to be a challenging issue.

II. RELATED WORK

A. Audit-Free Cloud Storage via Deniable Attribute-Based Encryption

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access.

All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage

providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

B. *Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation*

Data outsourcing is a promising service for data owners, where their data are stored on a cloud storage provider. Since the cloud is not fully trusted, data access control has challenging issue in the Cloud Storage System (CSS). In this paper, we propose a novel revocable Multi-Authority CP-ABE scheme, in which the access policy can be constructed as an arbitrary tree rather than a matrix used by existing schemes. The tree-like policy makes our scheme more flexible. Consequently, the encryption, decryption and attribute revocation operations are also more efficient. Our scheme is also proved to be secure under the standard assumption. It can resist user collusion attack, while the attribute revocation operation also achieves both forward security and backward security. Simulation results show that our scheme is highly efficient.

C. *Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing*

Recently in Dependable and Secure Computing (TDSC). proposed a new construction of attribute-based encryption (ABE) which can outsource the complicated encryption task to Encryption Service Provider (ESP) in a verifiable manner. Despite the authors claimed that the results of the outsourced encryption can be checked by the user, we show that Ma et al.'s proposal fails to provide the verifiability property for outsourced encryption, the most essential security goal that a verifiable computation scheme should achieve. Specifically, by giving concrete attacks, we demonstrate that the ESP can return forged intermediate ciphertext to the user without being detected.

D. *Fine-grained data sharing in cloud computing for mobile devices*

Due to the convenience, the data sharing in cloud computing via mobile devices has become more and more popular. However, data confidentiality and online computational cost still present practical concerns to the deployment of data sharing in cloud computing for mobile devices. Existing data sharing protocols in cloud computing either cannot support the flexible sharing style for the encrypted data, or suffer from massive

online computational cost that scales with the complexity of the access policy. In this paper, to cope with these challenging concerns, we propose a new data sharing protocol for cloud computing by using a new cryptographic primitive named online/offline attribute-based proxy re-encryption and the transform key technique. To the best of our knowledge, the proposed data sharing protocol is the first one featuring with fine-grained access control, flexible sharing, data confidentiality, At last, extensive analysis shows that our proposed data sharing protocol is secure in terms of data confidentiality, and suitable for mobile devices in terms of online computational cost.

III. PROPOSED METHODOLOGY

In Group key management and sharing protocols play a critical role in maintaining the data security by enabling efficient and secure key distribution among group members. Cloud computing is a model wherein resources on the Internet establish a resource pool and may be dynamically assigned to diverse applications as well as services. Enhanced Security:

Uses advanced encryption techniques to ensure secure group communication and protect sensitive data. Efficient Key Management: Generates, distributes, and updates group keys efficiently with minimal computational overhead.

Reduced Rekeying Cost: Minimizes the time and communication required for key updates when members join or leave the group. High Scalability: Supports a large number of users without significantly affecting system performance. Low Communication Overhead: Requires fewer message exchanges for key distribution, reducing network bandwidth usage. Improved Performance: Optimized key management algorithms reduce processing time and improve the overall efficiency of the system. Strong Access Control: Ensures that only authenticated and authorized users can access group resources and shared data. Resistance to Security Attacks: Protects against unauthorized access, key leakage, replay attacks, impersonation attacks, and other common security threats. Efficient User Addition and Revocation: Allows users to be added or removed quickly without affecting the security of the remaining group members. Reliable and Fault-Tolerant: Reduces dependency on a single key management entity, improving system reliability and availability.

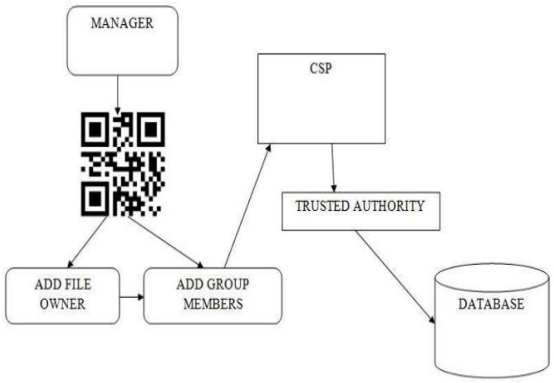


Fig. 1: System Overview

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

2. Manager

With a user ID and password, the manager can log in. A QR code is generated by the manager. the qr code it will generate a password like otp. The otp has a verify then the manager has a login with a user id and password. The manager has an approve a group member and the manager has an approve a file owner. The control of project is a manager.

3. File Owner

The file owner has a register with a detail. For login it will takes permissions of the manager has a approve then login. File owner has an upload a file and then sees all uploaded documents.

4. Group Members

The information user module has a register with all details and then takes a permission of a Manger after approve then login. Group member has a search a file .For the Search will have a match keyword. The keyword has a verify then it has a send. After verify the download a file owner what would have uploaded.

5. Trusted Authority

The trusted authority has a login with a user id and password. The trusted authority has a verify a data. The trusted authority has a share a key to the file owner data.

6. CSP

The CSP has with user id it will generate a password randomly. The CSP has a data attacker info. The CSP has a file owner info. The CSP has a group member info details.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed Group Key Management Protocol (GKMP) provides secure and efficient file sharing in cloud computing environments. The mixed encryption-based group key

generation mechanism ensures secure key distribution, while the verification scheme effectively prevents collusion attacks by cloud providers and malicious group members. Performance analysis demonstrates low communication overhead and efficient group key management with strong data confidentiality. Overall, the proposed protocol offers a reliable and scalable solution for secure group communication and cloud-based file sharing.

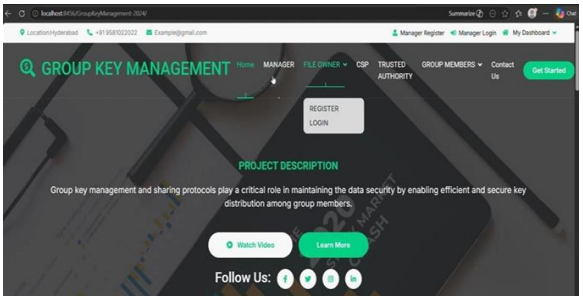


Fig. 2: Home Page

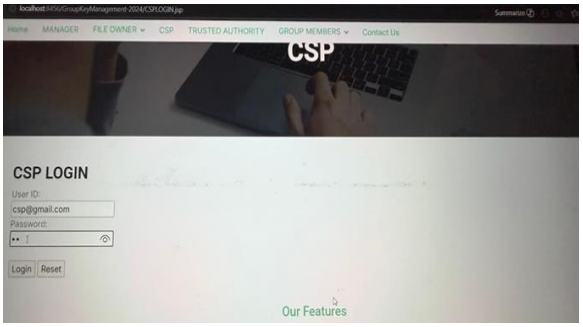


Fig. 3: Login

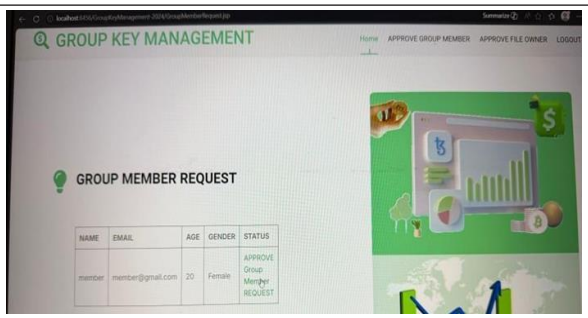


Fig. 4: Group Member Request

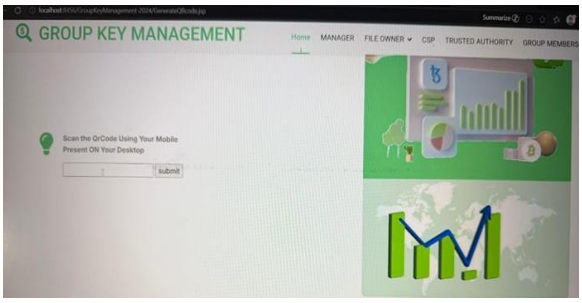


Fig. 5: Group Key Management

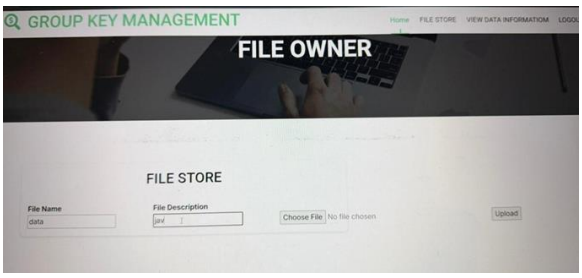


Fig. 6: File Store

V. CONCLUSION

In this paper, we propose a novel group key management protocol for file sharing on cloud storage. Public key is used by GKMP to guarantee the group key distribute fairly and resist attack from compromised vehicles or the cloud provider. We give detailed analysis of possible security attacks and corresponding defense, which demonstrates

that GKMP is secure under weaker assumptions. Moreover, we demonstrate the protocol exhibits less storage and computing complexity.

REFERENCES

[1] Po-Wen. C, Chin L, ”Audit-Free Cloud Storage via Deniable AttributeBased Encryption”, IEEE Transactions on Cloud Computing,vol.6, no.2, pp. 414-427, 2018.

[2] J. Zhou et al., "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation", Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.

[3] J.Wu, Y.Li, T.Wang, et al. CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing,IEEE Access, vol.7, pp.160482-160497, 2019.

[4] Hu.X, Jianfei.S, "Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", IEEE Transactions on Dependable and Secure Computing., vol. 14, no.4, pp. 461-462, Aug.2017.

[5] J. Shao, R. Lu, X. Lin, "Fine-grained data sharing in cloud computing for mobile devices", Proc. IEEE Conf. Comput. Commun. (INFOCOM), pp. 2677 2685, Apr./May 2015.

[6] R. Ahuja S. K. Mohanty K. Sakurai "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing" Comput. Elect. Eng. vol. 57 pp. 241-256 Jan. 2017.

[7] S.Roy, A.K.Das, S.Chatterjee, etal, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications" IEEE Transactions on Industrial Informatics vol. 5 no. 1 pp. 457-468 Jan. 2019.

[8] Z. Fu X. Sun S. Ji G. Xie "Towards efficient content-aware search over encrypted outsourced data in cloud" Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM) pp. 1-9 Apr. 2016.

[9] M. Blaze. ”A Cryptographic File System for Unix”, 1st ACM Conf. Comp. and Commun. Sec., 1992,11,pp 9-15.

AUTHORS Profile



Dr. NAVEEN REDDY NEMILI has received his MCA from Osmania University, Hyderabad in 2010, M.Tech degree in Computer science from JNTUH, Hyderabad in 2014 and Ph.D degree awarded in Computer Science from SSSUTMS, Madhya Pradesh in 2024 He is dedicated to teaching field from the last 12 years. His research area Cloud Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. GUDISE MANASA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. SINGAM VAISHNAVI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KOLLU NAVEEN REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. BATTINENI ESWAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.