An Efficient Group Key Management Using Cloud Computing

Gayatri Shinde[1], Priti Patil[2], and Rutuja More[3], Mrs.R.R.Gaur[4]
UG Student, Nanasaheb Mahadik College of Engineering, Peth
Assistant Professor, Department of Computer Science and Engineering, Nanasaheb Mahadik College of Engineering, Peth

Abstract- — the large-scale sharing of files is done with the help of cloud computing. While the cloud computing stores the files outside of trust domain of the owner so here security issue comes of files. In this paper our approach is to use a bunch Key Management Protocol for sharing of files. Round-faced with network attacks from public channel, a bunch key generation theme supported mixed secret writing technology is projected. The approach is to protect the files from being attacked by cloud providers and cloud members. Security and performance analyses indicate that the projected protocol is each secure and economical for knowledge sharing in Cloud computing. Here we will produce internet application which will generate groups as a user management like making teams. Once admin desires to share any documents inside teams with the assistance of cloud storage admin will assign security for that document and share the document. Here we will use secret writing decoding for viewing document.

Index terms- **Cloud Computing, Group Key Management**

I. Introduction

With the speedy development of cloud computing, additional individuals are returning to like moving each the massive burden of information storage and computation overhead to the cloud server in a very cost-effective manner. In spite of the advantages of cloud computing, secure knowledge access management remains one among the major difficult obstacles since the cloud server isn't absolutely trusted by the information user and also the data keep within the cloud may contain sensitive info. Hence, to safeguard the user's privacy and supply knowledge confidentiality, data owner has to inscribe the information before outsourcing the information to the cloud. Moreover, fine-grained get entry to control live at the outsourced touchy information is moreover favored from the point of view of statistics proprietor with a purpose to percentage the statistics with different customers WHO have certain attributes. For example, to alleviate the storage and computation burden, the personal health record (PHR) service Provider may assist the third-party cloud server to store the data. As the PHR data may include sensitive information, it should be guaranteed that only the doctor who is treating the patient has the privilege to access the data. A possible and practical cryptographic tool to provide confidentiality and impose fine-grained access control on Sensitive data is attribute-based encryption (ABE) which encrypts the plaintext with a set of attributes (Key Policy ABE) or an access policy (Cipher text-Policy ABE). However, in addition to data confidentiality and fine-grained access control, it is also essential that the access control mechanism has the ability to support anonymous authentication.

II. Related work

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 computingenvironment, data from different clients which can be hostedon separate virtual machines may reside on a single physical machine [1]. Under this paradigm, the data storage and management are under full control of the cloud provider, sodata owners are left vulnerable and have to solely rely onthe cloud provider to protect their data. Recent news showsthat Google provided the FBI all the documents of one ofits users after receiving a search warrant, but the users havenot been aware of the search until they are arrested. Becausecloud provider has the full access to the data, the privacy ofdata could be violated if user's data is intercepted or modified by the cloud provider.

A common thanks to guarantee privacy is encrypting and authenticating the shared files [2]. There's a series of cryptographically schemes [3] underneath such circumstance that a 3rd party auditor is ready to visualize the supply of files whereas nothing regarding the file leaks. Likewise, cloud users in all probability won't hold the article of faith that the cloud server is doing an honest job in terms of confidentiality. The cloud user's area unit actuated to inscribe their files with their own keys before uploading them to the cloud server.

The remaining challenge may be a thanks to share and manage the crypto graphical keys among valid users whereas not the participant of the cloud provider. on paper, access management [4] and cluster key management [5] [6] may be used for key management on file sharing. However, some distinctive options of cloud storage introduce new issues that haven't been totally thought of [7] [8]. Firstly, shared files square measure transmitted via the network and therefore the files could also be intercepted by varied network watching. simply mistreatment access management on the cloud storage cannot totally

address this drawback. Secondly, cluster key management depends on the cloud supplier to manage the cryptography key. which will forestall the shared files from intercepting by the network, whereas the shared files may be intercepted by the cloud supplier.

The security of storage systems has continuously been a district of active analysis. There square measure several actual systems, like CFS [9] and NASD [10]. CFS is ready-made towards single-user workstations and relied on user-supplied passwords for encryption. NASD proposes a distributed system comprising intelligent disks and users equipped keys as proofs of authorization. Approaches like NASD and SNAD [11] focus principally on securing network traffic and preventing out-side attacks.

Huang et al. introduced a novel public key encryption with authorized equality warrants on all of its cipher text or aspecified cipher text. To strengthen the securing requirement,Wu et al. proposed an efficient and secure identity-based encryption scheme with equality test in cloud computing.Xu et al. proposed a CP-ABE using bilinear pairingto provide users with searching capability on cipher text and fine-grained access control. He et al. proposed a schemenamed ACPC aimed at providing secure, efficient and fine-grained data access control in P2P storage cloud. Recently, Xue et al. proposed a new framework, named RAAC,to eliminate the single-point performance bottleneck of the exiting CP-ABE based access control schemes for public cloud storage. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy.

III. Proposed Work

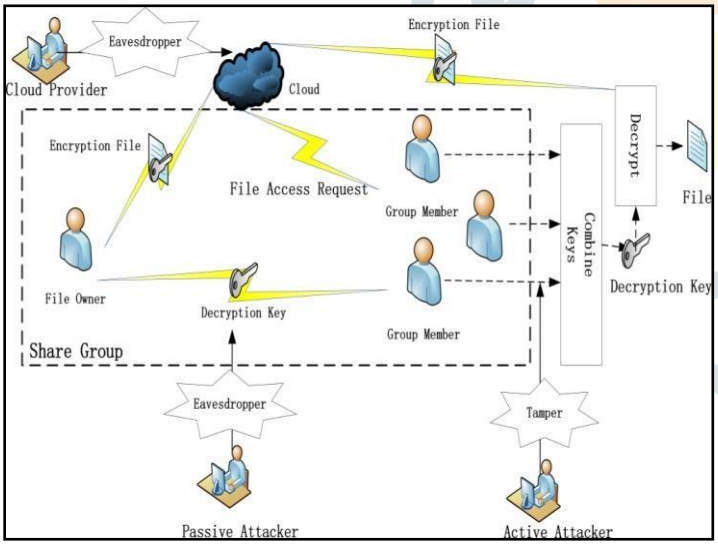

Fig. System Architecture

In this system HTML, CSS, JavaScript as a front end with the C#. NET Technology and MY SQL as a Backend database server.

GOALS

Our general goal is to develop an efficient group key management protocol for file sharing on cloud storage; the resulting techniques should be able to confront two main problems. One is ensuring that the content of the shared files cannot be learned by the unauthorized peoples. The other is protecting the files against disoperation by the cloud provider and interception by the network.

SHARE MODEL

Users WHO need to share files represent a sharing cluster; every sharing cluster is managed by the cloud supplier. each partaker within the sharing cluster owns a try of key accustomed method the communication message. The general public secret is managed by the cloud supplier, whereas the non-public secret is solely notable by the sharers. Whenever a partaker desires to share his file inside the cluster, it ought to generate a cluster key and write in code the file with the group key before transmission the file to the cloud. Then he uses a key distribution theme to distribute the cluster key to the opposite cluster sharers while not the participation of the cloud supplier. Sick the cluster key desires the collaboration of all the cluster members.

THREAT MODEL

Three kinds of adversary may threaten our protocol. The first is the cloud provider or passive adversary who only gathers information but does not affect the behavior of the group members in the communication. The second is the positive adversary who could alter the output information as a file sharer. The last is adaptive adversary who could compromise one or more group sharers and with the ability of gathering and alter the compromised ones' output information. Our goal is that once passive adversary or positive adversary is detected, our protocol will be terminated while the adaptive adversary has to compromise n group members to defeat our protocol, where n is the quantity of the group members.

The purpose of key share protocol is to distribute a group key to group members, and the other members cannot get any information of the key. In our approach, the file owner broadcasts a message, and all the group members can derive the key from the message. We propose an approach with been received from which has the combination of AES and RSA, AES is used to encrypt the shared file and RSA is used to encrypt the broadcast message. Suppose that U1 wishes to share a file F to U2, U3, ...Un.

IV. Results

1. Admin Group Master

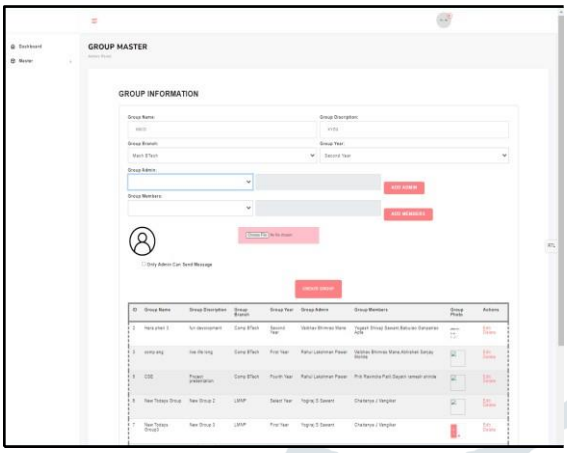

Fig. Admin Group Master

2. Admin Staff Master

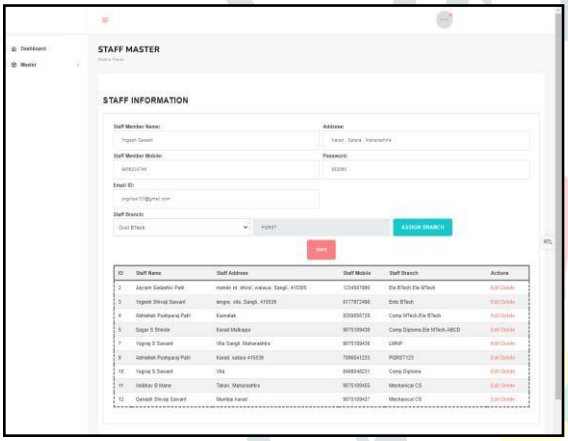

Fig. Admin Staff Master

3. OTP on Mail

Fig. OTP on Mail

4. OTP on SMS

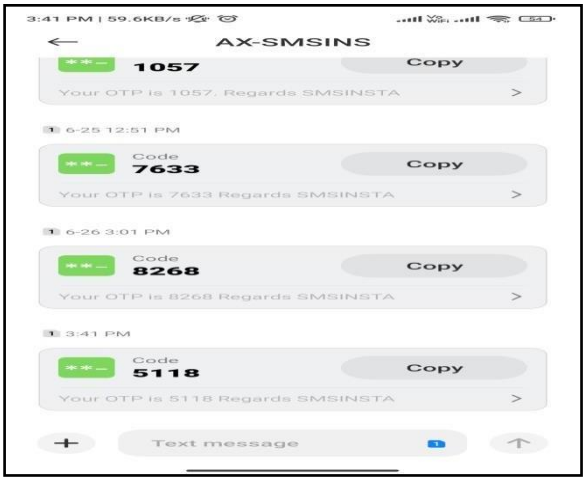

Fig. OTP on SMS

5. Verify Key

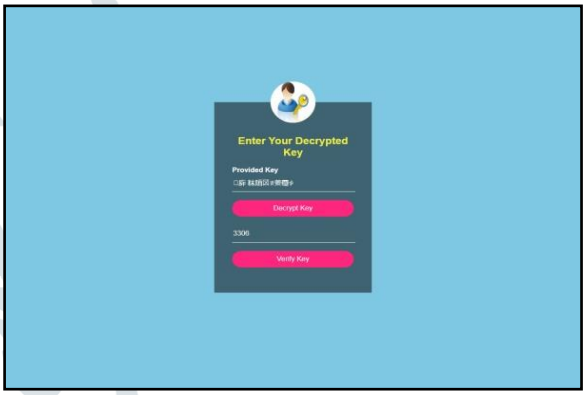

Fig. Verify Key

6. Final View

Fig. Final View

V. Conclusion

We have proposed novel cluster key management protocol for file sharing on cloud storage. Public key square measure used by Group Key Management Protocol to ensure the cluster key distributes fairly and resist attack from compromised vehicles or the cloud supplier. We provide careful analysis of potential security attacks and corresponding defense, whichdemonstrates that Group Key Management Protocol is secure below weaker assumptions. Furthermore, we have a tendency to demonstrate the protocol exhibits less storage and computing quality. Here we have used the group key management protocol with security. Admin can create the groups and admin will add the users like students and teachers into the groups and when admin is going to share the files like pdf ppt video it will add some encryption techniques to sharing of files so that it can't be available to other people apart from that group.

VI. Reference

[1] K. V. Pradeep1, V. Vijayakumar,1 and V. Subramaniyaswamy2," An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management
in Cloud Environment", 2021

[2] C. Xiao and Y. Li, "Analysis on the influence of the epidemic on the education in china," in 2020 International Conference on Big Data and Information Education (ICBDIE), 2020.

[3] A. Khattar, P. R. Jain, and S. M. K. Quadri, "Effects of thedisastrous pandemic covid 19 on
learning styles, activities and mental health of young indian studentsa machine learning approach," in 2020 4th International Conference on Intelligent Computing and Control system (ICICCS), 2020.

[4] A. S. Won, J. O. Bailey, and S. Yi, "Work-in-progress—learning about virtual worlds in virtual worlds: How remote learningin a pandemic can inform future teaching," in 2020 6th International Conference of the Immersive Learning ResearchNetwork (iLRN), 2020.

[5] Y. Safsouf, K. Mansouri, and F. Poirier, "Smart learning environment, measure online student satisfaction: a case study in the context of higher education in morocco," in 2020International
Conference on Electrical and Information Technologies (ICEIT),2020, pp. 1–5.

[6] J. Romero-Rodrıguez, I. Aznar-Dıaz, F. Hinojo-Lucena, and G.
Gomez-Garcia, "Mobile learning in higher education: Structural equation model for good teaching practices," IEEE Access, 2020.

[7] M. Sumathi & S. Sangeetha, "A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography",2019

[8] 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.

[9] 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.

[10] Q. Xu, Chengxiang Tan, Zhijie Fan, Wenye Zhu, Ya Xiao, Fujia Cheng," Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Sign encryption", Computer Science IEEE Access2018

[11] Po-Wen Chi, C. Lei, "Audit-Free Cloud Storage via Deniable Attribute-Based Encryption", Published 1 April 2018 Computer Science IEEE Transactions on Cloud Computing

[12] S. Ghazal, H. Al-Samarraie, and H. Aldowah, ""i am still learning": Modeling lms critical success factors for promoting students' experience and satisfaction in a blended learning
environment," IEEE Access, vol. 6, pp. 77179–77201, 2018.

[13] K. D. Rajab, "The effectiveness and potential of e-learning inwar zones: An empirical
comparison of face-to-face and online education in saudi arabia,"IEEE Access,2018.

[14] Y. S. Rao, "A secure and efficient ciphertext-policy attribute- based sign encryption for personal health records sharing in cloudcomputing", Future Gender. Computer. Syst. vol. 67 pp. 133-151 Feb. 2017.

[15] 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.