International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

Protocol for Group Key Management for Cloud Storage File Sharing

[1] M. Lavanya, [2]Dr S. Suresh

[1] MCA, [2] Assistant Professor

[3] Department of Computer Applications, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India.

ARTICLEINFO

Article History:

Accepted: 01 July 2023
Published: 20 July 2023

Publication Issue
Volume 9, Issue 4
July-August-2023

Page Number
153-158

ABSTRACT

Cloud storage is growing in popularity due to many businesses' large-scale sharing demands. Because shared files are stored outside of the owner's trust zone, cloud computing raises both expectations and concerns regarding file security. This paper proposes a Gathering Key Administration Convention for cloud record sharing. In response to public channel threats to the network, a hybrid encryption-based group key generation strategy is presented. Besides, a check framework is utilized to protect shared documents from cloud suppliers and gathering individuals intriguing to go after them. The suggested protocol is secure and efficient for data exchange in cloud computing, according to security and performance evaluations.

Keywords : Advanced Encryption Standards, Data Storage, Security, Encryption And Decryption.

I. INTRODUCTION

Modifying administrations as far as cloud has developed more famous considering the present creative blast of cloud advancements. In a common tenure distributed computing climate, information from numerous clients can be put away on a solitary actual framework, which can be facilitated on different virtual machines. Under this model, data owners are left vulnerable and must rely solely on the cloud provider to preserve their data because the cloud provider has complete control over data storage and administration. As indicated by late reports, in the wake of getting a court order, Google gave up every one of one of its clients' records to the FBI, yet the clients knew nothing about the pursuit until they were confined. Because the cloud provider has complete access to the data, data privacy could be jeopardized if the cloud provider intercepts or modifies the user's data. Encrypting and authenticating shared data is a popular method for ensuring privacy. There are a number of cryptographic systems that allow a third-party auditor to validate file availability while no information about the file is revealed. Similarly, cloud users are unlikely to have a strong conviction in the cloud server's secrecy. Before putting their files on the cloud server, cloud clients are urged to scramble them utilizing their own keys. The last test is to appropriate and oversee cryptographic keys among substantial clients without reaching the cloud supplier.

II. RELATED WORKS

CPDA: A Secrecy Safeguarding Deduplication Distributed storage with Public Cloud Reviewing: The number of people outsourcing data to cloud servers has risen rapidly as cloud storage has become more popular. From one viewpoint, the quickly developing volume of information on the cloud is joined overwhelmingly of information duplication. On the other hand, with a deduplication cloud storage system, the cloud server retains only a single copy of outsourced data, and the corruption or loss of that copy can result in unfathomable loss. As a result, file deduplication and integrity auditing are critical, and the question of how to achieve both securely and efficiently in academia and industry must be resolved quickly. We present a deduplicated cloud storage with secret-preserving public cloud auditing (CPDA). In any case, our CPDA plot accomplishes safe document deduplication on scrambled records, permitting public trustworthiness examining of the extraordinary duplicate in the deduplication distributed storage framework.. Secure authentication tag deduplication is also possible with our CPDA technique. Second, during the file deduplication and integrity auditing process, our CPDA system employs convergent encryption and random masking techniques to maintain data secrecy. Third, our approach not only allows each data owner to individually initiate integrity audits of their own files, but it also allows the cloud server to delegate various auditing jobs to a third-party auditor on a regular basis, ensuring the integrity of outsourced files. Finally, numerical analysis and simulation experiments demonstrate our scheme's security and performance.

Audit-Free Cloud Storage via Deniable Attribute-Based Encryption: Cloud storage is becoming more and more popular. Many distributed storage encryption methodologies have been proposed to protect information from people who don't approach on account of the significance of security. In reality, a few specialists (i.e., coercers) may drive distributed storage suppliers to uncover client mysteries or classified information on the cloud, subsequently totally dodging capacity encryption strategies. We propose our proposition for another distributed storage encryption framework in this work, which permits distributed storage suppliers to produce persuading misleading client privileged insights to shield client security. Because coercers have no way of knowing if secrets collected are accurate or not, cloud storage providers ensure that user privacy is maintained.

Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation: A possible service for data owners is data outsourcing, in which their data is stored on a cloud storage provider. Due to the cloud's lack of complete trust, data access control has become a challenging issue in the Cloud Storage System (CSS). In the CSS, Ciphertext-Strategy Property Based Encryption (CP-ABE) is a practical system for guaranteeing access control, with a trait expert responsible for overseeing credits and disseminating keys. We present a new revocable Multi-Authority CP-ABE plot in this work, in which the entrance strategy can be worked as an erratic tree as opposed to the grid used by earlier techniques. Our arrangement is more versatile because of the tree-like strategy. Subsequently, exercises like encryption, decoding, and characteristic repudiation are quicker. Our method has also been shown to be safe, contrary to common belief. It can withstand a user collusion attack, and attribute revocation ensures both forward and backward security. Our system is highly efficient, based on simulation results.

Comments on “Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in

Cloud Computing": Executing another property-based encryption (ABE) engineering that permits a certain rethink of the troublesome encryption cycle to an encryption specialist organization (ESP). Despite the authors' assertions that the outputs of outsourced encryption may be examined by the user, we demonstrate that the Ma et al. proposal does not provide the verifiability property for outsourced encryption, which is the most important security goal that a verifiable computing method should achieve. By demonstrating realistic attacks, we demonstrate that the ESP can return forged intermediate encrypted text to the user undetected.

III. Methodology

In proposed scheme, the verification system protects shared data against cloud providers and group members colluding to attack them. The suggested protocol is secure and efficient for data exchange in cloud computing, according to security and performance evaluations. A group key generation strategy based on hybrid encryption technology is presented in response to network threats via public channel.

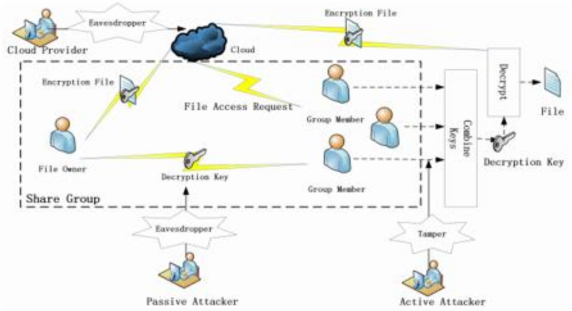


Figure 1: Block diagram of proposed method

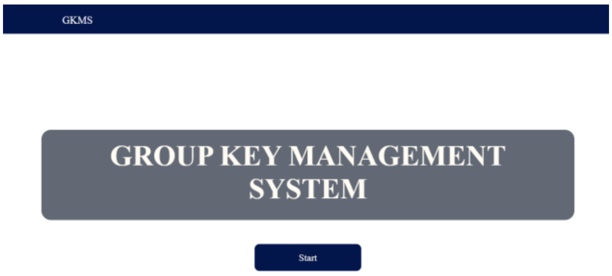
IV. Implementation

This project is implemented by introducing Group Key Management Protocol to project the data from attackers called Cloud Server Provider and group members. To implement the process we need to install required software packages. And we have to define problem solution and need to create flask and user interface, later on we need to run the user, admin and Cloud Server Providers modules those we have mentioned in below section called Results and Discussion along with Screen shots.

V. Results and Discussion

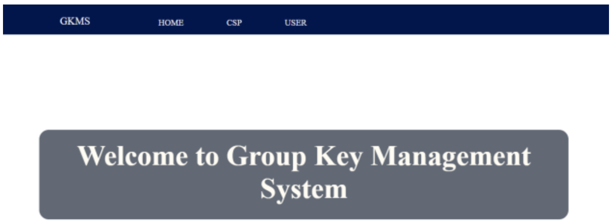
The following images will visually depict the process of our project.

Home page: In this home page we can see the logo designing of our website.



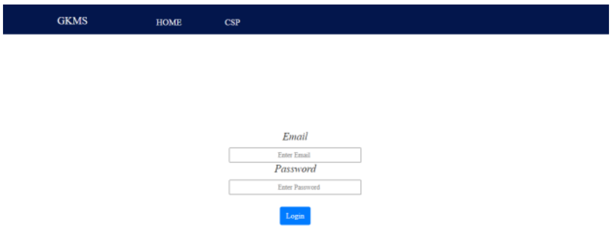
GROUP KEY MANAGEMENT SYSTEM

Start: This page is like a starting step to continue the process of project.



Welcome to Group Key Management System

Csp login page: Login with the valid credentials only.



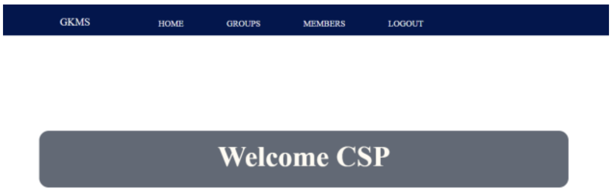
Email

Enter Email

Password

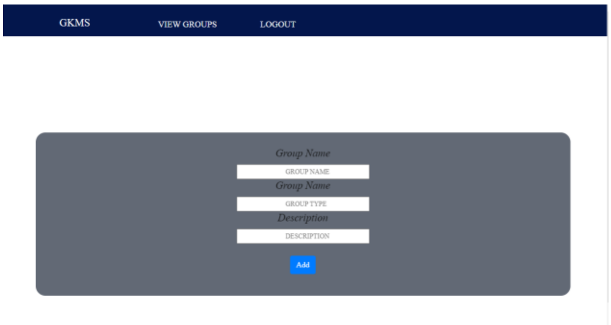
Enter Password

Csp home page: After successful registration and login the CSP can get the home page.

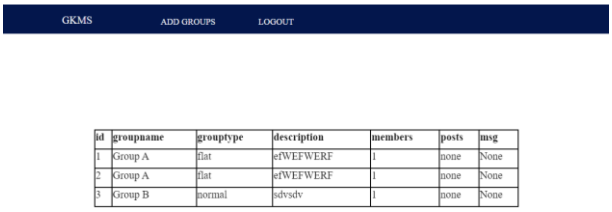


Welcome CSP

Csp add group page: Csp can create groups.

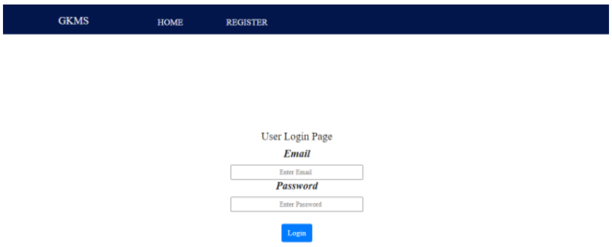


View groups page: Csp can view all groups then join in particular group if he is interested view his own groups.



id	groupname	grouptype	description	members	posts	msg
1	Group A	flat	efWEFWERF	1	none	None
2	Group A	flat	efWEFWERF	1	none	None
3	Group B	normal	sdvsdv	1	none	None

User login page: User having an account he can directly login into the system.

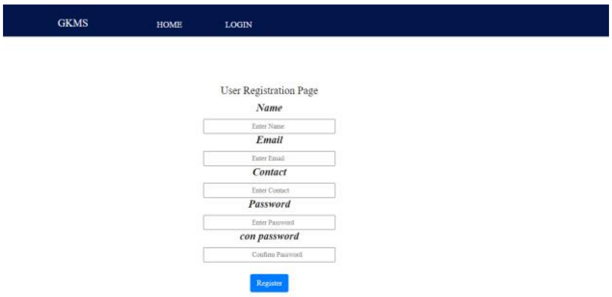


User Login Page

Email

Password

User registration page: If user don't have any account he has to register and login.



User Registration Page

Name

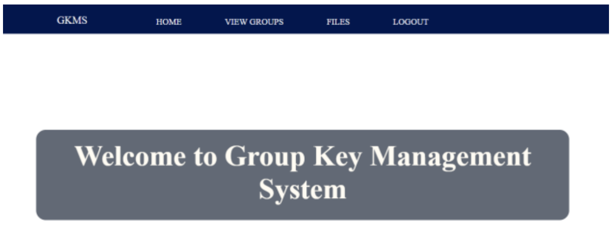
Email

Contact

Password

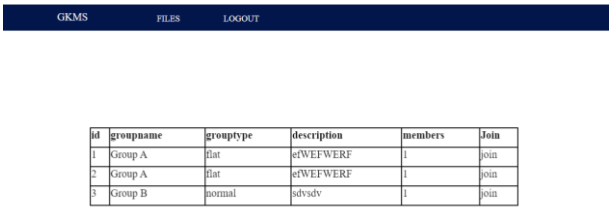
con password

User home page: User can access this page by login.



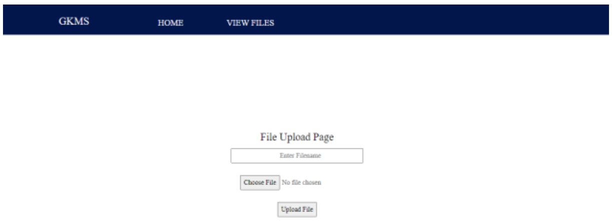
Welcome to Group Key Management System

View users group page: User can view groups and join in specific groups, view all his groups and view the time line.



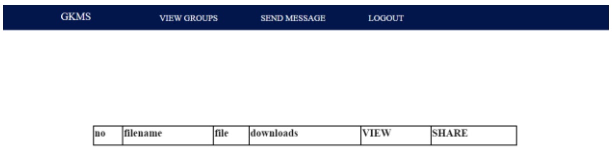
id	groupname	grouptype	description	members	Join
1	Group A	flat	efWEFWERF	1	join
2	Group A	flat	efWEFWERF	1	join
3	Group B	normal	sdvsdv	1	join

Upload files page: User can upload files.



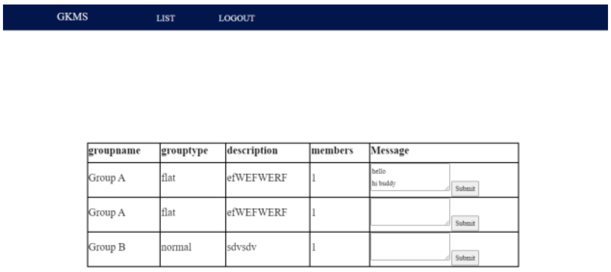
File Upload Page

View files page: User can view those files and share files to specific groups and finally time line of groups.



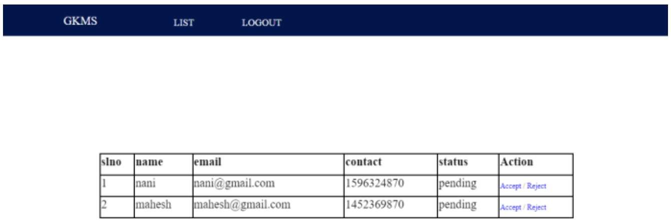
no	filename	file	downloads	VIEW	SHARE

Send messages: Here the group members can send their messages.



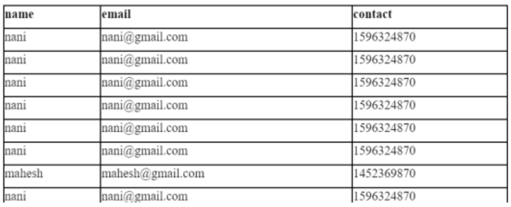
groupname	grouptype	description	members	Message
Group A	flat	efWEFWERF	1	hello hi buddy
Group A	flat	efWEFWERF	1	
Group B	normal	sdvsdv	1	

Request page: This page contains request details.



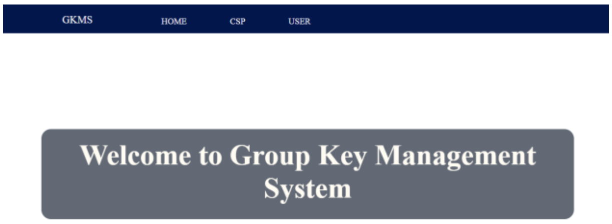
slno	name	email	contact	status	Action
1	nani	nani@gmail.com	1596324870	pending	Accept / Reject
2	mahesh	mahesh@gmail.com	1452369870	pending	Accept / Reject

List of group members: This page display the members having in group.



name	email	contact
nani	nani@gmail.com	1596324870
nani	nani@gmail.com	1596324870
nani	nani@gmail.com	1596324870
nani	nani@gmail.com	1596324870
nani	nani@gmail.com	1596324870
nani	nani@gmail.com	1596324870
mahesh	mahesh@gmail.com	1452369870
nani	nani@gmail.com	1596324870

Logout: This is logout page where the user or admin can logout from system.



Welcome to Group Key Management System

VI. Conclusion

We developed a revolutionary group key management mechanism for cloud storage file sharing in this research. GKMP use publickey to ensure that group keys are distributed properly and that the cloud provider is immune to assault. We provide a detailed study of potential security threats and their related defences, demonstrating that GKMP is secure even under more lenient assumptions. We also show that the protocol is less complicated in terms of storage and computation.

VII. REFERENCES

[1]. CPDA: A Privacy Protecting Deduplication Distributed Storage With Public Cloud Evaluating, IEEE Access, vol.7, pp.160482-160497, 2019. 1. J. Wu, Y. Li, T. Wang, et al.

[2]. C. Po-Wen and L. Jawline, "Review Free Distributed storage through Deniable AttributeBased Encryption," IEEE Exchanges on Distributed computing, vol. 6, no. 2, pp. 414-427, 2018.

[3]. J. Zhou and co., Getting rethought information in the multi-authority cloud with fine-grained admittance control and effective characteristic repudiation", Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.

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

[5]. Z. Fu X. Sun S. Ji G. Xie "Towards productive substance mindful pursuit over encoded reevaluated information in cloud" Proc. 35th Annu. Int. IEEE Conf. Comput. Public (INFOCOM), pages 1-9 Apr. 2016.

[6]. Y. S. Rao, "A protected and productive ciphertext-strategy property based signcryption for individual wellbeing record partaking in distributed computing," Group of people yet to come PC Frameworks, vol. 67, no. 1, pp. February 2017, pp. 133-151

[7]. H. liu Y. huang J. K. Liu "Secure sharing of Individual Wellbeing Records in distributed computing: Ciphertext-Strategy Property Based Signcryption" Future Gener. Comput. Syst. vol. 52 pp. 67-76 Nov. 2015.

[8]. Fu, Q., Zhang, Y., and Chen, J. (2013). A Solid Gathering Key Administration Plan for Distributed storage. In 2013 twelfth IEEE Global Meeting on Trust, Security and Protection in Processing and Correspondences (pp. 1530-1535). IEEE. doi: 10.1109/TrustCom.2013.192

[9]. Khan, N., and Alghathbar, K. (2015). A survey of gathering key administration strategies for cloud administrations. 50, 1-12, Journal of Network and Computer Applications. doi: 10.1016/j.jnca.2014.08.008

[10]. Yu, S., Zhang, Y., and Guo, S. (2016). Over encrypted cloud data, a secure and dynamic multi-keyword ranked search scheme. IEEE Exchanges on Equal and Conveyed Frameworks, 27(2), 340-352. doi: 10.1109/TPDS.2015.2391998

[11]. Shahriar, H., Rahman, M. S., and Islam, R. (2017). Group Key Management for Safe Cloud-Based Data Sharing In 2017 fourth Worldwide Meeting on Electrical Designing and Data and Correspondence Innovation (ICEEICT) (pp. 1-6). IEEE. doi: 10.1109/ICEEICT.2017.7930083

[12]. Zhang, Y., Zhang, J., and Xiong, H. (2014). A Safe Key Administration Plan for Gathering Information Partaking in Distributed storage. In 2014 IEEE Worldwide Gathering on Correspondences (ICC) (pp. 3575-3580). IEEE. doi: 10.1109/ICC.2014.6883887

[13]. Cao, N., Wang, C., Li, M., Ren, K., and Lou, W. (2012). Protection safeguarding multi-watchword positioned search over encoded cloud information. IEEE INFOCOM in 2012 (pp. 353-361). IEEE. doi: 10.1109/INFCOM.2012.6195497

[14]. Ren, K., Wang, C., and Wang, Q. (2014). Security challenges for the public cloud. IEEE Web Processing, 18(1), 69-73. doi: 10.1109/MIC.2014.5

[15]. Ruj, S., Stojmenovic, M., and Nayak, A. (2014). Cloud-based data can be anonymously authenticated with decentralized access control. Parallel and Distributed Systems, IEEE Transactions, 25(2), 384-394. doi: 10.1109/TPDS.2013.229

[16]. Lou, W., C. Wang, N. Cao, J. Li, K. Ren, and Toward secure and dependable limit organizations in conveyed figuring. IEEE Transactions on Services Computing, vol. 5(2), pages 220-232. doi: 10.1109/TSC.2011.39

[17]. Yang, K., Jia, X., and L. Xie In data outsourcing systems, attribute-based access control with efficient revocation. In Procedures of the fifth ACM Conference on Data, PC and Correspondences Security (pp. 1-10). ACM. doi: 10.1145/2185448.2185462

Cite this article as :

M. Lavanya, Dr S. Suresh, "Protocol for Group Key Management for Cloud Storage File Sharing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.153-158, July-August-2023.