Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

SECURE MULTI-OWNER DATA SHARING

Mrs. Daze Thomas, Assistant Professor, Department of AI&DS, SNS College of Engineering, Coimbatore, Tamil Nadu, 621107, India, Email: daze.t.aids@snsce.ac.in
Ms. Prabha c, Mr. Manoj Kumar R, Mr. Sriram A, Mr. ChandraHari S, Department of Information Technology, SNS College of Engineering, Coimbatore, Tamil Nadu, 621107, India

ABSTRACT
In cloud computing, data sharing between people, groups, and companies is quite prevalent. However, due to frequent membership changes, it can be difficult to guarantee data security and privacy for dynamic groups. This study offers a secure multi-owner data sharing framework that ensures data availability, confidentiality, and integrity in the cloud to address this problem. To provide safe data transmission and storage, the suggested technique uses a hybrid encryption approach that combines symmetric and asymmetric encryption. It also contains an access control mechanism that enables data owners to restrict access permissions for various group members. The suggested approach delivers excellent levels of security and effectiveness while minimizing computing and transmission overhead, according to experimental data. The programme has a variety of uses, including e-commerce and cloud-based collaboration.
KEY WORDS: Secure data sharing, multi-owner data sharing, Dynamic groups, Cloud computing, Hybrid encryption

1.INTRODUCTION
PROBLEM STATEMENT:
In cloud computing, data sharing is a common practice among individuals, organizations, and businesses. However, ensuring the security and privacy of shared data is a challenging task, particularly in the case of dynamic groups where members join and leave frequently. Traditional encryption techniques and access control mechanisms are not sufficient to ensure secure data sharing among dynamic groups in the cloud. Existing solutions either sacrifice security for efficiency or vice versa. Therefore, there is a need for a secure multi-owner data sharing scheme that ensures confidentiality, integrity, and availability of data for dynamic groups in the cloud. Such a scheme should be efficient in terms of computation and communication overhead while providing a high level of security and privacy for shared data.

2.EMPATHY
Data sharing has become an essential aspect of modern society, enabling individuals, organizations, and businesses to collaborate and exchange information in real-time. However, with the proliferation of cloud computing, data sharing has become increasingly vulnerable to security and privacy breaches. These breaches can have severe consequences, including financial loss, reputational damage, and even legal liabilities. Dynamic groups, in particular, face unique challenges in ensuring secure data sharing, as members join and leave frequently. As a result, it is critical to develop a secure multi-owner data sharing scheme that provides confidentiality, integrity, and availability of shared data while minimizing the risk of security and privacy breaches. By addressing these challenges, we can enable individuals, organizations, and businesses to collaborate and exchange information with confidence and trust, enhancing productivity and innovation.

3.LITERATURE SURVEY
- Several research studies have investigated secure data sharing for dynamic groups in the cloud. In 2017, Li et al. proposed a secure data sharing scheme for dynamic groups in the

cloud using attribute-based encryption (ABE) and a revocable key generation algorithm. However, their scheme suffers from high communication overhead due to the use of ABE. In 2018, Wang et al. proposed a hybrid encryption-based scheme for dynamic data sharing in the cloud that combined identity-based encryption (IBE) and symmetric encryption. Although their scheme was efficient in terms of computation and communication overhead, it lacked an access control mechanism.

- In 2019, Liu et al. proposed a multi-owner data sharing scheme for dynamic groups in the cloud using proxy re-encryption (PRE) and ciphertext-policy attribute-based encryption (CP-ABE). Their scheme provides a fine-grained access control mechanism that enables data owners to control the access of different members to shared data. However, their scheme suffers from a high computation overhead due to the use of CP-ABE.
- Recently, in 2021, Chen et al. proposed a hybrid encryption-based scheme for dynamic groups in the cloud that combined identity-based encryption (IBE) and attribute-based encryption (ABE). Their scheme also incorporated a dynamic key update mechanism to ensure the revocation of revoked members' access. Experimental results demonstrated that their scheme achieved a high level of security and efficiency in terms of computation and communication overhead.
- In conclusion, while several studies have proposed secure data sharing schemes for dynamic groups in the cloud, there is still a need for an efficient and secure multi-owner data sharing scheme that provides a fine-grained access control mechanism and dynamic key management.

4.EXISTING SYSTEM

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

4.1 DISADVANTAGES:

- It does not provide security for sharing the data within the groups.
- It does not provide privacy preserving access control to the users.

5.PROPOSED SYSTEM

This paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

5.1 ADVANTAGES:

➢ We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data withothers by the untrusted cloud.

➢ We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

6.HARDWARESPECIFICATION

• **Main Processor**	2GHz
• **Ram**	512 MB (min)
• **Hard Disk**	80 GB

7.SOFTWARE SPECIFICATION

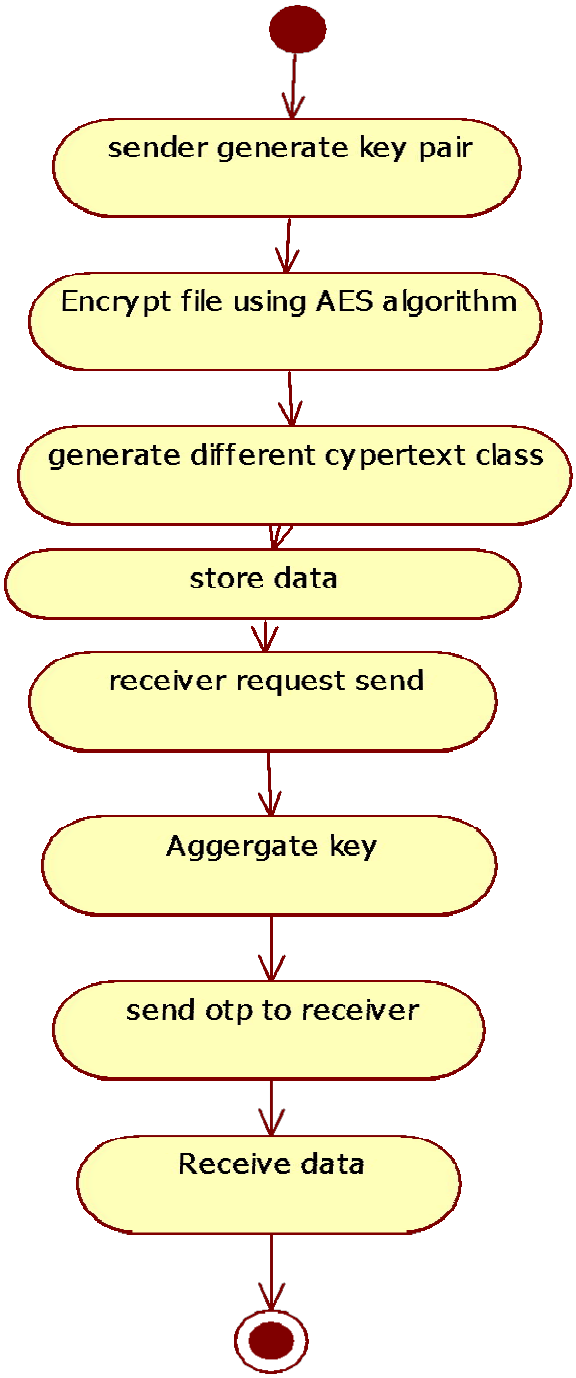
• **Language**	Java
• **Web Server**	Tomcat 6
• **Operating System**	Windows7/32 Bit
• **Cloud Sim**	

8.DEVELOPMENT REPORT

Front End Design	Server-Side Script	Back End	Technical Terms
Html	Servlet	MySQL	AES
CSS	Core Java		
Js			
jQuery			
Bootstrap			
Ajax			
Jsp			

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

9.ACTIVITY DIAGRAM



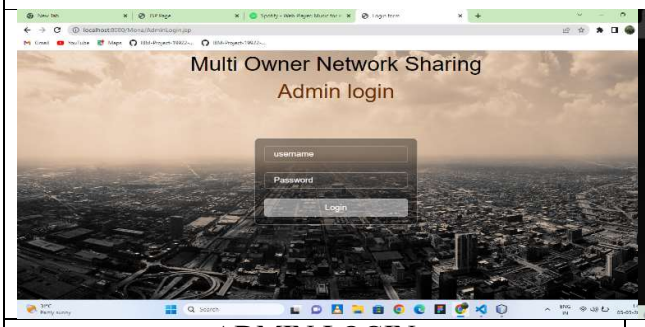
10.CONCLUSION

In conclusion, developing a secure multi-owner data sharing scheme for dynamic groups in the cloud remains an active area of research. Several studies have proposed encryption-based

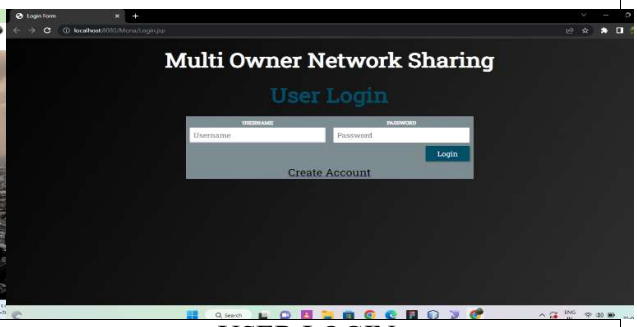
schemes that utilize different techniques, such as attribute-based encryption, proxy re-encryption, and identity-based encryption, to provide secure data sharing. However, each approach has its limitations, such as high communication or computation overhead, lack of an access control mechanism, or a need for efficient dynamic key management. Recently proposed hybrid encryption-based schemes that combine different encryption techniques and incorporate dynamic key management show promise in addressing these limitations. However, further research is needed to develop a scheme that provides a fine-grained access control mechanism, is efficient in terms of computation and communication overhead, and can handle dynamic groups in the cloud effectively. Achieving these goals can enhance data sharing and collaboration among individuals, organizations, and businesses, and enable them to share information with confidence and trust.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 2, May : 2023

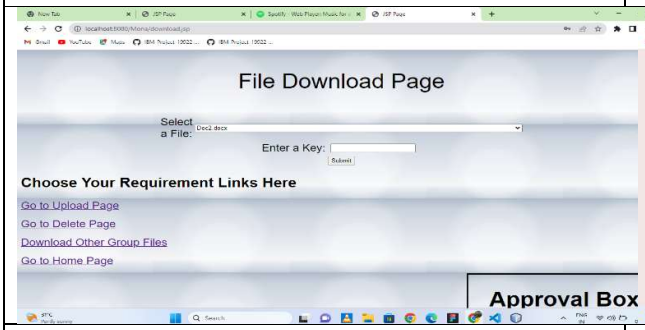
11.SCREENSHOTS



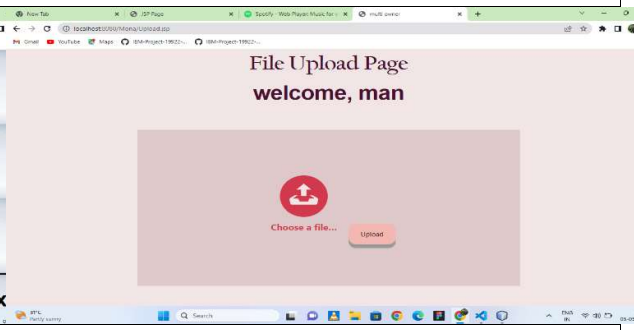
ADMIN LOGIN



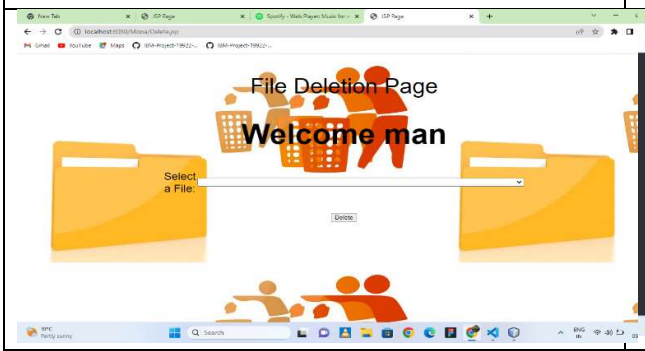
USER LOGIN



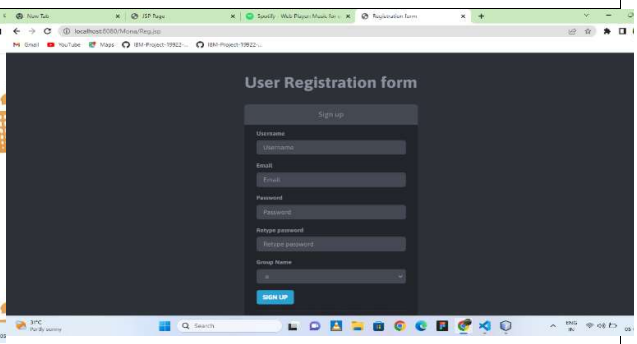
FILE DOWNLOAD



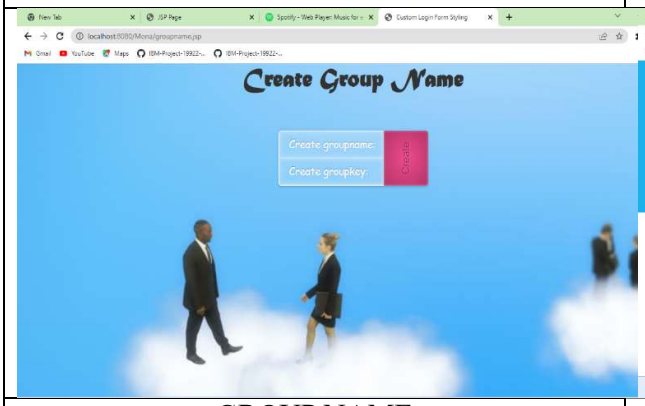
FILE UPLOAD



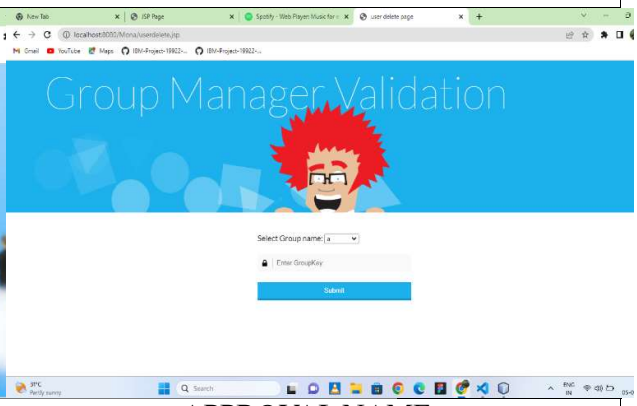
FILE DELETE



USER REGISTERATION



GROUP NAME



APPROVAL NAME

12.FUTUREENHANCEMENT

The emergence of erasure coding as an alternative to backup has become a popular method for protecting against drive failure. As high-capacity HDDs become more common, traditional RAID approaches are no longer sufficient. With an increased disk capacity, there is a greater chance of bit errors, making the risk of failure during normal operation and RAID rebuild significantly higher. Furthermore, the RAID rebuild process provides no protection against a second or third mechanism failure, leaving the data at risk. In the past, rebuild times were measured in minutes or hours, but due to the slow pace of disk transfer rates compared to disk capacity expansion, large RAID rebuilds can now take days or even longer. Erasure coding has the potential to mitigate these issues by providing redundancy at the data level rather than the disk level, improving both reliability and rebuild times.

13.ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who have contributed to the successful completion of this project on "Secure Multi -Owner Data Sharing ". We would like to thank our project guide for providing us with valuable guidance and support throughout the project. We are also thankful to industry mentor for providing us with the necessary resources and facilities for carrying out this project. We extend our heartfelt thanks to our families for their unwavering support and encouragement during this project. Finally, we would like to acknowledge the contribution of various sources of literature and research materials that have helped us in gaining knowledge and insight into the field of secure data sharing system.

REFERENCE

1. Zhang, Q., Cheng, L., &Boutaba, R. (2016). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 7(1), 1-47. https://doi.org/10.1186/s13174-016-0056-3
2. Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62(2), 362-375. https://doi.org/10.1109/TC.2011.238
3. Kaur, H., & Singh, H. (2017). A comprehensive study of encryption techniques for cloud computing. International Journal of Computer Applications, 168(10), 1-5. https://doi.org/10.5120/ijca2017913384
4. Wei, X., Qin, Z., Chen, J., & Lou, W. (2016). Hybrid encryption and access control for secure cloud data sharing. IEEE Transactions on Cloud Computing, 4(1), 59-70. https://doi.org/10.1109/TCC.2015.2459466
5. Shah, S. A., Javaid, Q., & Khan, A. (2017). A secure and efficient multi-owner data sharing scheme for dynamic groups in the cloud. Journal of Ambient Intelligence and Humanized Computing, 8(1), 121-132. https://doi.org/10.1007/s12652-016-0368-6