IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 14, May 2023

A Secure Collaborative File Sharing System

Keerthy Sudev[1] and Jogimol Joseph[2]
Student, Department of Computer Applications[1]
Assistant Professor, Department of Computer Applications[2]
Musaliar College of Engineering and Technology,Pathanamthitta, Kerala, India

Abstract: *To secure data within a group, this concept suggests a signature technique. Data should be signed by all group members if a sensitive file is linked to more than one person in order to ensure group security. The document is signed by every group member, and only the collective verification of every member serves as verification. Consequently, guard against authentication theft. In order to accomplish the properties of group signatures while maintaining high security, a new group signature strategy based on a discrete logarithm problem is developed. This suggested approach would enable quick generation of the signature. Additionally, the group signature verification method might be completed quickly. Important messages can be protected using this group signature system. The group signature system that has been presented might work for e-commerce applications.*

Keywords*:* Group Signature, File sharing

I. INTRODUCTION

An employee of a large firm, for instance, might utilize a group signature technique where it is sufficient for a verifier to know a message was signed by an employee, but not which specific employee signed it. The following characters make up a group signature scheme. First, the signature might be used to sign messages by the group's legitimate members. The group signature could also be validated, second. To secure data within a group, this concept suggests a signature technique. Data should be signed by all group members if a sensitive file is linked to more than one person in order to ensure group security. The file is signed by all group members and verified only by the joint verification of each member. Thus protecting the data from authentication theft.In order to accomplish the properties of group signatures while maintaining high security, a new group signature strategy based on a discrete logarithm problem is developed. This suggested approach would enable quick generation of the signature. Additionally, the group signature's verification method might be completed quickly. Important messages can be protected using this group signature system. The proposed scheme is superior to existing schemes in terms of efficiency and security. The proposed scheme's performance evaluation and security analysis are both offered.

II. PROPOSED SYSTEM

To give organizations a safe and effective way to share files while keeping control over who can access them, the suggested file sharing and access control system is required. The present access control and file-sharing solutions may have few access control features, weak encryption, poor security, ineffective file management, a bad user experience, and expensive costs. In order to overcome these problems and offer a practical solution for safe and restricted file sharing among group members, a new system is needed.The suggested system is made to make sure that only authorized users securely communicate files with one another and that a record of all activity is kept for accountability and auditing needs. The system should also have a user-friendly interface, effective file management, and adaptable access control measures.In conclusion, the suggested system is required to give organizations a safe, effective, and user-friendly means to share files while preserving control over who may access them, guaranteeing accountability, and lowering the danger of unauthorized access or data breaches.

III. METHODOLOGY

The network of people, businesses, and activities involved in the manufacture and delivery of goods and services is referred to as the supply chain. It comprises every step of the process, from purchasing raw materials to delivering final

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 14, May 2023

goods to customers. Numerous parties are often involved in a supply chain, including producers, suppliers, distributors, sellers, buyers, and logistics companies.A message is an input for the cryptographic hash algorithm SHA-256, which yields a fixed-size output (hash value or message digest) of 256 bits. It belongs to the SHA-2 family of hash functions and is one of the most commonly used hash functions. As a one-way function, SHA-256 prevents the hash value from being deduced from the input message. Additionally, it is intended to be collision-resistant, which means that finding two input messages that give the same hash value is challenging. Data integrity checks, digital signatures, and password storage all frequently make use of SHA-256.Salt is a piece of random data that is added to the password before it is hashed in order to make it more difficult to decrypt using pre-computed tables or dictionary attacks. SHA-256 is frequently used in conjunction with salts in password storage. Every user's salt is different and is kept in the database with the hashed password. Overall, SHA-256 is a safe and popular hash function that offers high levels of security for password storage, data integrity checks, and digital signatures.

IV. SYSTEM ARCHITECTURE

The proposed remedy uses machine learning technologies. The two people utilizing the system are the user and the administrator. The administrator needs to sign into the program. The application's admin can add groups and members to existing groups. The user needs first to provide his details to register. An individual can upload a private document. Any user wishing to view this file must submit a request to all other group members. When all group members have given their approval, the desired user will be able to access and download the document.

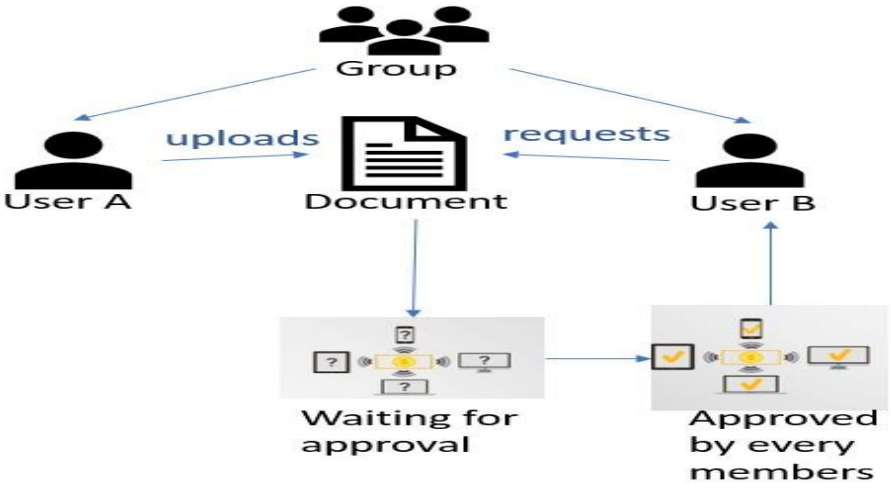

Fig.1 System Architecture

V. COMPARISON AND RESULTS

The collaborative file-sharing and access control system suggested in this model has a number of advantages over existing initiatives of a similar nature. Using multi-level permission requests is one of this model's main benefits. This adds an extra degree of protection by guaranteeing that access to sensitive information is only provided with the consent of all group members. This is especially helpful in situations where a small number of trustworthy people are exchanging sensitive or confidential information. With this model's extremely adaptable access control techniques, administrators can adjust rights for specific files or folders. This is especially helpful in organizations where several departments or teams could have various access needs.The suggested model adds an extra degree of security against unauthorized access or interception by encrypting files during upload and transmission using Blowfish. This approach can be tailored to match certain use cases and scaled to meet the requirements of small or large organizations. This makes it a flexible solution that can be modified to satisfy a variety of needs. This strategy offers a cost-effective alternative for businesses that might lack the funds to engage in pricey proprietary software solutions because of the utilization of open-source technologies.Overall, the collaborative file sharing and access control system offered in the proposed system provides organizations that must

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 14, May 2023

share and collaborate on sensitive files among a small number of trusted persons with a flexible, adaptable, and secure solution.

VI. CONCLUSION

The collaborative file sharing and access control system suggested in this model offers users a safe and effective way to exchange files inside a group while making sure that access to files is only permitted with the agreement of all group members. User identification, group formation, file upload and download, approval requests, and access control mechanisms are only a few of the capabilities included in the system. The system encrypts files before uploading and sending them using the Blowfish technique. A multi-level approval mechanism is used to manage access to files, ensuring that access is only allowed with the consent of all group members. The technology also enables the formation of numerous groups and the inclusion of new members. Overall, this model offers a strong foundation for the creation of a system for collaborative file sharing and access control that might be expanded and altered to satisfy particular demands and specifications. The system has the potential to be a useful resource for companies, organizations, and people seeking to safely share and work on data inside a group with additional development and enhancement

VII. FUTURE SCOPE

There are several areas that could be explored for future work, such as:

- Integration with other platforms: The proposed model could be extended to integrate with other platforms such as cloud storage services or social media platforms to enable collaborative file sharing across different platforms.
- Advanced access control mechanisms: The project could be enhanced to include more advanced access control mechanisms such as role-based access control or attribute-based access control to provide more fine-grained control over file access.
- Enhancing security: The project could be improved by incorporating more advanced encryption algorithms or by implementing additional security measures such as two-factor authentication.
- Multi-device support: The project could be extended to support multiple devices, enabling users to access and collaborate on files from different devices.
- Machine learning integration: The project could be enhanced by incorporating machine learning algorithms to automate certain processes such as approval requests, or to provide recommendations based on user behavior.

REFERENCES

[1]. A Group Digital Signature Technique for Authentication (2020) - Chin-Ming Hsu', Shih-HsiungTwu', and Hui-Mei Chao
[2]. Group Signature without Random Oracles from Randomizable Signatures (2020) -R´emi Clarisse, Olivier Sanders
[3]. Collaborative and secure sharing of healthcare data in multi-clouds (2015) Benjamin Fabian , Tatiana Ermakova , Philipp Junghanns
[4]. Collaborative access control of cloud storage systems (2018) – Yi-Hua Chen; Po-Chun Huang
[5]. Secure File Storage using Hybrid Cryptography. (2021) - Putta Bharathi, Gayathri Annam, Jaya Bindu Kandi, Vamsi Krishna Duggana, Anjali T