

Cyber Security Based File Sharing

**PROF. ANIK C. NAIK¹, PROF. MAYUR G. UHNALE², SARTHAK K. PAWAR³, SAGAR S. SAWANT⁴,
TUSHAR B. MULE⁵, SUYOG Y. THOMBRE⁶,**

¹(HOD, Dept .of Computer Engineering), S.Y.P Shreeyash College Of Engineering And Technology (Polytechnic),
Chh.Sambhajanagar, India

²(Prof (Guide) , Dept .of Computer Engineering), S.Y.P Shreeyash College Of Engineering And
Technology(Polytechnic), Chh.Sambhajanagar, India

^{3,4,5,6}(Students, Department of Computer Engineering),S.Y.P Shreeyash College Of Engineering And
Technology(Polytechnic), Chh.Sambhajanagar, India

Abstract - In recent years, the rapid growth of cloud-based services and online data sharing has increased the risk of data breaches and cyber-attacks. Traditional file sharing systems often fail to provide adequate security, leading to unauthorized access and data loss. This paper proposes a cyber security-based secure file sharing system that focuses on protecting data confidentiality, integrity, and access control. The proposed system employs user authentication, role-based access control, and encryption techniques to secure files during upload, storage, and transmission. Files are encrypted before being stored on the server, ensuring that data remains protected even in the event of unauthorized access. Secure key management is implemented to allow only authorized users to decrypt shared files. Additionally, the system maintains audit logs to monitor user activities and detect suspicious behavior. Experimental results show that the system effectively prevents unauthorized access while maintaining efficient performance. The proposed solution is suitable for secure file sharing in cloud and organizational environments.

Key Words: Cyber Security, Secure File Sharing, Data Encryption, Access Control, Cloud Security

1. Introduction

In recent years, the rapid growth of information technology and internet-based services has transformed the way data is stored, accessed, and shared. File sharing systems have become an essential component of modern communication, enabling users to exchange documents, multimedia files, and sensitive information efficiently across networks. Cloud computing and online storage platforms have further enhanced the convenience of file sharing by allowing users to access data anytime and from anywhere. However, this increased accessibility has also introduced significant security and privacy challenges.

As the volume of digital data continues to grow, cyber threats targeting file sharing systems have become more frequent and sophisticated. Unauthorized access, data leakage, identity theft, malware attacks, and man-in-the-middle attacks pose serious risks to both individuals and organizations. Traditional file sharing mechanisms often lack

adequate security features, making them vulnerable to such attacks. In many cases, files are transmitted or stored without proper encryption, allowing attackers to intercept, modify, or misuse sensitive information.

Cyber security plays a crucial role in addressing these challenges by protecting digital assets from unauthorized access and malicious activities. It involves the application of technologies, processes, and practices designed to safeguard networks, systems, and data. Key cyber security principles such as confidentiality, integrity, and availability are essential for ensuring secure file sharing. Confidentiality ensures that data is accessible only to authorized users, integrity guarantees that data remains unchanged during transmission, and availability ensures that authorized users can access data whenever required.

A cyber security based file sharing system integrates multiple security mechanisms to provide a secure environment for data exchange. Encryption techniques are used to convert plain data into unreadable formats before storage or transmission, ensuring data confidentiality even if it is intercepted. Secure authentication mechanisms verify user identities, preventing unauthorized access to the system. Access control policies further restrict file access based on user roles and permissions, reducing the risk of insider threats and data misuse.

This paper presents a cyber security based file sharing system designed to enhance data protection and user trust. The proposed system focuses on secure user authentication, encrypted file storage, and controlled file access to minimize security vulnerabilities. By incorporating cyber security techniques into the file sharing process, the system aims to provide a reliable and secure platform for data sharing over untrusted networks. The proposed approach is suitable for real-world applications such as corporate data sharing, cloud storage services, educational platforms, and government systems where data security and privacy are of utmost importance.

1.1 Objects of the System

The primary ideal of the Cyber Security Based train participating System is to give a secure, dependable, and effective platform for participating digital lines over the internet. The system is designed to address the security challenges associated with traditional train sharing styles by integrating advanced cyber security mechanisms.

The specific objects of the proposed system are as follows

- To insure secure stoner authentication so that only authorized druggies can pierce the train sharing system.
- To give confidentiality of data by cracking lines before storehouse and transmission.
- To maintain data integrity by precluding unauthorized revision of lines during transfer or storehouse.
- To apply access control mechanisms that circumscribe train access grounded on stoner places and warrants.
- To cover the system against common cyber- attacks similar as unauthorized access, data interception, and malware pitfalls.
- To enable secure train upload, download, and participating with minimum performance outflow.
- To enhance stoner trust and data sequestration in pall and network- grounded train sharing surroundings.

By achieving these objects, the proposed system aims to deliver a robust cyber security result that supports safe and effective train sharing for associations and individual druggies.

1.2 Methodology

The methodology of the Cyber Security Based File Sharing System focuses on designing and implementing a secure framework for storing and sharing files over a network. The proposed methodology integrates cyber security techniques such as authentication, encryption, and access control to ensure secure data handling throughout the file sharing process. The system follows a structured approach that includes user registration, secure authentication, encrypted file storage, controlled file access, and secure file transmission.

Initially, users are required to register in the system by providing valid credentials. During registration, user details are securely stored in the database using hashing techniques to protect sensitive information such as passwords. Once registered, users must authenticate themselves through a secure login process. Only authenticated users are granted access to system functionalities, which helps prevent unauthorized entry.

After successful authentication, users can upload files to the system. Before storing any file on the cloud or server, the system applies encryption algorithms to convert the original file into encrypted form. This ensures that even if unauthorized access occurs at the storage level, the data remains unreadable. The encrypted files are then stored securely on the file storage server.

When a user requests to download or access a file, the system verifies the user's access rights using an access control mechanism. Role-Based Access Control (RBAC) is applied to ensure that users can access only those files for which they have permission. Upon successful authorization, the encrypted file is retrieved from the storage server and decrypted before being delivered to the user.

To maintain data integrity, hashing techniques are used to verify that the file has not been altered during transmission. Secure communication protocols are employed to protect data while it is being transferred between the user and the server. This step-by-step methodology ensures confidentiality, integrity, and availability of data within the file sharing system.

Overall, the proposed methodology provides a systematic and secure approach to file sharing by integrating multiple cyber security mechanisms, making the system reliable and suitable for real-world secure data sharing applications.

1.3 Need for Cyber Security

With the rapid advancement of information technology and the widespread use of the internet, digital data has become one of the most valuable assets for individuals and organizations. Large volumes of sensitive information such as personal data, financial records, and confidential documents are stored and transmitted through online platforms. This increasing dependence on digital systems has also led to a significant rise in cyber threats, making cyber security a critical requirement in modern computing environments.

Traditional systems often lack adequate security mechanisms to protect data from unauthorized access and malicious attacks. Cyber threats such as hacking, data breaches, malware infections, phishing, and man-in-the-middle attacks can result in data loss, privacy violations, financial damage, and reputational harm. In file sharing

systems, the risk is even higher because data is frequently transmitted over public and untrusted networks.

Cyber security is essential to ensure the **confidentiality, integrity, and availability** of information. Confidentiality prevents unauthorized users from accessing sensitive data, integrity ensures that data is not altered during storage or transmission, and availability guarantees that authorized users can access data whenever required. Without proper cyber security measures, these fundamental principles cannot be maintained.

In cloud-based and online file sharing systems, cyber security techniques such as encryption, authentication, access control, and secure communication protocols play a vital role in protecting data. Encryption safeguards data by converting it into an unreadable format, while authentication and access control restrict system access to authorized users only. These mechanisms significantly reduce the risk of data misuse and cyber -attacks.

Therefore, the need for cyber security has become more critical than ever in order to protect digital assets, maintain user trust, comply with data protection regulations, and ensure secure and reliable system operation. Implementing strong cyber security measures is essential for the successful deployment of secure file sharing systems and other modern digital applications.

2. System Architecture

The proposed Cyber Security Based File Sharing System follows a layered and modular architecture to ensure secure, efficient, and reliable file sharing. The architecture is divided into three main layers: **User Interface (UI)**, **Application Backend**, and **Underlying Infrastructure**. Each layer plays a significant role in maintaining system security, scalability, and performance.

The **User Interface (UI)** layer represents the front-end of the system through which users interact with the application. It includes screens such as the home screen, access screen, and file upload interface. Users can securely log in, access their dashboard, and upload files using this interface. All user requests are forwarded to the backend for further processing.

The **Application Backend** layer is the core of the system where major security and file management operations are performed. It consists of multiple services that work together to provide secure file sharing. The **Authentication Service** verifies user credentials and ensures that only authorized users can access the system. The **File Management Service** handles file upload, download, and sharing operations. Before storage, files are processed by the **File Encryption Service**, which encrypts data to protect confidentiality.

Encrypted files are stored in the **File Storage Module**, where file identifiers and access control lists (ACLs) are maintained. This ensures that files can only be accessed by users with proper permissions. The **Access Control Mechanism** enforces role-based permissions to prevent unauthorized access. Additionally, the **Encryption/Decryption Module** manages cryptographic operations and generates secure shareable file links or IDs. The **Share/Notification Service** is responsible for sending notifications to users when files are shared or accessed.

User-related information such as account details and credentials is securely maintained in the **User Database**, further enhancing system security. All communication between modules is performed using secure channels to prevent data interception and tampering.

The **Underlying Infrastructure** layer provides the cloud-based support required for storage and processing. Cloud platform services such as Firebase and Cloud nary are used for scalable storage, database management, and secure data handling. This layer ensures high availability, fault tolerance, and efficient resource management.

Overall, the system architecture integrates authentication, encryption, access control, and cloud services to provide a secure and reliable file sharing environment. By enforcing security at every layer, the proposed architecture effectively protects data confidentiality, integrity, and availability, making it suitable for real-world cyber security applications.

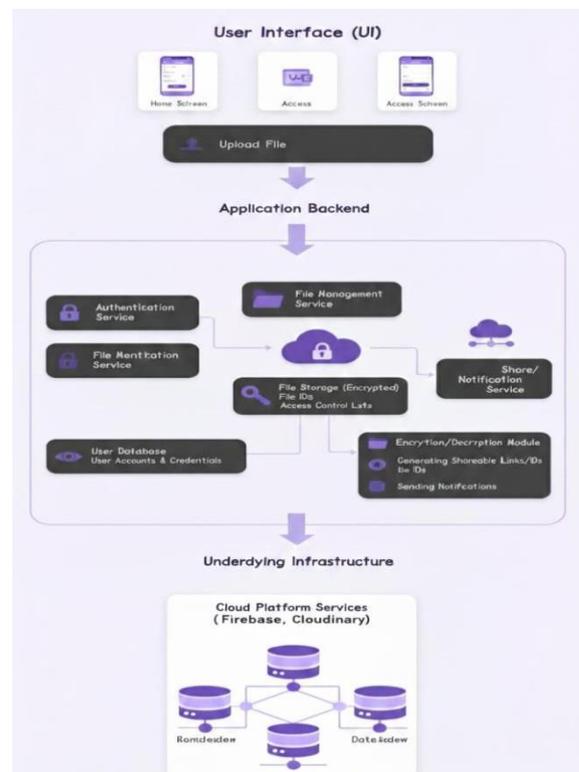


Fig-1 System Architecture

The working of a secure file-sharing system that uses authentication and encryption to protect user data. The process starts when the user clicks the sign-in option, which opens the Google OAuth authentication form. The system uses password.authenticate() to verify the user. The user enters an email and password, and the system checks whether the login credentials are correct. If the credentials are invalid, an error message is shown and the user is asked to re-enter the details. If the credentials are valid, the user successfully logs into the dashboard. After logging in, the user is given an option to encrypt the file. If encryption is selected, the file is encrypted using a password to ensure data security. The user can then choose whether to store the file or share it. If the file is stored, it is securely uploaded to storage. If the file is shared, a sharable link is generated and displayed through a chat client popup, along with the password required to access the file. The receiver can decrypt the file using the shared password. Finally, after completing the required actions, the user logs out, and the process ends.

Initially, the **User** selects a file from the local system through the user interface. Before uploading, the selected file is processed by the system and encrypted to prevent unauthorized access. This encrypted file is then forwarded to the **Upload File** module, which handles the secure transmission of data to the backend system.

The encrypted file along with its associated metadata is stored in the **System Database / Cloud Storage**. Metadata includes information such as file identifiers, ownership details, and access permissions. Storing only encrypted files in the database ensures that data remains protected even if the storage system is compromised.

After successful storage, the system generates a unique **File ID** for the uploaded file. This File ID is provided to the user and is used as a secure reference for accessing or sharing the file. When a user requests to access a shared file, the system verifies the request using the provided File ID and checks access permissions.

Authorized users can view their uploaded files through the **View Uploaded Files** interface. When an access request is approved, the encrypted file is retrieved from the cloud storage and passed to the **Access Shared File** module. At this stage, the system performs decryption to convert the file back into its original format.

Finally, the decrypted file is delivered to the authorized user for viewing or downloading. Throughout this process, secure communication and access control mechanisms ensure that only authenticated users can upload, access, or share files. This structured data flow ensures secure file handling while maintaining system efficiency and reliability.

3. CONCLUSIONS

In this paper, a Cyber Security Based File Sharing System has been presented to address the growing security challenges associated with traditional file sharing platforms. With the increasing use of cloud services and online data exchange, protecting sensitive information from unauthorized access and cyber threats has become essential. The proposed system focuses on enhancing data confidentiality, integrity, and secure accessibility through the integration of cyber security mechanisms.

The system architecture incorporates secure user authentication, file encryption, controlled access, and encrypted cloud storage to ensure that files are protected at every stage of the sharing process. By encrypting files before storage and transmission, the system minimizes the risk of data leakage even if the storage infrastructure is compromised. The use of access control mechanisms ensures that only authorized users can upload, access, or share files, thereby improving overall system reliability and trust.

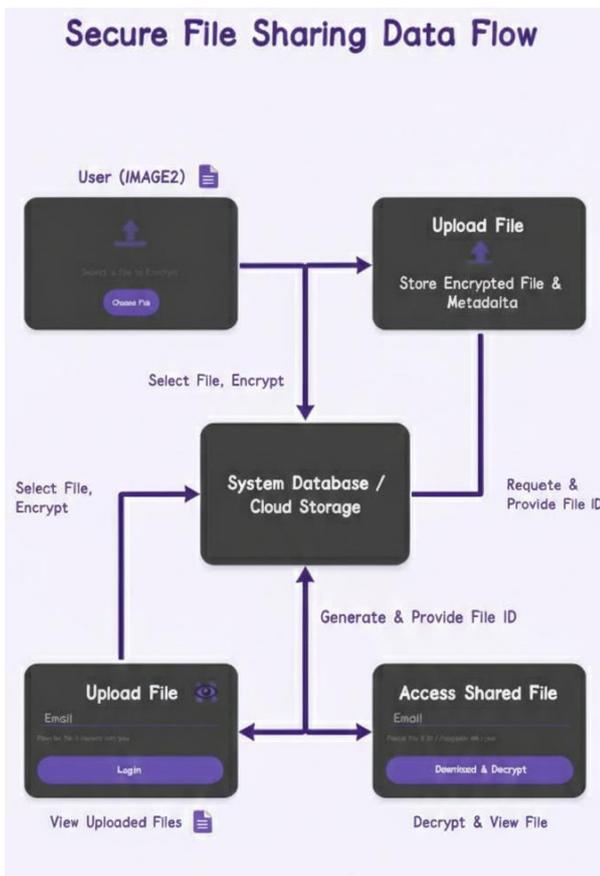


Fig -2: Data Flow Diagram

The Secure File Sharing Data Flow Diagram illustrates the flow of data within the cyber security based file sharing system from file upload to secure access by authorized users. The diagram highlights how encryption, storage, and access control mechanisms are applied at each stage to ensure data confidentiality and security.

The data flow analysis demonstrates that the proposed approach efficiently manages secure file upload, storage, sharing, and retrieval while maintaining system performance. The modular design of the system makes it scalable and adaptable for various real-world applications such as corporate data sharing, educational platforms, and cloud-based storage services.

In conclusion, the cyber security based file sharing system provides a secure and effective solution for modern file sharing requirements. Future enhancements may include the integration of multi-factor authentication, blockchain-based access management, and advanced intrusion detection techniques to further strengthen system security and resilience against emerging cyber threats.

REFERENCES

1. William Stallings, *Cryptography and Network Security Principles and Practice*, 7th Edition, Pearson Education, 2017.
2. Atul Kahate, *Cryptography and Network Security*, 3rd Edition, McGraw- Hill Education, 2018.
3. Behrouz A. Forouzan, *Data Dispatches and Networking*, 5th Edition, McGraw- Hill, 2013.
4. NIST, "companion to Cyber Security," National Institute of norms and Technology, NIST Special Publication 800- 53 and 800- 171.
5. Subashini and V. Kavitha, " A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1 – 11, 2011.
6. Armbrust et al., " A View of Cloud Computing," *Dispatches of the ACM*, vol. 53, no. 4, pp. 50 – 58, 2010.
7. Sahai and B. Waters, " Fuzzy Identity- Grounded Encryption," *Advances in Cryptology – EUROCRYPT*, Springer, 2005.
8. Rivest, A. Shamir, and L. Adleman, " A system for carrying Digital Autographs and Public- Key Cryptosystems," *Dispatches of the ACM*, vol. 21, no. 2, pp. 120 – 126, 1978.
9. Boneh and M. Franklin, " Identity- Grounded Encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586 – 615, 2003.
10. OWASP Foundation, " OWASP Top 10 – Web operation Security pitfalls," OWASP Documentation, 2021.

11. Ren, C. Wang, and Q. Wang, " Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69 – 73, 2012.
12. Buyya, C. Yeo, and S. Venugopal, " request-acquainted Cloud Computing Vision, Hype, and Reality," *Future Generation Computer Systems*, Elsevier, 2009.
13. Mell and T. Grance, " The NIST Definition of Cloud Computing," NIST Special Publication 800- 145, 2011.

ABOUT THE AUTHORS

PROF.ANIL NAIK

HOD, Dept . of Computer Engineering

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)

PROF.MAYUR.G.UHNALE

Guide Dept . of Computer Engineering

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)

MR.SARTHAK . K.PAWAR

Pursuing Poly(Co)

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)

MR.SAGAR . S. SAWANT

Pursuing Poly(Co)

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)

MR.TUSHAR .B. MULE

Pursuing Poly(Co)

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)

MR.SUYOG . Y.THOMBRE

Pursuing Poly(Co)

S.Y.P Shreeyash College of Engineering and Technology (POLYTECHNIC)