International Journal of Scientific Research in Engineering & Technology
Volume6, Issue2 (March-April 2026), PP: 244-248.
https://www.doi.org/10.59256/ijsreat.20260602031
www.ijsreat.com
ISSN No: 2583-1240

Secure File Sharing System with Access Expiry

S.Suman[1], VimalRaj P[2], Venu Madhav G[3], ThulasiRam D T[4], Sunil N[5]
[1]*Assistant Professor: Department of Information Technology, Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*
[2,3,4,5] *UG Scholer, Department of Information Technology, Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

To Cite this Article: *S.Suman[1], VimalRaj P[2], Venu Madhav G[3], ThulasiRam D T[4], Sunil N[5], "Secure File Sharing System with Access Expiry", International Journal of Scientific Research in Engineering & Technology, Volume 06, Issue 02, March-April 2026, PP: 244-248.*

Abstract: *In the digital era, secure sharing of sensitive files has become a major concern for individuals and organizations. This paper proposes a Secure File Sharing System with Access Expiry that enables users to upload and share files securely with controlled access permissions. The system incorporates authentication mechanisms and time-based or view-based access expiry to ensure that files become automatically inaccessible after a specified duration or number of accesses. Additionally, encryption techniques are used to protect files stored on the server, while access logs are maintained to monitor user activity and prevent unauthorized usage. The proposed system enhances data confidentiality, improves security, and ensures controlled file distribution. Experimental implementation demonstrates that the system provides secure, reliable, and efficient file sharing, making it suitable for educational institutions, organizations, and enterprises where confidentiality and controlled document sharing are essential.*

Key Words: *Secure File Sharing, Access Expiry, File Encryption, Authentication, Access Control, Data Security, Cloud Storage*

I. INTRODUCTION

In today's digital world, sharing files over the internet has become a common practice in educational institutions, organizations, and enterprises. However, secure file sharing remains a major challenge due to risks such as unauthorized access, data leakage, and misuse of sensitive information. Traditional file sharing methods like email attachments, cloud links, and messaging platforms often lack proper access control and security mechanisms, which may lead to confidentiality issues.

To address these challenges, a Secure File Sharing System with Access Expiry is proposed. This system allows users to upload files securely and share them with controlled permissions such as time-based expiry and limited number of views. These features ensure that shared files automatically become inaccessible after a specified duration or access limit, reducing the risk of unauthorized distribution.

Additionally, the system incorporates authentication and encryption techniques to protect sensitive files and maintain data privacy. Access logs are also maintained to track user activity and monitor file usage. By integrating these features, the proposed system enhances security, improves file management, and ensures safe sharing of confidential information.

II.LITERATURE SURVEY

In recent years, several studies have focused on improving secure file sharing systems to protect sensitive data from unauthorized access and misuse. Traditional file sharing methods such as email attachments and public cloud storage services provided convenience but lacked strong security features like access control, expiry mechanisms, and encryption. These limitations increased the risk of data leakage and unauthorized distribution.

Researchers introduced secure file sharing systems with authentication and encryption techniques to enhance data confidentiality. Some systems implemented password-protected file sharing, while others used token-based authentication to verify user identity. These approaches improved security but often lacked automated access expiry and proper monitoring mechanisms.

Recent advancements have introduced time-based and view-based access control mechanisms, allowing files to expire after a specific duration or number of accesses. Additionally, logging systems have been implemented to track user activity and detect unauthorized access attempts.

Despite these improvements, challenges such as secure key management, scalability, and user- friendly implementation remain critical issues in developing efficient and reliable secure file sharing systems.

III.METHODOLOGY

A. User Registration and Authentication

The system begins with user registration and authentication to ensure secure access. Users create an account using credentials such as username and password. Authentication mechanisms verify user identity before allowing access to system

features. This helps prevent unauthorized users from accessing sensitive files.

B. File Upload and Access Rule Configuration After authentication, users can upload files to the system. During upload, users define access control rules such as:

- Time-based expiry (e.g., file expires after 24 hours)
- View-based expiry (e.g., limited number of downloads)
- Password protection (optional)

These access rules ensure controlled file sharing and improve data security.

C. Encryption and Secure Storage

Once files are uploaded, encryption techniques are applied to secure the files before storing them on the server or database. The encrypted files are stored securely to prevent unauthorized access.
Only authorized users with valid permissions can access and decrypt the files.

D. File Access and Verification

When a user requests access to a shared file, the system verifies:

- User authentication
- Access expiry time
- Number of allowed views
- File availability

If all conditions are satisfied, the file is made available for download. Otherwise, access is denied.

E. Logging and Monitoring

The system maintains access logs to record user activity such as:

- File access time
- User details
- Number of downloads
- Access status (allowed/denied)

These logs help monitor system usage and detect unauthorized access attempts. The system performance is evaluated based on security, reliability, and controlled file access efficiency.

III.PROPOSED SYSTEM

The proposed system is a secure file sharing system with access expiry.

Workflow:

1. User login
2. File upload
3. Encryption and access control
4. Verification
5. Output result

The system helps users by providing secure and controlled file sharing, reducing unauthorized access.

Fig. 1. Flowchart for the proposed system.

V.ANALYSIS AND COMPARISON

Parameter	Traditional File Sharing	Proposed System
Security	Low	High
Access Control	Limited	Time/View Based
Encryption	Not Available	Available
Unauthorized Access	High	Low
File Expiry	Not Available	Available
Monitoring	Limited	Access Logs

Table I. Comparison of File Sharing Methods

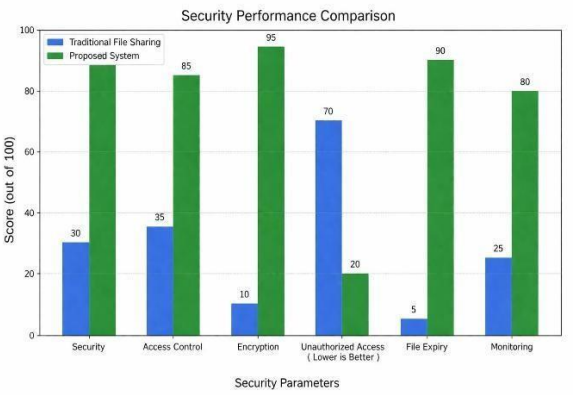

Fig. 2. Graph showing various security performance comparison

Description

Table 1 compares traditional file sharing methods with the proposed secure file sharing system. The comparison includes parameters such as security, access control, encryption, and file expiry. The proposed system provides better security and controlled access compared to traditional methods. Fig. 2 illustrates the graphical comparison of security performance. The figure clearly shows that the proposed system improves security and reduces unauthorized access.

Feature	Traditional System	Proposed System
Authentication	Basic	Strong
Data Protection	Moderate	High
Access Control	Manual	Automatic
Reliability	Medium	High

Table Ii. System Performance Comparison

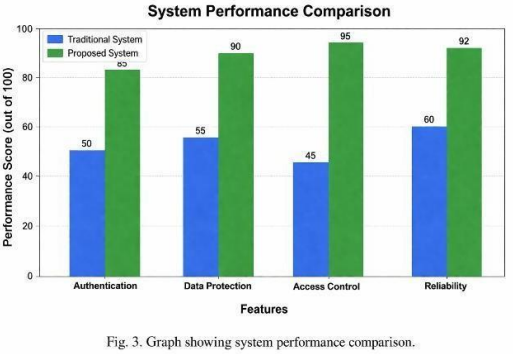

Fig. 3. Graph showing system performance comparison.

Fig. 3. Graph showing system performance comparison

Description

Table 2 presents the system performance comparison between traditional and proposed systems. The comparison includes authentication, data protection, access control, and reliability. The proposed system demonstrates improved performance in all features. Fig. 3 shows the graphical representation of system performance comparison. The figure highlights the efficiency and reliability of the proposed system.

Parameter	Traditional	Proposed
Time Expiry	No	Yes
View Limit	No	Yes
Access Limit	No	Yes
User Control	Low	High

Table Iii. Access Control Comparison

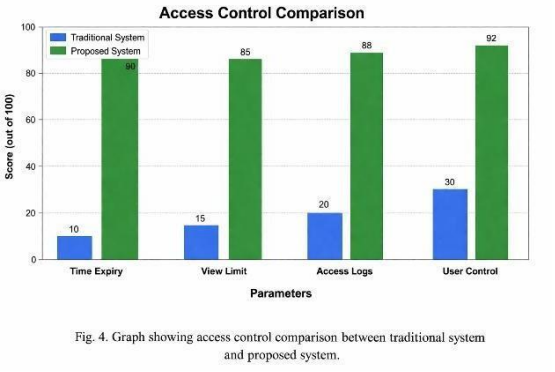

Fig. 4. Graph showing access control comparison between traditional system and proposed system.

Fig. 4. Graph showing access control comparison

Description

Table 3 compares access control features between traditional and proposed systems. The comparison includes time expiry, view limit, access logs, and user control. The proposed system provides advanced access control mechanisms. Fig. 4 illustrates the graphical comparison of access control features. The figure clearly shows that the proposed system performs better in all aspects.

VII.SCOPE OF RESEARCH

This research focuses on developing a secure file sharing system with access expiry to protect sensitive data during file transmission and storage. The study demonstrates how authentication mechanisms, encryption techniques, and access control policies can enhance data security and prevent unauthorized access. The system also implements time-based and view-based expiry features to ensure files become inaccessible after a specified duration or number of accesses, thereby improving data confidentiality and reducing security risks.

The scope of this work can be extended to real-time enterprise applications, integration with cloud storage platforms, and implementation of advanced security mechanisms for improved protection.

Future research may also explore multi-factor authentication, blockchain-based file sharing, and developing the system as a web or mobile application for wider accessibility and better user experience.

VIII.CONCLUSION

This paper presents a secure file sharing system with access expiry for protecting sensitive files. The proposed system provides authentication, encryption, and access control to ensure secure file sharing. The system reduces unauthorized access and improves data confidentiality, making it useful for organizations and institutions. Future improvements can further enhance security and enable real-world deployment.

REFERENCES

1. M. Blaze, G. Bleumer, and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,” *EUROCRYPT*, 1998.
2. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” *IEEE INFOCOM*, 2010.
3. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 6, pp. 847–859, 2011.
4. A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” *EUROCRYPT*, 2005.
5. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABE Ciphertexts,” *USENIX Security Symposium*, 2011.
6. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
7. D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
8. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” *IEEE Symposium on Security and Privacy*, 2007.

9. NIST, "Guide to Storage Encryption Technologies for End User Devices," *National Institute of Standards and Technology*, 2007.
10. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, 2011.
11. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *IEEE Cloud Computing*, 2010.
12. M. Armbrust et al., "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
13. R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
14. OWASP, "Top 10 Web Application Security Risks," *Open Web Application Security Project*, 2021.
15. A. Kumar and R. Singh, "Secure File Sharing System with Access Control and Expiry Mechanism," *International Journal of Computer Applications*, 2022