International Journal of Technology, Leadership and Sciences (IJTLS)

ISSN: 3107-9083
www.ijtls.com
Research Paper
DOI:https://doi.org/10.5281/zenodo.20800612

SECURE MANAGEMENT OF ENCRYPTED CLOUD DATA USING ROLE-BASED ACCESS CONTROL

KORNIPATI SUHASINI[1],S MANI KUMAR[2], DR.VUNNAVA DINESH BABU[3], Dr.CHAVA HARI BABU[4], R.VAMSI KRISHNA[5], D.SRIDHAR[6]

[1]*M.Tech Student,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[2]*Associate Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[3]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[4]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[5]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[6]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

ABSTRACT:

For the sake of the confidentiality, availability, and integrity of sensitive information in today's digital environment, secure storage and limited file access are essential. This project proposes the development of a secure file storage system using advanced encryption and role-based access control (RBAC). This solution will provide data protection and limited access. Access to certain resources inside the system is limited to authorized users with defined roles, such Admin, Manager, or Employee, therefore ensuring the safe upload, storage, and retrieval of data online. To safeguard data at rest and avert illegal access without the requisite decryption key, we encrypt all files uploaded to the system using the Advanced Encryption Standard (AES-256). To augment data security, the system communicates information using encrypted HTTPS connections. Role-based access follows the concept of least privilege by granting users just the rights need for their responsibilities. An administrative interface facilitates comprehensive monitoring and control of system use, allowing for the administration of user accounts, role assignments, and audit logs. Timestamps are assigned to all activity, such as logins, file uploads, downloads, and sharing, to improve accountability and traceability. Organizations aiming to protect sensitive data while ensuring operational flexibility and compliance with security standards can employ this system, which combines strong encryption with exact access control, to meet the increasing demand for secure file management solutions in corporate and personal settings.

Keywords: Secure File Storage, Role-Based Access Control (RBAC), Data Security, File Encryption, Confidentiality, Integrity, Audit Logging, User Authentication, Secure Cloud Storage.

Received Date: 5 June 2026**; Accepted Date:** 15 June 2026**; Published Date:** 20 June 2026;

I. INTRODUCTION

The amount of data created, saved, and sent online is expanding dramatically in our digital age. Individuals and companies are increasingly relying on web-based and cloud-based technology to handle sensitive assets, including financial information, personal papers, corporate data, and secret conversations. Nevertheless, considerable concerns persist over data privacy, unlawful access, and cyberattacks linked to this increasing reliance.

File storage systems are susceptible to breaches, leaks, and abuse in the absence of sufficient security measures, which may result

in considerable financial and reputational harm. Consequently, there is an immediate need for a dependable and secure file storage system that guarantees data confidentiality and allows regulated access.

Encryption is an essential element of data security, guaranteeing that stored information remains inaccessible and useless to unauthorized users, even if they get access to it. The AES-256 algorithm, part of the Advanced Encryption Standard (AES), is considered one of the most secure encryption methods available today. Data security during transmission and at rest may be achieved by the use of AES encryption in file storage systems. Data exposure due to system breaches or physical loss of storage devices may be mitigated by encrypting data before its storage on the server.

Data security relies on encryption and role-based access control (RBAC), which restricts user rights based on their responsibilities. RBAC enables administrators to define specific roles, such as "Admin," "Manager," and "Employee," each assigned certain powers, unlike other access control systems. This restricts user access to just those resources relevant to their work responsibilities. An administrator may have complete authority over all user accounts and file permissions, but an employee may only have access to a restricted subset of those privileges. The use of these access control techniques may alleviate insider risks and inadvertent data leaks.

This project intends to provide a secure file storage system using advanced encryption methods and rigorous role-based access control. Users must authenticate themselves using secure login mechanisms to maintain accountability. Additionally, all system interactions will be observed and recorded. The system will encrypt all data using AES-256 before to storage, and the designated user function will rigorously regulate access to those files. Entities such as corporations and educational institutions that handle sensitive data will find the system's all-encompassing solution for safe file storage very appropriate, as it effectively handles both internal and external security concerns.

II.LITERATURE REVIEW

S. Rajasekaran and M. Priyanka use the Advanced Encryption Standard (AES) algorithm to provide a secure data storage method that safeguards user information. The authors recommend encrypting data before uploading to the cloud to avoid illegal access. Their investigation reveals that AES is an optimum choice for real-time applications because to its speed and security. The research indicates that symmetric encryption is the most efficient method for protecting data while ensuring computing efficacy. This study informed the encryption methodology of the proposed system, namely the use of AES-256 to augment file security and secrecy.

The RBAC model, developed by R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, provides a structured framework for the allocation of rights and duties to govern resource access. The authors provide a taxonomy of RBAC models and illustrate its applicability in corporate settings with many users requiring varied permissions. Adhering to the concept of least privilege, their initiatives guarantee that users get just the rights essential for performing their responsibilities. The implementation of secure user access management in the proposed system is essentially grounded on this study.

C. Wang, Q. Wang, K. Ren, and W. Lou present a cloud-based file storage system that integrates public auditing measures with data encryption, while preserving user privacy. The authors examine techniques to ensure the precision and comprehensiveness of outsourced data while safeguarding sensitive information from auditors. The need of maintaining accountability and trust in cloud storage systems is emphasized by their results. The proposed secure file storage system incorporates features of accountability and transparency based on the principles of logging, monitoring, and audit trails examined in this work.

K. D. Bowers, A. Juels, and A. Oprea analyze the difficulties associated with secure data storage on the cloud and suggest cryptographic measures, including digital signatures and encryption, to address these issues. The authors also discuss secure key management and the protection of file metadata. The importance of

safeguarding both the file content and associated information is critical, as shown by their work. The encryption module and secure metadata management strategy of the proposed system were substantially shaped by these notions.

M. Ali, S. U. Khan, and A. V. Vasilakos examine and distinguish among RBAC, ABAC, and DAC, three prominent access control mechanisms in cloud computing. The authors evaluate the advantages, disadvantages, and potential uses of each model in various computing contexts. Their research demonstrates that RBAC is well suited for organizational use owing to its efficient integration of extensive permission management, scalability, and simplicity. This research illustrates that role-based access control (RBAC) is an efficient and viable method for managing access inside the proposed secure file storage system.

III.EXISTING SYSTEM

The ability to upload, get, and disseminate data is a fundamental feature of modern file storage systems. Prominent providers including Google Drive, Dropbox, and Microsoft OneDrive provide cloud storage equipped with security measures like HTTPS encryption and user authentication. However, the encryption keys for these platforms are often administered by the service provider, since they rely on server-side encryption. The encryption technique and key access are outside the user's control, resulting in security issues. Should the service provider or server be hacked, confidential information may be jeopardized.

Traditional file storage systems are deficient in essential access control mechanisms. The bulk of systems lack granular role-based administration and instead depend on basic permission models, which either fully give or entirely deny access. This complicates the process of assigning rights according to job titles such as "Manager," "Administrator," or "Employee" inside the business. The outcome is a heightened probability of data leakage due to unauthorized persons gaining access to sensitive information. The difficulty of overseeing user activity and detecting fraudulent actions is intensified by the prevalence of systems that provide inadequate audit logging.

Moreover, most current systems cannot integrate structured role-based access control (RBAC) with strong encryption. Many systems still use outdated encryption and access control techniques that lack full integration. This undermines data security and hinders the enforcement of regulations in organizations that need secure and controlled file access.

DISADVANTAGES

- Users have little influence over data security, since the service provider often controls the encryption keys.
- The probability of data leakage increases with server-side encryption if the provider or backend is breached.

IV.PROPOSED SYSTEM

The suggested solution integrates Role-Based Access Control (RBAC) with AES-256 encryption to provide robust data security and regulated access to essential files. It serves as a resolution for access control. Access to the stored data will be limited to authorized persons with relevant organizational duties, guaranteeing its security. After authentication using a secure login method, each user is assigned a role: Admin, Manager, or Employee. This role delineates the rights users have for uploading, downloading, viewing, sharing, and managing files. Employing the concept of least privilege allows us to reduce the danger of unauthorized access or data abuse by limiting personnel to just the information essential for their duties. The AES-256 encryption of all provided files is a critical component of the system. This ensures that data remains inaccessible in the event of unwanted server access, as long as the relevant decryption keys are not compromised. These encryption keys are created and stored securely to ensure their secrecy and prevent misuse. The solution further integrates a multi-tiered RBAC framework. The Administrator is responsible for managing users, permissions, and system settings. The Manager is tasked with reviewing and supervising documents within their department. Employees are permitted to upload and view files that are specifically shared with them or relevant to their respective department. All user activities, including as file uploads, downloads, login attempts, and sharing actions, are painstakingly recorded with timestamps and user information in the system's extensive audit

logging framework. This enables the monitoring and assessment of questionable activities, hence enhancing accountability and transparency. Administrators may monitor logs, user roles, and file permissions in real-time using an admin dashboard, giving them comprehensive control over system operations. The system employs HTTPS and SSL protocols to encrypt data during transmission over the network, protecting files both in transit and at rest. The proposed solution is ideal for organizations such as educational institutions, governmental agencies, and businesses requiring efficient file management with a user-friendly interface. It offers secure file management and role-based access control.

ADVANTAGES

• Employs AES-256 encryption for data before storage.

• Protects private information in the event of a storage server compromise.

V.SYSTEM MODEL

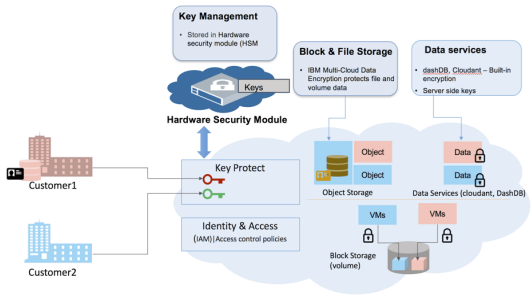


Fig 1.System Model

A more secure, efficient, and scalable framework is proposed to overcome the constraints of current file storage systems; Fig. 1 System Model depicts the whole operating process of this system. The system model begins by assessing user needs, organizational frameworks, and particular data types to develop appropriate security protocols, access rights, and encryption methods for various user groups. The investigation identifies considerable shortcomings in conventional file storage systems, such as insufficient security against internal attacks, inadvertent data disclosure, poor authorization structures, and lack of end-to-end encryption. The suggested methodology combines AES-256 encryption with Role-Based Access Control (RBAC) to overcome these constraints and provide secure file storage with regulated access. Users are designated roles with defined rights and responsibilities inside the system architecture. The positions include Administrator, Manager, and Employee. Users authenticate their identity using a safe verification procedure. By assigning users to specific roles, we may implement the principle of least privilege and limit access to permitted resources related to file uploads, downloads, views, sharing, and management. Files are encrypted using AES-256 before to storage, making them inaccessible without the requisite decryption keys, even in the case of a storage server compromise. The system has a responsive and secure frontend interface, supported by a backend server that stores encrypted files, a relational database for user data, metadata, roles, and audit logs, among other elements. A system administrator may monitor system activities and investigate suspicious actions using an administrative dashboard. All user activities, including file uploads, downloads, login attempts, and sharing actions, are recorded in audit logs, accompanied by timestamps and user details. This enhances accountability. Moreover, files are comprehensively protected during transmission and storage with HTTPS/SSL protocols, which encrypt data in transit. The system model includes properties that provide dependable functionality in real-world organizational settings, such as security, scalability, performance, session management, encryption key management, and secure file-sharing protocols. Figure 1 provides a comprehensive depiction of the architecture and functionalities of the proposed secure file storage system. This model clarifies the cooperation of the system's elements—encryption, authentication, role-based access control, logging, and secure communication—in safeguarding sensitive information and upholding the organization's security protocols.

VI.MODULES

The following modules were developed to improve the project's implementation:

1)New User Signup Here: Application registration process.

2)User Login: Upon system login, users will get a one-time password (OTP) in their email

inbox. Subsequently, they must use this OTP to complete the login process.

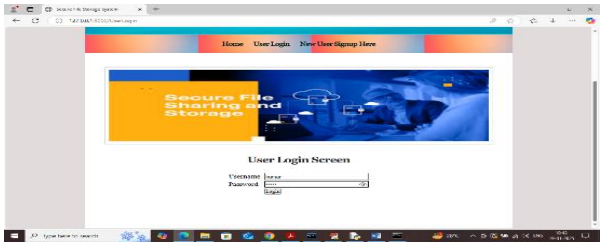
3)Upload & Share File: The user may upload and disseminate files to designated persons. The files will be preserved in an encrypted manner under the static/files directory.

4)Decrypt & Download File: This module allows users to see a detailed list of rights for any files they have uploaded or shared, hence simplifying the download of requested items.

VII.SCREENSHOTS

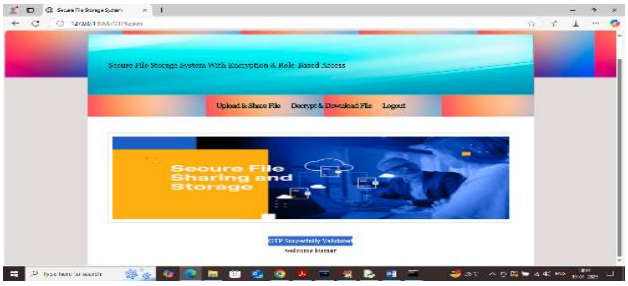
To go to the next page, choose the "New User Sign Up" option on the previous screen.

You may add an infinite number of users on the previous screen; to go to the next page, choose the "User Login" option.

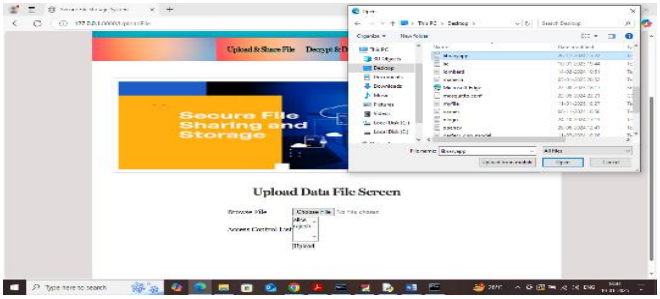


Upon signing in, the user will get a one-time password (OTP) via email, similar to the site mentioned below.

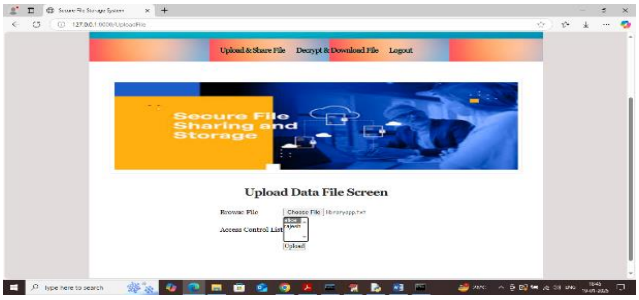
Press the button to go to the next page after verifying your OTP on the previous screen



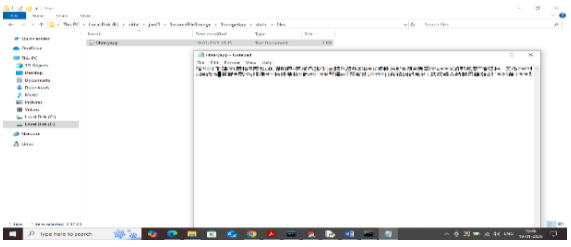
Choose the "Upload & Share File" option on the previous screen to upload the file. Thereafter, go to the website indicated below.



To distribute the file to several persons, press and hold the CTRL key while choosing the users in the specified panel. Thereafter, you may save the file and return to the page below.

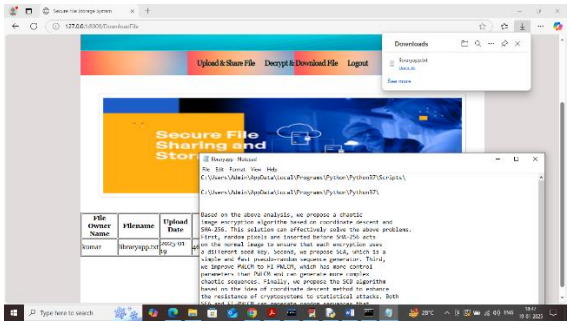


After picking the users on the previous screen, use the button to go to the next page. On the previous screen, assign Alice the job of sharing permission.



All encrypted files will be located in the 'StorageApp/static/files' directory, as shown on the preceding page. You may submit an

unlimited number of files; to see them all, just choose "Decrypt & Download File.



The encrypted file has been downloaded, as seen in the image above.

VIII.CONCLUSION

The proposed secure file storage system efficiently resolves critical challenges encountered by current storage systems via the use of advanced encryption methods and extensive role-based access control. The solution guarantees data security and safeguards against unwanted access during transmission and at rest with AES-256 encryption. This encryption level substantially reduces the probability of data breaches and improves privacy relative to previous storage alternatives using inferior or server-managed encryption.

Role-based access control (RBAC) improves security by limiting file access according to clearly defined user roles, including Admin, Manager, and Employee. This permission model is structured to guarantee that users access just the information essential for their job tasks, in accordance with the concept of least privilege. Thus, the solution ensures adherence to corporate security regulations and reduces the probability of internal data breaches. The adaptability of the RBAC approach enables effortless system growth alongside organizations and their user populations.

The system's extensive logging and auditing functionalities track all user activities in real-time, guaranteeing transparency and accountability. In forensic investigations, identifying dubious conduct and assuring adherence to regulations, these audit trails are crucial. Data in transit is protected by secure communication protocols, which are essential to the comprehensive security architecture necessary in modern digital and threat-prone contexts.

The system is designed for clarity and use, accommodating individuals with diverse levels of technical proficiency. The intuitive interface promotes the upkeep of rigorous security protocols, allowing for effective file management. The system's modular and scalable design facilitates straightforward adaptation and growth to meet the needs of many sectors, including commercial, governmental, and educational entities.

Our secure file storage solution provides robust and practical security for digital assets with advanced encryption and adaptable access control. Users and stakeholders may be certain that sensitive data is protected by a system that combines scalability, usability, and security. This research establishes a solid basis for future improvements to increase data security in dynamic organizational settings. Potential improvements may include cloud-native implementations, advanced threat detection, and multi-factor authentication.

IX.FUTURE ENHANCEMENTS

A multitude of possibilities exists to improve and optimize the secure file storage system, possibly making it more secure, user-friendly, and scalable than it already is.

Implementing multi-factor authentication (MFA) to improve the login process would be an exemplary first step. Passwords, together with one-time codes (OTCs) sent by email or text message, biometric verification, hardware tokens, and biometric authentication, illustrate the multifactor authentication (MFA) techniques required for user implementation. This substantially reduces the danger of unauthorized access, even in the event of compromised login credentials.

The system may be enhanced to include dynamic and context-sensitive access control rules. Permissions may fluctuate depending on variables such as access time, device used, user's geographical location, or behavioral patterns, rather than being static like roles. To enhance flexibility and strengthen protections against internal threats or compromised accounts, access may be limited during non-

business hours or from untrusted devices, for example.

Enhancing data integrity and auditability with blockchain technology need further emphasis for future progress. Logs and file information may be securely maintained on the distributed and immutable ledger of blockchain technology, ensuring that audit trails are both verifiable and unchangeable. Entities undergoing external audits or adhering to stringent compliance requirements would find this very beneficial.

Moreover, using containerization and orchestration technologies like as Kubernetes and Docker may enhance scalability and enable cloud-native deployment. Thus, the system would enable updates and maintenance, improve fault tolerance, and dynamically allocate resources based on demand. A viable solution for safe and scalable encryption key management is the implementation of a cloud-based Key Management System (KMS).

Integrating machine learning methodologies for anomaly identification might enhance the system's efficacy. The system may detect anomalous actions, such repeated unsuccessful login attempts, unusual file access, or possible data exfiltration, by examining user behavior and access patterns. Prompt incident reaction and mitigation may be facilitated by early threat identification.

Ultimately, features like mobile application compatibility, version control, and secure file sharing with other entities will improve user experience and increase system acceptance and flexibility. Automated backup and disaster recovery processes may provide data accessibility and resilience against system faults or assaults.

Upcoming improvements to the secure file storage system will strengthen its robustness, user-friendliness, and comprehensiveness, including features such as adaptive access control, multi-factor authentication, cloud-native scalability, blockchain-based audit trails, and enhanced usability. These enhancements may more effectively handle the developing security landscape and the increasing expectations of contemporary digital companies.

X.REFERENCES

[1] J. Daemen and V. Rijmen, AES Proposal: Rijndael. NIST AES Proposal, 2001.

[2] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[3] N. Koblitz and A. Menezes, “The random oracle model: A twenty-year retrospective,” Designs, Codes and Cryptography, vol. 77, no. 2–3, pp. 587–610, 2015.

[4] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[5] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, “Role-based access control models,” IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.

[6] B. Schneier, Applied Cryptography, 2nd ed. New York, NY, USA: Wiley, 1996.

[7] M. Bishop, Computer Security: Art and Science. Boston, MA, USA: Addison-Wesley, 2003.

[8] D. Eastlake and P. Jones, “US Secure Hash Algorithm 1 (SHA1),” RFC 3174, 2001.

[9] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.

[10] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[11] C. Paar and J. Pelzl, Understanding Cryptography. Berlin, Germany: Springer, 2010.

[12] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.