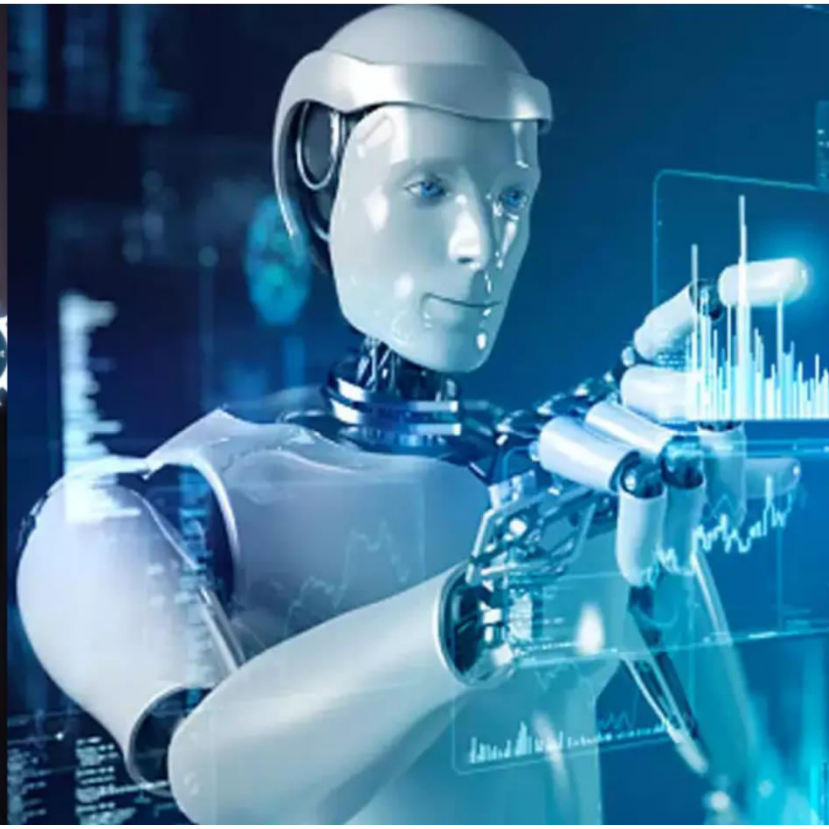
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412077|

Secure File Storage with Hybrid Encryption

Ullas G T, Ms Kavya H V

P.G. Student, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

Assistant Professor, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: Secure data sharing is the modern digital environment's most demanding requirement since it is the most common practice of users to transfer sensitive files through untrusted networks. The authors of the present study have put forth a hybrid cryptographic system that takes advantage of the speed of AES for data encryption and the key protection of RSA to ensure confidentiality and secure key management at a very high level. The proposed model facilitates users to deliver files or texts, set a custom encryption password, and keep the encrypted data in a secure place, while Gmail notifications help to improve communication between the sender and the receiver.

Password-based decryption on the receiver's end ensures that the original content can be retrieved only by the authorized, even when the storage is hacked. A series of experiments showed that the system's performance in terms of speed for encryption was very satisfactory, it had a strong resistance to unauthorized access, and it was easy to use for the application of the real world. In short, this research has resulted in a secure and practical framework for the protection of digital data which is based on hybrid cryptography and user-driven access control.

KEYWORDS: Hybrid Cryptography, AES Encryption, RSA Algorithm, Secure File Storage, Data Protection, Password-Based Encryption, Cloud Security, Secure File Sharing, Authentication, Gmail Notification System.

I. INTRODUCTION

In the era of digital communication and cloud computing, security of data sharing is a requirement of necessity in modern computing. The sensitive data usually goes through untrusted networks, risking it to be accessed by unauthorized persons, also being it possible to get data breaches or even cyberattacks. The research herein proposes a hybrid cryptographic system that is built around AES and RSA for secure key management and it is therefore capable of providing strong protection in both storage and transmission. In addition to the above, the system leverages password-based encryption (PBE) for user-controlled security, while Gmail notifications serve to better the communication between sender and receiver. The merging of all these mechanisms into a single framework brings about the proposed model that is not only practical but also cost-effective, efficient, and secure when it comes to protecting confidential files in real-world applications.

II. LITERATURE SURVEY

Research regarding secure data storage as well as communication with each other constantly emphasizes the hybrid cryptography as the most effective way of protecting sensitive information in both cloud and distributed environments. Among the studies carried out possibly the most prominent ones are those of Maitri and Verma (2016) revealing the combination of AES and RSA increases not only encryption speed but also confidentiality, thereby, Singh and Vora (2016) giving stress to privacy-preserving auditing of the cloud data in encrypted form. Gajendra et al. (2016) achieved a further heightening of data integrity through the use of identity-based encryption in combination with third-party auditing, while Bhandari et al. (2016) proved hybrid methods to be the most flexible and the most trustworthy as compared to any single-algorithm approach. Later studies such as Taha et al. (2018) and Kranthi Kumar and Devi (2018) illustrated that the application of multi-layer techniques in cryptographic methods enhances security in mobile and distributed environments without compromising on usability aspect. Shimbre and Deshpande (2015) gave the nod to AES-based security for distributed storage and Karani et al. (2020) brought forward the practical advantages hybrid cryptography for secure file storage. Additional studies by Khan and Tuteja (2015) and Patil et al. (2016) reiterated the

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412077|

requirement of strong, user-centric encryption for confidentiality maintenance in cloud data sharing. The literature as a whole confirms that hybrid cryptography offers a strong, efficient, and very flexible solution for today's secure data-sharing systems.

III. PROPOSED METHODOLOGY

The suggested approach places a strong emphasis on using a hybrid cryptographic approach to secure file sharing combining RSA for robust key protection with AES for fast and efficient data encryption. The system generates an exclusive AES key to encrypt the content as soon as a sender uploads a file or enters text. This AES key is then encrypted using the recipients RSA public key. Additionally when the sender chooses to assign a unique encryption password a password-based key derivation function is implemented to give users additional control. Unauthorized users cannot access or decode the protected data because all encrypted outputs including ciphertext encrypted keys and associated metadata are stored in the system securely.

On the side of the receiver, the procedure provides a secure and properly authenticated decryption operation. The receiver gets a notification through Gmail once he/she logs into his/her account and then he/she can acesso the file by entering the proper encryption password. The system begins with the decryption of the AES key through RSA and then, if necessary, the password key before decrypting the original data. This whole process ensures confidentiality, integrity, and access control, and thus, it is a reliable method for file storage and transmission security. The combined approach increases security certainly but also facilitates operational efficiency, hence, it can be said that it is suitable for practical implementations where both speed and data protection are required.

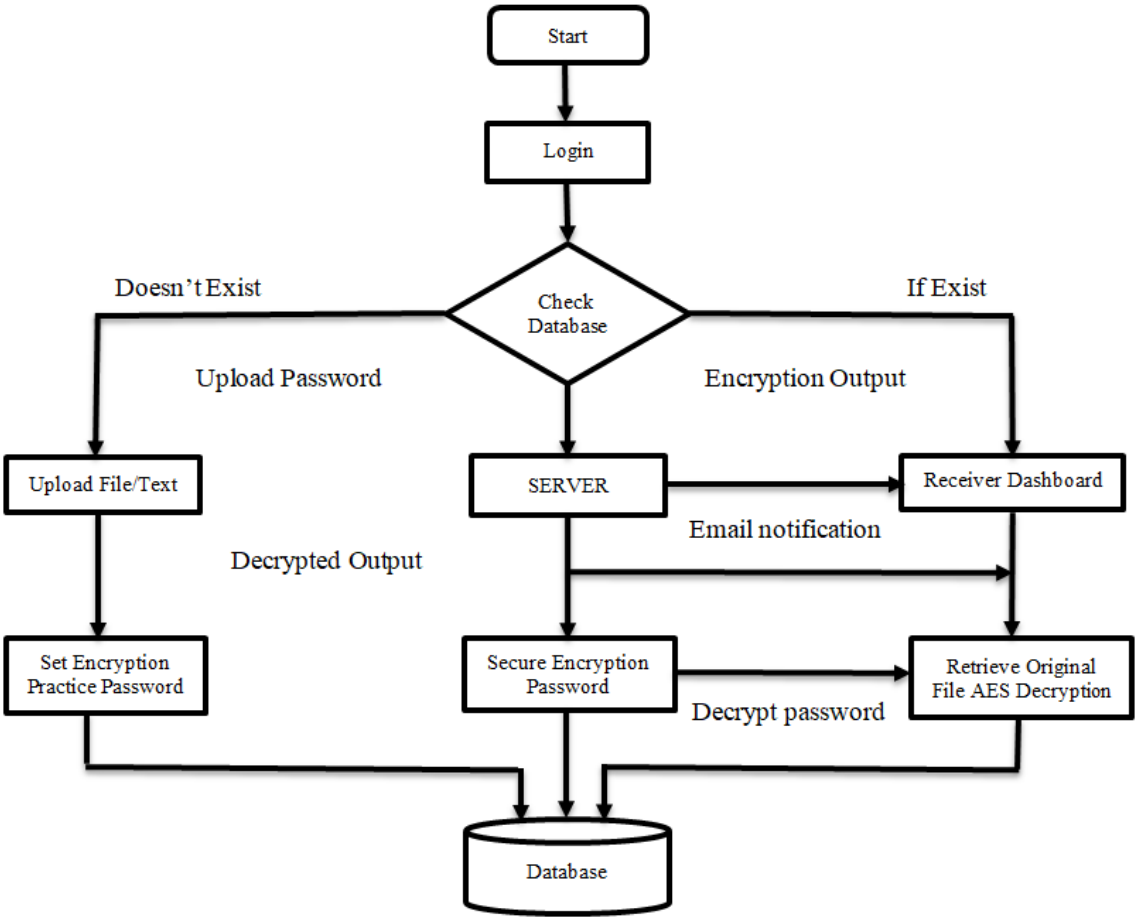


Fig. 1 Data Flow Diagram

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412077|

The Data Flow Diagram depicts the flow of data across the secure file encryption and sharing system, starting with the sender logging in to the dashboard and uploading a file or inputting text with an optional encryption password. The information is transferred to the backend, where an AES key is created, the content is encrypted, and the AES key is secured via RSA or password-based wrapping. The encrypted file along with its metadata and the wrapped key is kept in both secure storage and the database. A Gmail notification is subsequently sent to the receiver to alert him/her/them that the encrypted content is ready. After the receiver logs in and enters the correct password, the system gets the encrypted data that was stored, unwraps the AES key, decrypts the content, and sends the original file or message back. Such a flow guarantees that user data is securely handled at all stages from input till storage, notification, and final decryption, thereby ensuring confidentiality and access control during the entire process.

Algorithms Used: The system employs AES for the purpose of secure, fast, and efficient encryption of both file and text data. RSA is then utilized to secure the AES key thereby allowing only the authorized users to decrypt the content. In the case of a password being set, a KDF enhances the password to become a secure key, thus providing an additional layer of security.

1. AES (Advanced Encryption Standard): Due to its speed and low power consumption for large amounts of data AES is the primary symmetric cipher used for encrypting files and text content. The Galois/Counter Mode or AES-GCM is suggested in this study because it provides integrity (authenticated encryption) and confidentiality in a single action. Use 256-bit keys create a fresh 12-byte nonce or IV for each encryption and retain the 16-byte authentication tag with the ciphertext. AES supports streaming for extremely large files while handling bulk encryption with very little CPU/memory impact.
2. RSA (Rivest–Shamir–Adleman): RSA is mainly used for secure key management rather than for encrypting data directly. The intended recipients public key is used to encrypt (wrap) the AES session key making it unreadable by anyone without the matching private key. RSA-OAEP padding is recommended for security purposes against chosen-ciphertext attacks. RSA key sizes of at least 2048 bits are recommended (3072+ bits are preferred for long-term security) and the private keys should be kept safe (encrypted during storage or stored in a secure keystore/HSM).
3. Password-Based Key Derivation Function (KDF): When a sender chooses a unique encryption password the KDF transforms it into a strong symmetric key that can be used to either add an extra encryption layer or wrap the AES key. Argon2 is the suggested technique for contemporary deployments (memory-hard GPU cracking resistant) PBKDF2 or scrypt are the other options that are still deemed suitable. To achieve the ideal balance between security and usability it is always a good idea to use a random salt (of at least 16 bytes) and carefully adjust work factors (iterations/memory). To ensure accurate key derivation during decryption store the salt and KDF parameters in the metadata.

Testing:
Testing was performed to verify that all system functions such as login, file upload, encryption, and decryption work correctly and securely. Different scenarios were checked to ensure errors, wrong passwords, and unauthorized access are properly handled. The results confirmed that the system is reliable, secure, and user-friendly.

1. Unit Testing: Tests individual functions like encryption, decryption, and file handling.
2. Integration Testing: Ensures modules such as login, storage, and encryption work smoothly together.
3. System Testing: Checks the whole application to verify all features operate correctly.
4. Security Testing: Ensures protection against unauthorized access, wrong passwords, and attacks.
5. Acceptance Testing: Ensures the system meets user expectations before deployment.

Test Cases:

Test ID	Module	Input	Expected Output	Status
TC-01	User Registration	Name, valid email, strong password	Account created, confirmation saved in DB, success message shown	Pass
TC-03	User Login	Registered email, correct password	Login success, session/JWT issued, access to dashboard	Pass
TC-05	File Upload	PDF/image/text file under limit	Upload accepted, file stored temporarily, encryption begins, metadata saved	Pass
TC-06	File Download &	A previously uploaded	The user receives a decrypted file identical	Pass

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

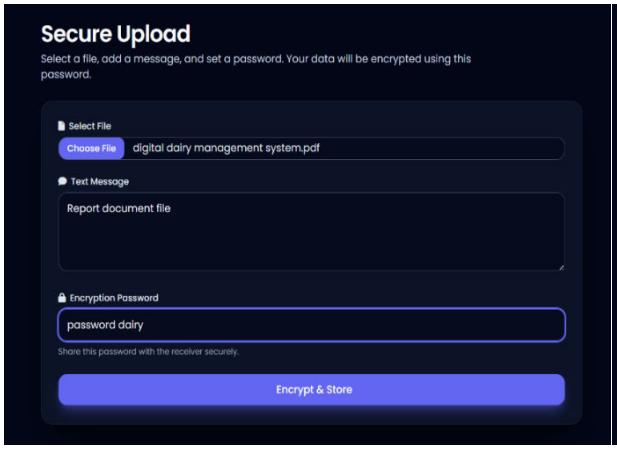
Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412077|

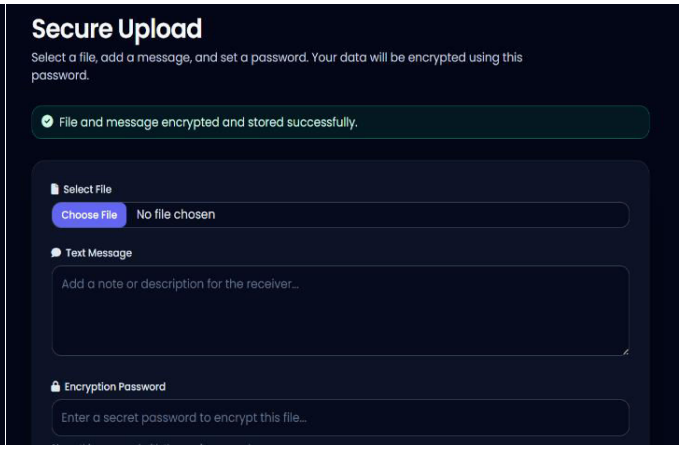
	Decryption	encrypted file	to the original	
TC-07	Text Encryption	Plain text with punctuation and unique code	Encrypted ciphertext returned/stored; original cannot be read from storage	Pass
TC-08	Custom Encryption Password	Password during upload, same password during decrypt	Password-based unwrap succeeds; file/text decrypts correctly	Pass
TC-09	Wrong Encryption Password	Wrong password at decrypt step	Decryption denied, error shown; attempt logged, no plaintext returned	Pass
TC-10	Gmail Notification Sent	Upload + share action with recipient email	Gmail API/SMTP called; email delivered notification status saved	Pass

IV. EXPERIMENTAL RESULTS

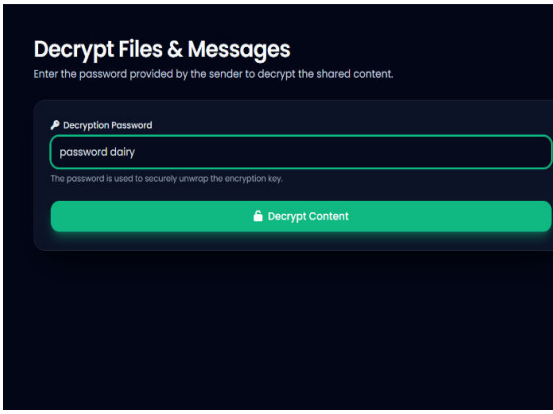
The results show that the files on the sender dashboard have been successfully encrypted with a password and their secure storage has been guaranteed. When the recipient enters the right password the decrypted file can be downloaded and the original message is restored. Furthermore Gmail notifications are operating flawlessly as a result the sender is notified when a file has been decrypted and the recipient is notified when a file is uploaded. Overall the system reliably completes encryption decryption and notification tasks.



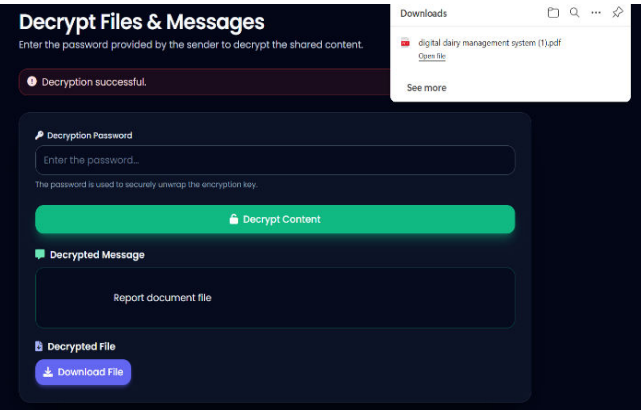
FILE ENCRYPTION SECTION



FILE, AND MESSAGE ENCRYPTED



Receiver Decryption Dashboard



Receiver Decryption Results

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412077|

V. CONCLUSION

By combining hybrid cryptography with password protection the proposed system demonstrates a good way to share files securely. While RSA provides secure key protection preventing unwanted access AES ensures fast and reliable file and message encryption. The user-defined encryption password increases confidentiality and gives the user more control over data security. The systems well-organized workflow which includes upload encryption notification and decryption demonstrates that a user-friendly interface can help achieve high security.

Every important feature of the system including encryption decryption password validation and file recovery is stable according to the experiments. By alerting users when a file will be shared or decrypted Gmail notifications are essential for communication. The system can be utilized by both private individuals and organizations because it is a dependable user-friendly and secure solution for todays file sharing requirements.

REFERENCES

[1] Maitri, P. V., & Verma, A. (2016). *Secure file storage in cloud computing using a hybrid cryptography algorithm*. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 1635–1638.
[2] Shaikh, S., & Vora, D. (2016). *Secure cloud auditing over encrypted data*. 2016 International Conference on Communication and Electronics Systems (ICCES).
[3] Gajendra, B. P., Singh, V. K., & Sujeet, M. (2016). *Achieving cloud security using third party auditor, MD5, and identity-based encryption*. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304–1309.
[4] Bhandari, A., Gupta, A., & Das, D. (2016). *Secure algorithm for cloud computing and its applications*. 6th International Conference on Cloud System and Big Data Engineering (Confluence), 188–192.
[5] Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). *An improved security schema for mobile cloud computing using hybrid cryptographic algorithms*. Far East Journal of Electronics and Communications, 18(4), 521–546.
[6] Kranthi Kumar, K., & Devi, T. (2018). *Secured data transmission in cloud using hybrid cryptography*. International Journal of Pure and Applied Mathematics, 119(16), 3257–3262.
[7] Shimbre, N., & Deshpande, P. (2015). *Enhancing distributed data storage security for cloud computing using TPA and AES algorithm*. 2015 International Conference on Computing Communication Control and Automation (ICCUBEA).
[8] Karani, R., Choudhari, T., Bhajan, A., & Nashipudimath, M. (2020). *Secure file storage using hybrid cryptography*. International Journal of Innovative Research in Technology, 6(9).
[9] Khan, S. S., & Tuteja, R. R. (2015). *Security in cloud computing using cryptographic algorithms*.
[10] Patil, A., Patel, N., & Patel, H. (2016). *Secure data sharing using cryptography in cloud environment*.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details