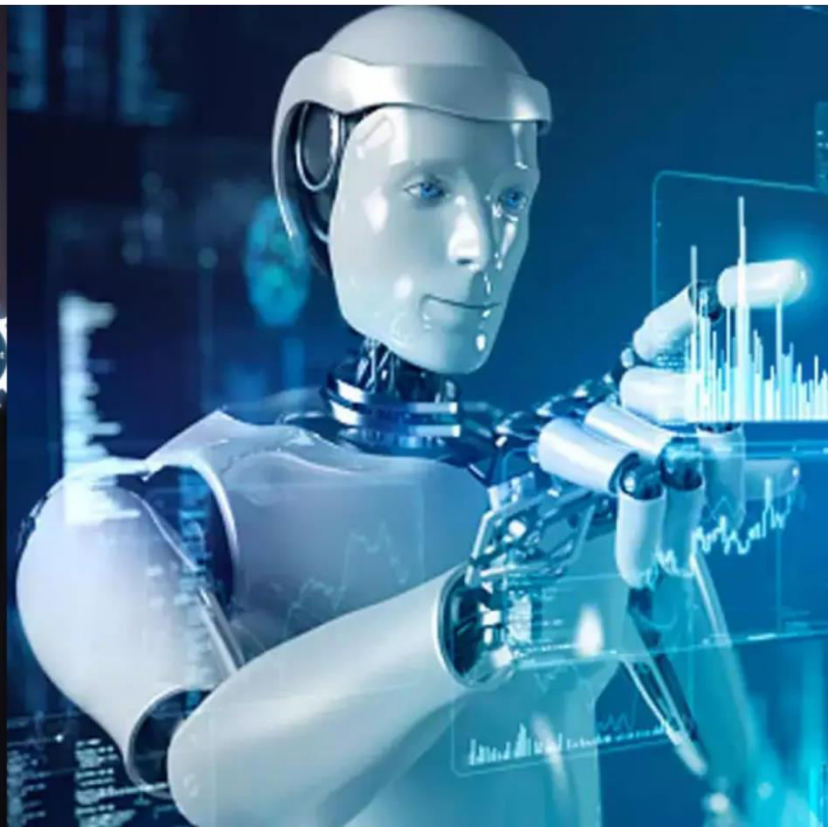
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 15, Issue 4, April 2026

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

A Cryptography Based Secure File Encryption System

Somagani Venkatesh, Prasanna Laxmi Siddenki, Bharath Kumar Gaddam

Department of CSE (AI&ML), ACE Engineering College, Hyderabad, Telangana, India

ABSTRACT: In today's digital world, keeping data safe is very important. Many people store and share files using cloud storage, online platforms, and remote systems. Because of this, there is a higher risk of cyber-attacks, hacking, and unauthorized access to sensitive information. Protecting important files from misuse has become a major need.

This project presents a Cryptography-Based Secure File Encryption System that protects files by converting them into a secure, unreadable format using encryption techniques. Only users who have the correct key can decrypt and access the original file. The system includes secure key generation, encryption, and decryption processes to ensure data remains safe during storage and sharing.

By using strong cryptographic methods, the system helps maintain data privacy, prevents unauthorized access, and keeps sensitive information secure in modern digital environments.

KEYWORDS: Cryptography, File Encryption, Data Security, Decryption, Encryption Algorithms, Key Management, Confidentiality.

I. INTRODUCTION

Today, digital information is growing very fast. People store and share files through cloud storage, websites, emails, and other online platforms every day. While this makes communication and data sharing easier, it also increases the risk of data leakage and cyber-attacks. Sensitive information can be stolen, misused, or accessed by unauthorized users if proper security measures are not used.

To solve this problem, a Cryptography-Based Secure File Encryption System is developed to protect digital files. This system uses mathematical techniques to convert normal files into an encrypted format that cannot be read without the correct key. Even if someone gains access to the file, they will not be able to understand the content without proper authorization.

The system also allows authorized users to decrypt the file and restore it to its original form. By using encryption keys as access control, it ensures that only permitted users can view or modify the data.

Overall, this approach improves data security, builds trust in digital storage systems, and reduces risks associated with cloud storage, file sharing, and online communication. It provides a reliable solution for managing and protecting sensitive information in modern computing environments.

II. LITERATURE SURVEY

[1] An Efficient Lattice-Based Verifiable Public-Key Authenticated Encryption With Keyword Search Scheme, Saba Karimiani, Taraneh Eghlidos (2025)

The paper proposes a verifiable Public-Key Authenticated Encryption with Keyword Search (PAEKS) scheme based on the Middle-Product Learning With Errors (MP-LWE) problem. The approach integrates sender authentication to resist insider attacks, lattice trapdoor techniques for verifiability, and structured lattice constructions to reduce overhead.

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

The proposed scheme achieves strong resistance against Chosen Keyword Attacks (CKA) and Inside Keyword Guessing Attacks (IKGA) in the Random Oracle model. It significantly reduces computation and communication costs compared to existing LWE-based PEKS and PAEKS schemes while maintaining post-quantum security.

[2] An Intelligent Audio Encryption and Compression Algorithm Inspired by the Encoding of Various Biological Sequences, Mohammad Nassef (2025)

The paper proposes an Audio-to-Peptide (A2P) framework that encrypts and compresses raw WAV audio files by mimicking the biological encoding process of DNA → RNA → peptide sequences. An Artificial Neural Network (ANN) is trained to automatically generate key parameters based on audio characteristics such as frequency and file size, eliminating user involvement in key selection

Experimental results demonstrate that the A2P algorithm provides strong resistance against known security attacks, including brute-force attacks. The encrypted output is highly scrambled, non-correlated with the original audio, and smaller in size due to integrated compression.

[3] An Inner Product Predicate-Based Medical Data-Sharing and Privacy Protection System, Zigang Wu, Haijiang Wang, Jian Wan, Lei Zhang, Jie Huang (2024)

The paper presents an IPPE-based medical data sharing system that embeds access policies into ciphertexts using inner product predicates to enable fine-grained, privacy-preserving access control with secure encryption, key generation, and verification across medical institutions.

The system guarantees medical data confidentiality and access policy privacy, resists chosen-plaintext attacks, and achieves lower computational overhead than existing schemes, making it practical for medical data sharing.

[4] Descriptor: Benchmarking Secure Neural Network Evaluation Methods for Protein Sequence Classification (iDASH24), Arif Harmanci, Luyao Chen, Miran Kim, Xiaoqian Jiang (2024)

The authors present the iDASH24 homomorphic encryption benchmarking dataset, featuring protein sequences and a transformer-based classifier to evaluate secure encrypted inference using accuracy and execution time under standardized security settings.

The dataset standardizes benchmarking for secure transformer inference, and iDASH24 results demonstrate that homomorphic encryption can achieve practical accuracy and runtime while preserving data privacy.

[5] A Novel Hybrid Multikey Cryptography Technique for Video Communication, Youcef Fouzar, Ahmed Lakhssassi, M. Ramakrishna (2023)

A hybrid multi-key cryptography framework combining RSA, ECC, and AES. Video data is split into chunks, and each chunk is encrypted using a dynamically generated unique key. Keys are generated automatically using ECC without explicit key exchange.

The proposed method improves security by isolating video chunks with separate keys while maintaining real-time performance. Experimental results show resistance to brute-force attacks and efficient encryption/decryption suitable for live video streaming.

[6] An Audio Encryption Scheme Based on Empirical Mode Decomposition and 2D Cosine Logistic Map, Alenrex Maity, Bibhas Chandra Dhara (2023)

The paper proposes an audio encryption scheme that combines Empirical Mode Decomposition (EMD) with a 2D Cosine Logistic chaotic map. Audio signals are decomposed into intrinsic mode functions (IMFs) using EMD. Chaotic sequences generated by the 2D Cosine Logistic map are used for scrambling and diffusion of audio components to enhance security.

Security analysis shows that the proposed scheme has a large key space, high key sensitivity, and strong resistance against statistical, differential, and brute-force attacks. Experimental results demonstrate low correlation between original and encrypted audio signals and good reconstruction quality after decryption.

[7] ESVSSE: Enabling Efficient, Secure, Verifiable Searchable Symmetric Encryption, Zhenkui Shi, Xuemei Fu, Xianxian Li, Kai Zhu (2022)

The paper proposes ESVSSE, a secure and efficient verifiable searchable symmetric encryption scheme. The design minimizes verification costs while preserving forward and backward privacy and supporting dynamic data updates.

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

Security analysis proves that ESVSSE achieves confidentiality, verifiability, and resistance against malicious cloud servers. Performance evaluation shows that ESVSSE significantly reduces computation and communication overhead compared to existing verifiable SSE schemes, making it suitable for practical cloud storage applications.

III. EXISTING SYSTEM

In the existing system, file protection is often limited to simple password-based security. Many systems rely on basic encryption tools that may not use strong algorithms. Some files are stored without encryption, making them vulnerable to unauthorized access. Traditional methods may not include secure key generation and management practices. Authentication mechanisms are often limited to single-layer verification. Existing systems may lack proper logging and monitoring features. They may not provide protection against advanced cyber threats. Performance issues can arise when encrypting or decrypting large files. Scalability is limited in many traditional encryption solutions. Cloud storage integration is often not securely implemented. Error handling and recovery mechanisms may be insufficient. Compatibility across different platforms can be restricted. Regular security updates may not be consistently maintained. Therefore, existing systems highlight the need for a more advanced and secure encryption solution.

IV. PROPOSED SYSTEM

The proposed Cryptography Based Secure File Encryption System provides enhanced security using advanced encryption algorithms like AES and RSA. It integrates secure user authentication and proper key management mechanisms. Files are encrypted before storage or transmission to ensure complete data protection. The system includes logging and monitoring features to detect unauthorized activities. It is designed to handle large files and multiple file formats efficiently. Overall, the proposed system offers improved security, scalability, and reliability compared to existing methods. It implements secure key rotation and encrypted key storage to prevent key compromise. Cloud integration is supported to enable secure remote file access and backup. Advanced error handling ensures system stability and reliable recovery mechanisms. Overall, the system is designed to be future-ready, adaptable, and resistant to evolving cyber threats.

V. METHODOLOGY

i. User Authentication and Access Control
The system authenticates users through a secure login and registration mechanism using hashed passwords. Only verified users are granted access to the dashboard and encryption features.
ii. File Acquisition and Validation
The user selects a file, and the system validates its type, size, and integrity. Validated file metadata is displayed before proceeding to encryption.
iii. Secure Key Generation
A strong cryptographic key is generated using AES (and optionally RSA for key protection). The key is securely stored or provided to the user for safe handling.
iv. File Encryption Process
The selected file is converted into binary format and encrypted using AES-256.An encrypted file with a new extension (e.g., enc) is generated.
v. Secure Storage and Key Handling
The encrypted file is securely stored on the server or provided for download. Access to the file is restricted without the correct encryption key.
vi. File Decryption Process
The user uploads the encrypted file and provides the correct decryption key. The system decrypts the file and restores the original data.
vii. Integrity Verification
A hash function such as SHA-256 is used to verify file integrity. Any mismatch in hash values indicates tampering or corruption.
viii. Error Handling and Logging
The system displays appropriate error messages for incorrect keys or corrupted files. All encryption and decryption activities are logged for auditing purposes.

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

ix. Secure Session Termination

The user logs out, and the system securely clears session data.The user is redirected to the login page to prevent unauthorized access.

VI. SYSTEM ARCHITECTURE

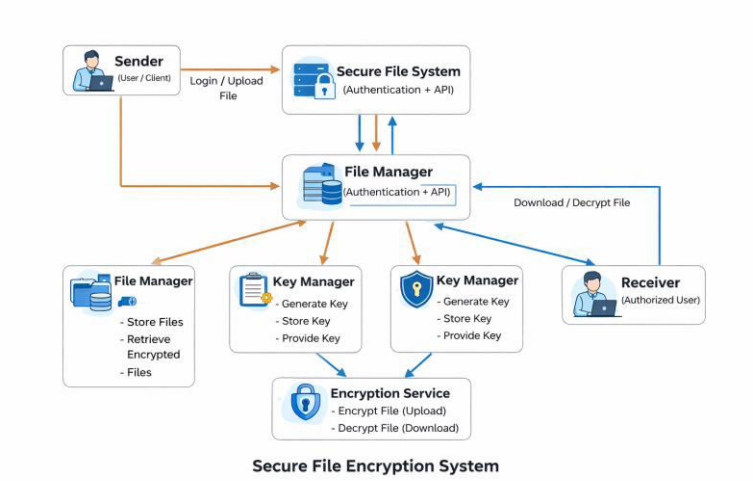


Fig 6.1: System Architecture Diagram of A Cryptography Based Secure File Encryption System

The architecture of a Cryptography-Based Secure File Encryption System ensures secure storage and transmission of data using a combination of Advanced Encryption Standard and RSA algorithm. The process begins when the sender (user/client) uploads a file through a secure interface, where authentication is performed by the secure file system. Once verified, the file is passed to the encryption service, which encrypts the data using AES for efficient and strong protection. Simultaneously, the key manager generates and manages cryptographic keys, ensuring they are securely stored and handled. The AES key used for encryption is further protected using RSA to enable secure key exchange.

After encryption, the file manager stores the encrypted file and handles retrieval requests. When an authorized receiver requests the file, the system authenticates the user and retrieves both the encrypted file and the corresponding key. The key manager provides the necessary decryption key securely, and the encryption service decrypts the file before delivering it to the receiver. This architecture ensures confidentiality, integrity, and controlled access by combining efficient encryption, secure key management, and authentication mechanisms, making the system robust against unauthorized access and data breaches.

VII. RESULTS AND OUTPUT

Fig 7.1: Dashboard

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

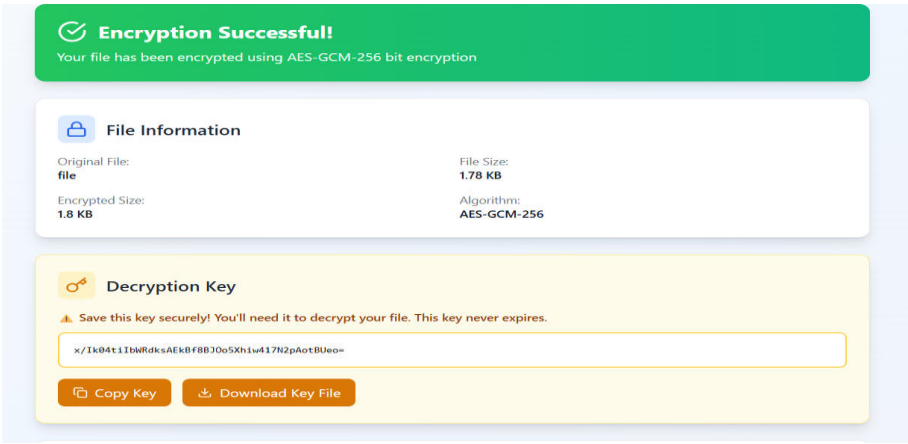


Fig 7.2: Successful encryption of a file

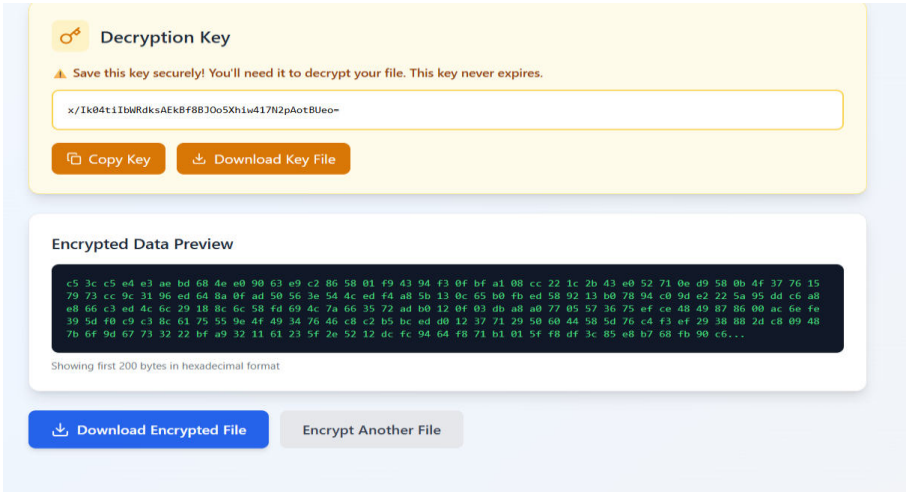


Fig 7.3: Generation of a decryption Key

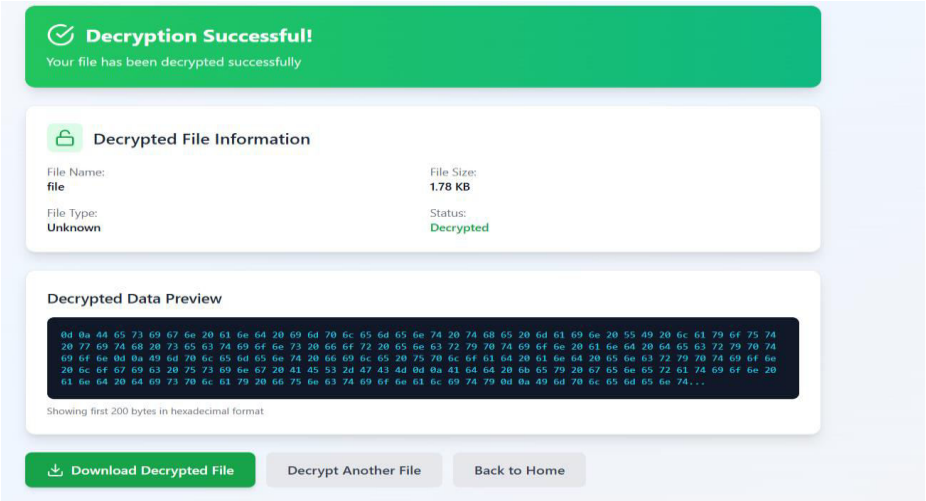


Fig 7.4: Successful decryption of a file

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 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504095|

VIII. CONCLUSION

The Cryptography-Based Secure File Encryption System provides a secure and reliable solution for protecting sensitive data from unauthorized access. By integrating strong cryptographic techniques such as AES for encryption, optional RSA for secure key handling, and SHA-256 for integrity verification, the system ensures confidentiality, data integrity, and controlled access. The implementation of secure user authentication and hashed password storage further strengthens system security.

Overall, the proposed system demonstrates efficiency, scalability, and practical applicability in real-world environments where data protection is critical. With proper key management, secure storage, and structured error handling mechanisms, the system offers a comprehensive approach to secure file encryption and decryption, making it suitable for individuals, organizations, and cloud-based applications.

IX. FUTURE SCOPE

The Cryptography-Based Secure File Encryption System can be further enhanced by integrating advanced security features such as multi-factor authentication (MFA) and biometric verification to strengthen user authentication. Future improvements may also include implementing advanced encryption modes like AES-GCM for authenticated encryption, automated key rotation mechanisms, and secure cloud-based key management systems to enhance scalability and enterprise-level deployment.

Additionally, the system can be extended to support cloud storage integration, mobile application compatibility, and real-time encrypted file sharing between users. Incorporating blockchain technology for tamper-proof audit logs and exploring post-quantum cryptographic algorithms can further improve long-term security, making the system more robust against emerging cyber threats.

REFERENCES

[1] Saba Karimiani, Taraneh Eghlidos. “An Efficient Lattice-Based Verifiable Public-Key Authenticated Encryption with Keyword Search Scheme”. IEEE Access. 2025.
[2] Mohammad Nassef. “An Intelligent Audio Encryption and Compression Algorithm Inspired by the Encoding of Various Biological Sequences”. IEEE Access.2025.
[3] Zigang Wu, Haijiang Wang, Jian Wan, Lei Zhang, Jie Huang. “An Inner Product Predicate-Based Medical Data-Sharing and Privacy Protection System”. IEEE Access. 2024.
[4] Arif Harmanci, Luyao Chen, Miran Kim, Xiaoqian Jiang. “Descriptor: Benchmarking Secure Neural Network Evaluation Methods for Protein Sequence Classification (iDASH24)”. IEEE Data Descriptor. 2024.
[5] Youcef Fouzar, Ahmed Lakhssassi, M. Ramakrishna. “A Novel Hybrid Multikey Cryptography Technique for Video Communication”. IEEE Access. 2023.
[6] Alenrex Maity, Bibhas Chandra Dhara. “An Audio Encryption Scheme Based on Empirical Mode Decomposition and 2D Cosine Logistic Map”. IEEE Access. 2023.
[7] Zhenkui Shi, Xuemei Fu, Xianxian Li, Kai Zhu. “ESVSSE: Enabling Efficient, Secure, Verifiable Searchable Symmetric Encryption”. IEEE Transactions on Information Forensics and Security. 2022.

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