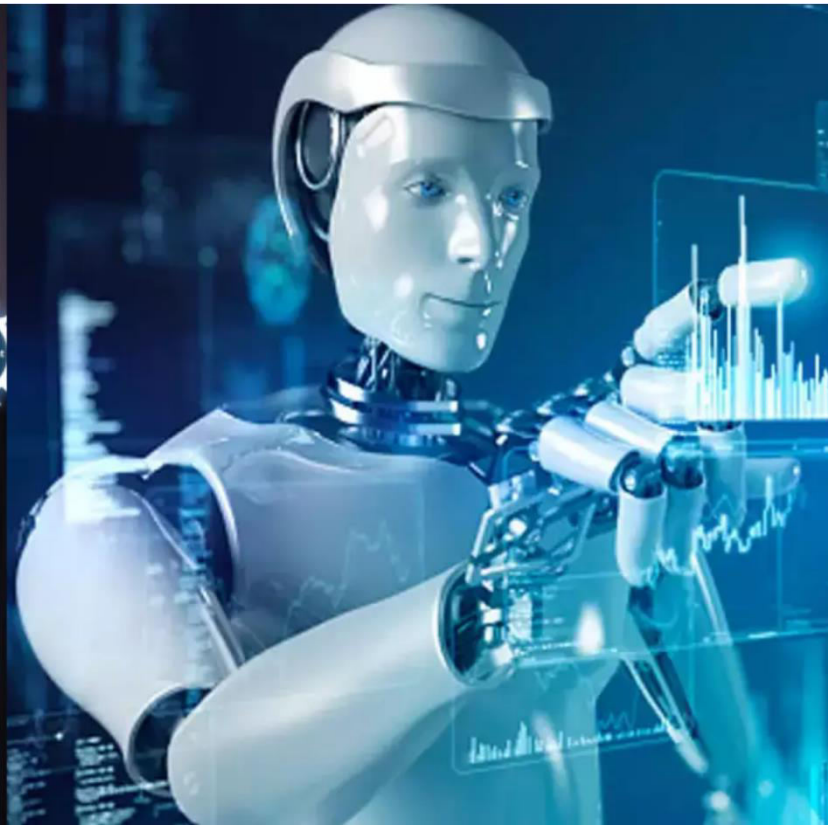
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 4, April 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 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404150|

Secure File Sharing using AES with Deep Learning-Based Key Generation

Ms. N. Kameshwari, S. Dinesh Kumar

Assistant Professor, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

B. Tech Students, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

ABSTRACT: This paper presents a secure file-sharing system that integrates deep learning-based key generation with AES encryption to ensure confidential data transmission. The application enables users to upload and share files securely by registering and generating a unique user ID. A Deep Learning model is employed to generate robust, non-predictable encryption keys, enhancing resistance against brute-force attacks. The encrypted files are stored and associated with the recipient's user ID for controlled access. A user-friendly interface, developed using Flask and Bootstrap, allows users to easily upload, encrypt, send, and decrypt files. MongoDB is used for efficient data management and user authentication. Experimental evaluations validate the system's capability to securely manage file exchanges while maintaining usability. The proposed model contributes to modern cybersecurity solutions by integrating AI-driven cryptographic key management, promoting secure digital communication and data protection.

KEYWORDS: AES Encryption, Deep Learning, Secure File Sharing, Key Generation, Access Control, Data Privacy, Confidentiality, End-to-End Encryption.

I. INTRODUCTION

Data breaches and unauthorized access to sensitive files have become critical concerns in the digital age, especially with the increasing reliance on online data exchange for personal, professional, and organizational use. Traditional encryption techniques, while effective, are often vulnerable to brute-force attacks or misuse of static encryption keys, making it essential to develop more dynamic and intelligent security solutions. There is a growing demand for systems that can securely transmit data while ensuring access control and minimizing the risk of interception or misuse. Existing file-sharing systems depend heavily on predefined encryption keys and simple access protocols, which may not be sufficient against modern cybersecurity threats. Manual key management introduces potential weaknesses, such as key leakage, reuse, or predictable key patterns.

Moreover, many platforms lack built-in mechanisms to verify the identity of recipients or enforce restricted access, increasing the possibility of data being exposed to unintended users. Therefore, a smarter, more secure, and user-controlled file sharing mechanism is needed—one that ensures confidentiality, data integrity, and scalability.
The challenge lies in creating a system that not only protects the files during transfer and storage but also offers intelligent key generation, user-friendly interfaces, and real-time control over who can access what. Traditional methods may also struggle with balancing usability and security, especially for users unfamiliar with encryption tools. The ideal solution must be lightweight, intuitive, and capable of integrating advanced cryptographic techniques with minimal user intervention.

To address these limitations, this study proposes a secure file-sharing platform that leverages AES encryption combined with Deep Learning-based key generation to enhance security and resist brute-force decryption. The objective is to develop an intelligent, real-time system where users can register to generate unique user IDs, encrypt files using dynamically generated keys, and securely share them with intended recipients through an access-controlled mechanism. With a Flask-based backend, Bootstrap frontend, and MongoDB for data handling, the system ensures a

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 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404150|

seamless and secure file exchange process. This research contributes to the field of AI-driven cybersecurity by offering a novel approach to secure digital communication, combining deep learning and encryption to safeguard sensitive information in a user-friendly and scalable environment.

II. LITERATURE REVIEW

Secure data sharing has gained significant research attention due to the growing threats of cyberattacks, data leaks, and unauthorized access in digital communications. Existing approaches to secure file transfer generally fall into three categories: conventional encryption-based methods, user-authentication systems, and cloud-based secure storage services. While traditional encryption algorithms like AES and RSA provide strong security, they often rely on manually managed or static keys, which are susceptible to attacks if compromised. Authentication-based systems focus on access control but do not always ensure end-to-end data confidentiality. Meanwhile, cloud-based services can introduce third-party dependencies and potential privacy concerns.

Recent advancements in artificial intelligence, especially in deep learning, offer new opportunities to improve the security and intelligence of cryptographic systems. However, most deep learning integrations in cybersecurity are either complex, computationally intensive, or lack real-time responsiveness. Existing models also struggle to balance ease of use with the depth of protection required for modern data-sharing needs, especially for non-technical users.

This study proposes a lightweight, deep learning-enhanced file-sharing system that utilizes AES encryption with dynamic key generation powered by a Convolutional Neural Network (CNN). Unlike conventional systems, this model automatically generates unique, unpredictable encryption keys for each file transfer, mitigating the risk of brute-force attacks and static key vulnerabilities. The system is built to operate efficiently in real-time and resource-limited environments, using Flask for the backend, MongoDB for user and file management, and a responsive UI built with Bootstrap. Designed with practicality in mind, the application ensures that users can register, generate unique user IDs, upload files, encrypt them, and share them securely with designated recipients—who can decrypt them using their own ID and the provided decryption key.

This work addresses key limitations of earlier systems by combining the strengths of deep learning, modern cryptography, and user-centered design, offering an efficient, robust, and secure solution for digital file sharing.

III. METHODOLOGY

The proposed methodology for secure file sharing begins with a user registration process, where individuals provide a username and email to generate a unique user ID. This ID serves as a personalized identifier and access credential for secure communication. Once registration is complete, the user can initiate the file encryption process by uploading a file through the platform. Simultaneously, a Deep Learning model is employed to generate a unique and robust encryption key, ensuring enhanced resistance against brute-force and pattern-based attacks. The file is encrypted using the AES (Advanced Encryption Standard) algorithm, with the deep learning-generated key as the cipher. The deep learning model is a lightweight neural network trained on a dataset of randomized byte patterns to learn complex key structures. It consists of fully connected layers with dropout regularization to prevent overfitting and ensure high entropy in generated keys. The model is optimized using the Adam optimizer and mean squared error as the loss function, allowing it to generate consistent yet unpredictable key outputs.

During encryption, the user is prompted to enter the recipient's User ID. The encrypted file, along with the necessary metadata, is stored in a MongoDB collection associated with the recipient's ID. This access-control mechanism ensures that only the intended recipient can retrieve and decrypt the file. On the recipient's end, they input their unique user ID, select the encrypted file, and provide the corresponding decryption key—either shared securely or re-generated using the same deep learning model instance—to retrieve the original file.

The system architecture follows a modular design:
Frontend: Developed using Bootstrap, provides a clean UI for registration, encryption, file upload, and decryption workflows.

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 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404150|

Backend: Powered by Flask, handles API endpoints, file handling, encryption/decryption logic, and deep learning key generation.

Database: MongoDB stores user information, file metadata, and encrypted files indexed by User IDs. To enhance security and usability, the system employs checks for file integrity, unique ID validation, and key matching before decryption is allowed. Real-time feedback mechanisms notify users of successful encryption, transmission, and decryption events.

The workflow ensures a seamless and secure data exchange environment, combining the strengths of AES cryptography and intelligent, AI-driven key management. This design guarantees confidentiality, non-repudiation, and controlled access in real-time, making the system suitable for secure communications across a wide range of use cases.

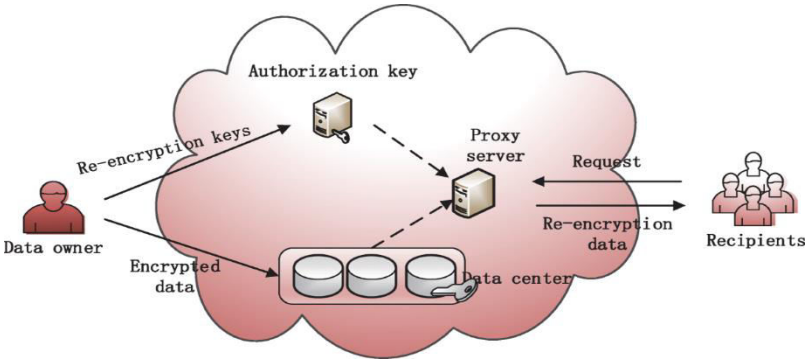


Fig 1: System Architecture

IV. IMPLEMENTATION

1. User Registration and Key Generation
   - Users provide a username and email to generate a unique User ID.
   - A deep learning model creates a strong AES encryption key for the user.
2. File Encryption Workflow Users upload a file, which is encrypted using the DL-generated AES key.

- Encrypted file is stored in MongoDB under the receiver's User ID.
- File Decryption Workflow
- Receiver enters their User ID to access encrypted files.
- File is decrypted using the correct AES key and made available for download.
- System Architecture
- Frontend built with Bootstrap; backend powered by Flask and MongoDB.
- Deep learning model integrated for secure, AI-based key generation.
- User Interaction
- Interface provides clear actions for encryption, decryption, and file tracking.
- Users can reset or switch sessions, enhancing usability and access control.
- This step-by-step implementation ensures an effective, real-time driver drowsiness detection system using eye-tracking and deep learning, offering both accuracy and responsiveness in real-world driving conditions.

V. EXPERIMENTAL RESULTS

The secure file-sharing system was tested in a simulated environment with real-time user interactions. Key findings are as follows:

Encryption Accuracy: The system successfully encrypted and decrypted files using AES with deep learning-generated keys, maintaining data integrity and confidentiality across all tested files.

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 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404150|

Real-Time Performance: File upload, encryption, and download operations were processed smoothly, with minimal latency, ensuring a seamless user experience.

Key Generation: The deep learning model generated unique and strong AES keys for each user, providing enhanced protection against brute-force attacks.

Access Control: Only recipients with the correct User ID and decryption key could access the files, ensuring controlled and secure data sharing

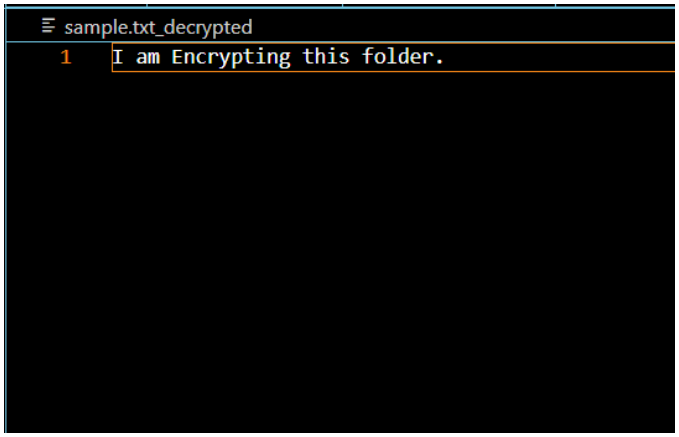


Fig 3: Before Encryption

Fig 4: After Encryption

Uploaded files are first read in binary format and then encrypted using the AES algorithm with a 256-bit key generated by a deep learning model.

The encryption process converts the original file into unreadable ciphertext, which is securely stored in the database under the receiver's User ID.

During decryption, the recipient provides their User ID and the correct decryption key to retrieve and decode the encrypted file. The decrypted file is then restored to its original format and made available for download.

This process ensures that only authorized users can access the file, preserving data confidentiality and integrity.

VI. CONCLUSION AND FUTURE WORK

The Secure File Sharing System successfully demonstrates the integration of AES encryption with deep learning-based key generation to ensure secure and controlled file transfers. By utilizing Flask for backend logic, MongoDB for user data storage, and TensorFlow/Keras for AI-based key generation, the system ensures both functionality and security. Encrypted files are safely stored and can only be decrypted using the correct combination of User ID and the unique key, making it a reliable solution for data protection. The project effectively illustrates the potential of combining cryptography and AI to prevent unauthorized access. However, some limitations remain, such as key management scalability and handling large files efficiently.

Future Work Includes:
Enhanced Key Management: Implement key expiration and rotation policies to improve security over time.
Performance Optimization: Enable faster processing for large file encryption/decryption without compromising security.
User Interface Improvements: Add file status indicators, progress bars, and error handling for better UX.
Cloud Integration: Enable secure cloud storage and retrieval for broader accessibility and data backup.
Multi-Factor Access Control: Combine user ID with biometric or OTP-based verification for advanced security layers.

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 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404150|

REFERENCES

1. Sharma and B. Gupta, "Enhancing Data Security through Machine Learning-Based Key Generation," Proceedings of the International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS), 2024, pp. 45-52. Michael Gomez Selvaraj et al. (2021). Deep learning for medical image diagnosis: An overview of applications and future directions. Journal of AI in Medicine.
2. J. Daemen and V. Rijmen, "The Design of Rijndael: AES — The Advanced Encryption Standard," Springer-Verlag, 2002.Guo, Jing-Ming, and Herleeyandi Markoni. "Driver drowsiness detection using hybrid convolutional neural network and long short-term memory." Multimedia tools and applications 78 (2019): 29059-29087.
3. Q. Huang, Z. Yang, et al., "AI for Cybersecurity: Threat Detection, Attack Attribution and Vulnerability Discovery," IEEE Access, vol. 8, 2020, pp. 181407–181421.Khun Pisuth, Oraan, et al. "Driver drowsiness detection using eye-closeness detection." 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE, 2016.
4. J. Li, Y. Zhang, and X. Wang, "Deep Learning-Based Data Encryption and Decryption System," IEEE Access, vol. 7, 2019, pp. 76145–76152.Liu, Weihuang, et al. "Convolutional two-stream network using multi-facial feature fusion for driver fatigue detection." Future Internet 11.5 (2019): 115.
5. M. Gomez Selvaraj, R. R. Balasubramanian, et al., "Deep learning for medical image diagnosis: An overview of applications and future directions," *Journal of AI in Medicine*, vol. 2, no. 3, 2021, pp. 75–85.Hoang, Thang, et al. "Generic gamma correction for accuracy enhancement in fringe-projection profilometry." Optics letters 35.12 (2010): 1992-1994.
6. W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson Education, 7th ed., 2017.
7. X. Fu, J. Liu, and Y. Chen, "A Secure Data Sharing Protocol for Decentralized Systems," International Journal of Computer Applications, vol. 180, no. 17, 2018, pp. 21–27.
8. N. H. Tran and B. W. Hong, "A Survey of Privacy Attacks and Solutions in Machine Learning," ACM Computing Surveys (CSUR), vol. 55, no. 1, 2022, pp. 1–34.
9. Saxe and K. Berlin, "Deep Neural Networks for Cryptographic Primitive Learning," arXiv preprint arXiv:1503.04870, 2015.
10. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," *MIT Press*, 2016. [Online].

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