International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |

Web based application for secure file storage using hybrid cryptography

1. Dr. V. Subrahmanyam, Associate Professor, CSE Department, Anurag University
2. Juhi Mohta, 20EG105221, Anurag University
3. Pagidoju Shivani, 20EG105237, Anurag University
4. Koganti Hemasri, 20EG105240, Anurag University

ABSTRACT: In today's digital age, the security of sensitive information and data is of paramount importance. As data breaches and cyberattacks continue to escalate, ensuring secure file storage on a local host is a critical concern. This project aims to address this issue through the implementation of hybrid cryptography techniques to protect files stored on a local host. Hybrid cryptography combines the strengths of both symmetric and asymmetric encryption to provide a robust security solution. Symmetric encryption is efficient and fast, while asymmetric encryption offers strong key management and distribution. By combining these two methods, this project provides a secure and efficient approach to safeguarding local file storage. But sometimes a single technique or algorithm alone cannot provide high-level security. So, we have introduced a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric keys. All the algorithms use 128-bit keys
Key information will contain the information regarding the encrypted part of the file, the algorithm, and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithms simultaneously with the help of a multithreading technique.

KEYWORDS: Data security, secure storage, hybrid cryptography, robust, efficient algorithm, key management, multithreading.

I. INTRODUCTION

The protection of sensitive data and information is of utmost importance in the modern digital age. As cyberattacks and data breaches become more frequent, it is essential to provide safe file storage on a local host. By using hybrid cryptography techniques to safeguard files kept on a local host, this project tries to address this problem.

To create a strong security solution, hybrid cryptography combines the benefits of symmetric and asymmetric encryption. Asymmetric encryption enables reliable key management and distribution whereas symmetric encryption is quick and effective. This project offers a reliable and effective solution for securing local file storage by combining these two techniques.

II. RELATED WORK

In modern evolution, individuals and organizations rely on computers and local servers to store a wide range of files, including personal documents, financial records, and confidential business information. Ensuring the confidentiality and integrity of these files is essential to prevent data breaches and privacy violations. Cryptography plays a pivotal role in achieving this goal. Traditional symmetric encryption algorithms, such as AES, are efficient in terms of speed and resource usage but have challenges related to key management. Asymmetric encryption algorithms, like RSA, address these key management issues but tend to be slower and resource-intensive for bulk data encryption. Hybrid cryptography combines the strengths of both symmetric and asymmetric encryption. In this approach, a random symmetric key is generated for each file, and the file is encrypted with this key. The symmetric key is then encrypted using an asymmetric key pair (public-private key) and stored alongside the encrypted file. In an era of increasing digitalization, the need for secure file storage solutions is crucial, particularly when it comes to sensitive or confidential data stored on local machines. Traditional encryption methods have their limitations, often posing challenges in terms of both security and user-friendliness. The existing system for secure file storage on a local host likely relies on conventional encryption methods or simple file access controls. It may involve basic password protection, file permissions, or software that

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |

provides basic encryption. The existing system might use symmetric encryption methods, where a single encryption key is used for both encryption and decryption. This key may be stored locally on the host, posing a risk if the host is compromised. User access is usually controlled by basic username and password authentication, which can be vulnerable to password-guessing attacks or breaches. The existing system may not be resistant to advanced attacks, and the security of stored files might be compromised if the encryption keys or access credentials are stolen.

This project aims to address these issues by developing a system for secure file storage on a local host using hybrid cryptography. In the realm of data security, traditional file storage systems are vulnerable to a multitude of threats, including unauthorized access, data breaches, and malicious attacks. To safeguard the confidentiality and integrity of stored files, an advanced security mechanism becomes imperative. However, it's essential to strike a delicate balance between robust security and user-friendliness, as overly strong encryption can create complications for users, particularly in managing encryption keys, potentially leading to data loss if these keys are forgotten or misplaced. Through the implementation of this secure file storage system, the project endeavors to contribute to enhancing data security practices at the local level.

III. PROPOSED ALGORITHM

The proposed system for secure file storage on a local host will leverage hybrid cryptography, which combines the benefits of both symmetric and asymmetric encryption methods. It will use a more robust and secure approach to protect files on the local host. User access will be controlled with strong multi-factor authentication, such as one-time passwords. The combination of symmetric and asymmetric encryption algorithms in this proposed system provides high-quality security for confidential information such as files and other data.

1. Symmetric Encryption: Using advanced methods of encryption like AES, each file will be securely encrypted with a distinct symmetric key.

2. Asymmetric Encryption: Asymmetric encryption will further protect the symmetric keys that are used for file encryption. The public keys will be applied to cipher the symmetric keys, and each user will receive their own set of private and public keys.

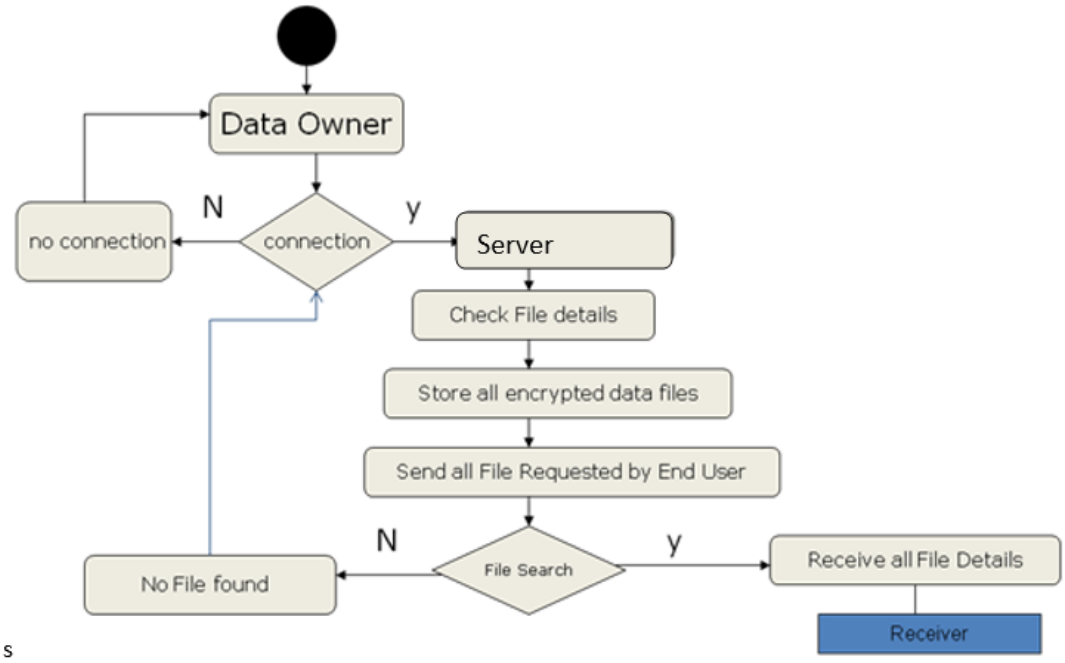
By implementing these features and leveraging hybrid cryptography, the proposed system will provide a much higher level of security for file storage on a local host, making it significantly more resistant to various forms of attacks and data breaches. A secure backup and recovery mechanism will be established to ensure that data can be restored in the event of hardware failures or data corruption.

Block Diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |



s

Activity Diagram

IV. PSEUDO CODE

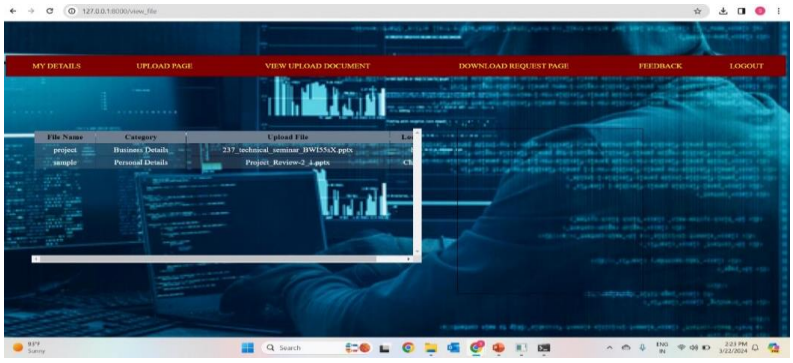
Step 1: Symmetric Key Generation
Step 2: User uploads the desired files.
Step 3: AES Algorithm is employed to encrypt the content of the file.
Step 4: The symmetric key is encrypted using an asymmetric encryption algorithm, such as RSA.
Step 5: The encrypted symmetric key can be securely transmitted or stored.
Step 6: Encrypted files and the encrypted symmetric key are stored on the local host.
Step 7: When a user requests to download an encrypted file, the symmetric key is retrieved from secure storage or decrypted using the recipient's private key (in the case of transmission). The AES algorithm is then employed to decrypt the file's content using the retrieved symmetric key.
Step 8: End.

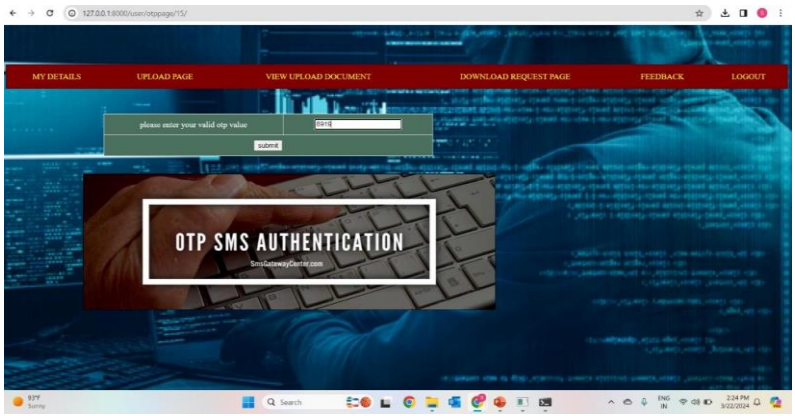
V. RESULTS

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |

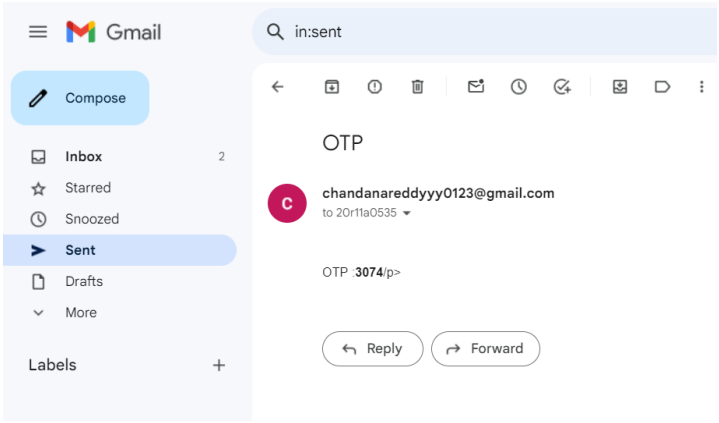


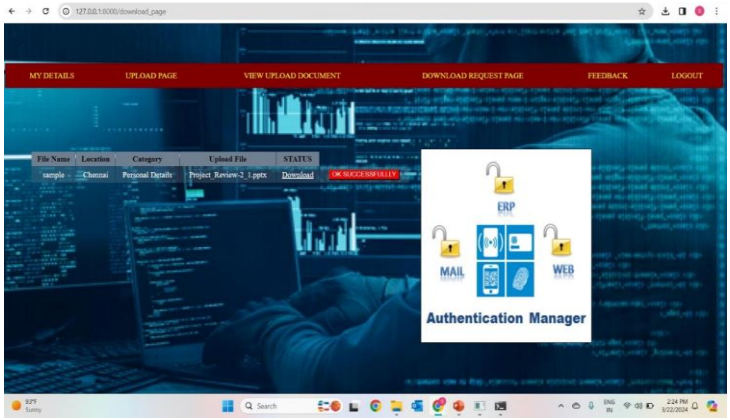


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |





VI. CONCLUSION AND FUTURE WORK

Based on the survey it was identified that secure file storage and sharing would not only require confidentiality but also authentication and integrity. To overcome these drawbacks a architecture is proposed which tries to provide a complete solution for securely storing the files. Our project, "Secure File Storage on Local Host using Hybrid Cryptography" within the Django framework, marks a pivotal achievement in data security. By employing hybrid cryptography, it offers a two-tiered defense, safeguarding data during transmission and at rest. The interface, enriched by Django's features, ensures easy file management, enhancing accessibility. Hosting files locally provides users control and privacy, reducing reliance on third-party cloud services. In conclusion, our project responds to the pressing need for data security, combining advanced encryption with a user-friendly platform. Local hosting and scalability are key strengths. This project serves as a foundation for robust data protection and future developments in secure data management. As technology evolves at a rapid pace, it's essential to consider the potential enhancements for our project, "Secure File Storage on Local Host using Hybrid Cryptography". This project evolves into exciting possibilities for further development, taking data security and user experience to the next level.

1. Multi-Platform Compatibility: To broaden the project's accessibility, extending compatibility to various platforms, including mobile devices and different operating systems, is paramount.

2. Integration with Cloud Services: The project can be further improved by allowing users to back up encrypted files to cloud storage providers while maintaining local hosting. This redundancy not only ensures data availability but also adds an extra layer of protection.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1204001 |

REFERENCES

1. Cryptography and Network Security: Principles and Practice" by William Stallings.
2. Network Security and Cryptography: Bernard Menezes Cengage learning Bernard L. Menezes
3. Cryptography and Network Security: Atul Kahate, McGraw Hill, 3rd Edition 2013
4. Django for Beginners by William S. Vincent
5. S. Hesham and Klaus Hofmann, "High Throughput Architecture for the Advanced Encryption Standard Algorithm", *IEEE International Symposium on Design and Diagnostics of Electronic Circuits & Systems*, pp. 167-170, April 2014.
6. M. Nagle and D. Nilesh, "The New Cryptography Algorithm with High Throughput", *IEEE ICCCI*, pp. 1-5, January 2014. The author has included the *Improved DES algorithm uses a 112-bit key size for data encoding and decoding.*
7. Singh Inder and M. Prateek, "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma A. Hasan "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", *IEEE International Conference on Reliability Optimization and Information Technology*, pp. 310-313, Feb 2014.