File storage system using hybrid cryptography - Advanced Secure Storage

Harshal Chauhan
Apex Institution of Technology *Chandigarh University*
Mohali,Punjab
harshalchauhan291@gmail.com

Saurav
Apex Institution of Technology *Chandigarh University*
Mohali,Punjab
sauravjanartha30@gmail.com

Pardarshee Priya
Apex Institution of Technology *Chandigarh University*
Mohali,Punjab
pardarsheepriyal@gmail.com

Anushka Rai
Apex Institution of Technology *Chandigarh University*
Mohali,Punjab
14anushkar@gmail.com

Abstract— ***In an increasingly digital age, safeguarding data has become a top priority. The Secure File Storage Using Hybrid Cryptography initiative addresses this issue by merging symmetric as well as asymmetric encryption techniques. This method provides a vigorous solution for ensuring the security of data both at rest and during transmission.***

By leveraging the strengths of both encryption approaches, this project enhances data confidentiality, integrity, and authenticity. Its goal is to address vulnerabilities that are present in standalone encryption methods by employing symmetric encryption for efficient data processing and asymmetric encryption for secure key exchange.

This project is adaptable to a wide range of hardware and offers an intuitive user interface for secure file management. Through this innovative approach, Secure File Storage Using Hybrid Cryptography sets new standards for data security and contributes to the field of cybersecurity.

Keywords *— Hybrid Cryptography, Symmetric Cryptography, Asymmetric Cryptography, Key Management, Public Key Cryptography, IOT(Internet of Things), Authentication, Encryption, Decryption.*

I. INTRODUCTION

Sensitive data is more susceptible to breaches and unauthorized access in today's digital environment. Although encryption methods work well, they might not offer complete defense against ever changing cyberthreats. In order to overcome this difficulty, the Secure File Storage Using Hybrid Cryptography project has created a sophisticated encryption technique that combines symmetric and asymmetric cryptography to strengthen data security.

A. PROBLEM DEFINITION

The majority of file storage systems in use today usesingle-layer encryption methods, which are prone to flaws and possible hacks. There are two issues at hand:

• Data Vulnerability: Sensitive information is frequently exposed to unauthorised access, data breaches, and espionage because current systems frequently lack the resilience required to protect data against sophisticated cyber threats.

• Complexity of Key Management: Handling encryption keys, a vital part of safe file storage, is difficult and frequently prone to human error. Implementing efficient key creation, distribution, and storage on a regular basis is difficult.

Therefore, the task at hand is to create a cutting-edge, novel secure storage system that tackles these issues by:

- Boosting data protection against contemporary online threats.
- Streamlining and fortifying essential management procedures.
- facilitating more precise access control.
- Providing the ability to monitor and audit.
- Ensuring redundancy and scalability of data.
- Keeping accessibility and user-friendliness intact.

The proposed approach aims to address the risks linked with data infringementation and unauthorised access by utilizing hybrid cryptography techniques, which combine symmetric and asymmetric encryption, to establish a resilient file storage system that ensures data confidentiality, integrity, and availability.

B. PROBLEM OVERVIEW

The main task of the project is to create a data protection solution that is more advanced than traditional encryption techniques. While the speed and efficiency of traditional symmetric encryption are excellent, key exchange security is still a worry. The key exchange problem is solved via asymmetric encryption, although performance overhead is added. By combining symmetric encryption for quick data processing with asymmetric encryption for safe key exchange, the project aims to use the advantages of both techniques.

The project's goal is to develop a hybrid encryption strategy that improves data confidentiality and integrity and makes effective data management possible by combining different approaches. This novel method redefines current data security paradigms by recognizing the dynamic nature of data breaches and attempting to build a strong defence against unauthorised access.

C. HYBRID CRYPTOGRAPHY

Hybrid cryptography is a cryptographic technique that blends two distinct encryption methods: asymmetric-key encryption and symmetric-key encryption. This approach combines the advantages of both encryption types while mitigating their individual drawbacks. Here's an overview of how it functions:

Symmetric-Key Encryption: In symmetric-key encryption, the identical key is utilized for encrypting and decrypting data. It is efficient and rapid for securing data, but it necessitates a secure means of key exchange between involved parties. If the key is compromised during transmission or storage, it can result in a security burst.

Asymmetric - Key Encryption: Asymmetric-key encryption, or public-key encryption, employs two keys –

one public key for encryption and another private key for decryption. This approach ensures dependable key exchange because the public key can be freely distributed, while the private key remains confidential. However, asymmetric encryption is computationally more intensive and slower compared to symmetric encryption.

In a hybrid cryptography system, data is first encrypted with a symmetric key. Subsequently, this symmetric key is encrypted using the recipient's public key. The recipient can then employ their private key to decrypt the symmetric key and, consequently, use it to decrypt the data. This strategy marries the regulation of symmetric encryption for data protection with the surety of asymmetric encryption for key exchange.

Hybrid cryptography finds extensive application in secure communication systems, including secure email, SSL/TLS for secure web browsing, and numerous other contexts where ensuring secure data transmission and data confidentiality is of paramount importance. It adeptly strikes a balance between security and performance considerations in cryptographic operations

II. LITERATURE SURVEY

A comprehensive collection of studies and articles on cryptography, safe file storage, data protection, and key management should be included in an advanced secure storage system that uses hybrid cryptography. An overview of some important topics and pertinent works in the discipline is given below:

• Hybrid cryptography:

Samia Bouzefrane and Abdelmadjid Bouabdallah's "A Survey on Hybrid Cryptography Algorithms" gives a general review of the different hybrid cryptography algorithms and how they might be used to improve security.

• Safe File Storage Systems:

Cong Wang et al.'s "A Survey of Cloud Storage Services" Insights into different cloud storage services and their security characteristics are provided in this paper; these are pertinent to safe file storage.

The article "A Survey on Secure Data Storage in Cloud Computing" by Prachi Singhal and Priyanka Varshney states: This study addresses potential solutions as well as security issues with cloud-based storage systems.

• Key Management:

"A Survey of Key Management in Cryptographic Systems" released by NIST: This National Institute of Standards and Technology paper offers a thorough examination of important management techniques and difficulties.

I. F. Akyildiz et al.'s "A Survey of Key Management Issues and Solutions in Wireless Sensor Networks": Despite its emphasis on wireless networks, this study covers important management issues and their fixes for secure storage systems.

• Access Control:

The idea of role-based access control (RBAC) and its applications in secure data storage and access control are introduced in the classic work "Role-Based Access Control" by David F. Ferraiolo et al.

Sandhu, Ravi S., et al.'s "Attribute-Based Access Control": The applicability of attribute-based access control (ABAC) in contemporary secure storage systems is examined in this review.

• Auditing and Logging:

Yang Xiao et al.'s "A Survey of Security and Privacy in Cloud Computing Environments": This survey explores privacy and security features in cloud computing

environments that are pertinent to cloud storage security, such as auditing and monitoring.

The article "A Comprehensive Study on Cloud Storage" by Abdelfattah Shalaby and Mohamed Elsafory: Aspects of cloud storage security, such as auditing procedures, are included in this survey.

• Scalability and Redundancy:

Daniel J. Abadi et al.'s study "Scalable Data Storage" addresses the methods and obstacles involved in creating scalable and redundant data storage systems, which are essential components of safe storage solutions.

• User-Friendly Interfaces:

Andrew Patrick and Maritza Johnson's "Usable Security and Privacy: A Case Study of Developing Privacyware": This paper explores the value of usability in security systems and offers suggestions for improving the usability of safe systems.

These sources can be used as a jumping off point for an extensive review of the literature on cutting edge secure storage systems that employ hybrid cryptography. To keep up with the most recent developments and trends in this subject, make sure to check out more recent papers and research articles.

A. HISTORICAL DEVELOPMENTS

File storage systems incorporating cryptography have witnessed significant historical advancements over time. Here are some notable milestones and transformations in this domain:

1. Early Encryption Techniques (Pre-20th Century): Encryption has been employed for centuries to protect written communications and documents. Classical ciphers like the Caesar cipher and Vigenère cipher constituted the initial encryption methods used for safeguarding information. These methods, though, were relatively rudimentary and lacked the sophistication of contemporary cryptographic approaches.

2. The Enigma Machine (20th Century): The Enigma machine, utilized during World War II, marked a revolutionary development in cryptographic technology. It served as a tool for secure communication within the German military and played a pivotal role in the war. The successful decryption of the Enigma code by the Allies significantly advanced the comprehension of cryptography and its limitations.

3. Public Key Cryptography (1970s): In 1976, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography. This innovation laid the groundwork for modern cryptographic systems, enabling secure communication without necessitating pre-shared secret keys. The RSA encryption algorithm, formulated by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977, represented one of the initial practical implementations of public-key cryptography.

4. Secure File Storage and Encryption (Late 20th Century): As personal computers gained prominence, the demand for secure file storage and transmission surged. Software and systems such as Pretty Good Privacy (PGP), introduced by Phil Zimmermann in the early 1990s, permitted individuals to encrypt their files and email communications securely.

5. AES (Advanced Encryption Standard, 2001): In 2001, the U.S. National Institute of Standard and Technology (NIST) designated the Advanced Encryption Standards (AES) as the official encryption standard. AES, a symmetric-key encryption algorithm, has since found widespread use in securing data, including file storage.

6. Hybrid Cryptography for File Storage (Late 20th Century to Present): Hybrid cryptography, which amalgamates symmetric and asymmetric encryption, has

become a favored choice for securing file storage and transmission. This approach provides a balance between efficiency and security, rendering it fit for various applications, such as cloud storage services and secure backups.

7. Cloud Storage and Data Encryption (21st Century): With the ascent of cloud storage services, the imperative to encrypt data in the cloud has become paramount. Numerous cloud providers now offer encryption features, and users can also employ client-side encryption to assure the security of their files, even when stored remotely.

8. Quantum-Safe Encryption (Ongoing): In response to the progress of quantum computing, the field of cryptography is evolving to address the potential threat it poses to existing encryption methods. Quantum-safe or post-quantum encryption algorithms are under development and exploration to ensure data security in an era of post-quantum computing.

These historical developments represent only a segment of the progress in file storage systems employing cryptography. The domain continues to evolve in response to technological shifts and the growing significance of data security in our digital landscape.

B. EXISTING SYSTEMS

Conventional encryption techniques have been widely used in the field of secure file storage to safeguard confidential information both during transmission and storage. Both asymmetric and symmetric encryption methods have certain benefits and drawbacks. Symmetric encryption guarantees quick data processing in the current environment, however handling the safe exchange of encryption keys presents difficulties. Asymmetric encryption solves issues with key exchange, however because of its complexity, it may result in processing cost. Nonetheless, conventional approaches might not be completely impervious to advanced cyberattacks. Data integrity and confidentiality can be jeopardised by attack vectors such cryptographic weaknesses, key leaks, and brute-force assaults. As a result, even if the current system is somewhat functional, it needs creative ways to keep up with the constantly changing danger environment of digital technologies.

III. PROPOSED SYSTEM

By utilising a hybrid cryptography technique, the safe File Storage Using Hybrid Cryptography project presents a paradigm change in safe file storage. The symmetric and asymmetric encryption techniques are used in this suggested system to create a strong defence against contemporary cyberthreats.

The fundamental innovation is the smooth combination of asymmetric encryption for safe key exchange with symmetric encryption for effective data processing. A round-robin encryption process utilising distinct algorithms is applied to every segment of an uploaded file, strengthening the system's defence against cryptographic assaults.

Additionally, the project guarantees the security of the key exchange process by safeguarding the cryptographic keys using a unique technique and making the key available to users as a public key.

The suggested approach overcomes the drawbacks of conventional techniques by establishing a multi-layered security measure that improves data

confidentiality, integrity, and authenticity while also streamlining the safe file storage and retrieval procedure. By using this cutting-edge strategy, the project hopes to completely transform the safe data management market by providing a complete answer that can change with the times to meet the ever-changing risks posed by cyberattacks.

IV. APPLICATIONS

File storage systems incorporating cryptography, including hybrid cryptography, are utilized in various domains to ensure data security and confidentiality. Here are some typical applications:

1. Secured File Sharing and Collaboration: Hybrid cryptography is applied to safeguard files and documents shared among individuals or teams, whether through cloud-based collaborative tools, email attachments, or file-sharing platforms. This guarantees the privacy of sensitive information during both transmission and storage.

2. Cloud Storage Security**:** Numerous cloud storage services employ encryption to protect files stored on their servers. Hybrid cryptography plays an essential role in securing data in the cloud, allowing users to securely store their files and manage access control.

3. Backup and Disaster Recovery: Data backup systems often incorporate encryption to safeguard backup files. Hybrid cryptography can be employed to ensure the secure storage of backup files, preventing unauthorized access to critical data in the event of data loss or disasters.

4. Financial Services: In the financial sector, hybrid cryptography is employed to secure sensitive financial data, transactions, and communication. It ensures the protection of online banking, digital payment systems, and confidential financial records, guarding against unauthorized access and fraud.

5. Healthcare: Hybrid cryptography is indispensable for securing electronic health records (EHRs) and patient information in the healthcare industry. It assures patient confidentiality and ensures compliance with regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

6. Government and Defence: Government agencies and defence organizations rely on hybrid cryptography to protect classified information and national security data. It is vital for secure communication, data storage, and intelligence sharing.

7. Secure Messaging Apps: Many secure messaging applications utilize hybrid cryptography to encrypt messages and files exchanged between users. This ensures end-to-end encryption and upholds privacy in communication.

8. E-commerce: Online shopping platforms employ encryption to secure customer data, encompassing payment information and personal details. Hybrid cryptography ensures the security of sensitive data during online transactions and while it is stored in databases.

9. Legal Services: Legal firms use encryption to safeguard client confidentiality and sensitive legal documents. Hybrid cryptography ensures that legal files remain secure both during transmission and while at rest.

10. Academic Institutions and Research: Educational and research institution use hybrid cryptography to protect research data, student records, and sensitive academic information. This maintains data integrity and confidentiality.

11. IoT (Internet-of-Things): In the realm of Internet of things(IoT), hybrid cryptography can secure communication between IoT devices and cloud servers, ensuring that data transmitted by sensors and devices remains confidential and unaltered.

12. Compliance and Regulatory Requirements: Various industries must adhere to specific data security and privacy regulations. Hybrid cryptography aids organizations in meeting these compliance requirements by ensuring the confidentiality and integrity of data.

13. Personal Data Security: Individuals can utilize hybrid cryptography to secure their personal files, including financial documents, photographs, and private messages. This is particularly relevant when employing encryption software or secure storage solutions.

Hybrid cryptography is a versatile approach that strikes a balance between security and efficiency, making it fit for a wide array of applications where data confidentiality, authenticity and integrity are of utmost importance.

V. APPROACHES

Designing a file storage system using cryptography, particularly hybrid cryptography, involves several fundamental approaches and techniques to ensure data security. Here are some of the key strategies:

1. Data Encryption:

- Symmetric Encryption: This method employs a sole classified key for both data decryption and encryption. It offers speed and erderliness in data encryption but necessitates secure key management and sharing among authorized users.

- Asymmetric Encryption: Asymmetric encryption uses a set of two keys: a private key for decryption and a public key for encryption. Although it is slower compared to symmetric encryption, it provides a secure mechanism for key exchange. As such, it is often employed in conjunction with symmetric encryption for hybrid cryptography.

2. Key Management:

- Key Generation and Storage: Securely generating and storing cryptographic keys is of paramount importance. Key management systems are used to create, protect, and manage keys. In the context of hybrid cryptography, a secure key exchange mechanism is crucial for sharing symmetric keys securely.

3. Secure Communication Protocols:

- TLS/SSL (Transport Layered Security/ Secure Socket Layer): These protocols guarantee firm communication over networks, including the internet. They employ hybrid cryptography to encrypt data during transmission, such as when accessing a website via HTTPS.

4. Authentication and Authorization:

- Access Control: Implementing access control mechanisms certifies that only the authorized individuals can access and modify stored files. This encompasses user authentiction and role-based access control (RBAC) systems.

5. Integrity affirmation:

- Hash Functions: Hash functions are used to prove the probity of files. By comparing hash values before and after storage, it is possible to detect any tampering with files.

6. Data Compression and Deduplication:- Data compression and deduplication techniques can be applied before encryption to reduce file sizes and optimize storage efficiency. Care must be taken to ensure effective data encryption post-compression.

7. Secure Storage Protocols:- Various storage protocols and file systems are designed with security in mind. Examples include Network Attached Storagess (NAS) systems, Distributed File Systems (DFS), and cloud storage services that offer encryption at rest.

8. End-to-End Cipher:- Implementing end-to-end cipher/encryption sees that data is encrypted on the client side and remains encrypted until it reaches the intended recipient, providing the highest level of security and privacy. Many secure messaging and email services employ this approach.

9. Data Backups and Redundancy:- Creating backups of encrypted data and ensuring redundancy is crucial for data recovery in the event of system failures or data loss. Secure backup solutions can replicate encrypted data to prevent data loss.

10. Secure Authentication and User Management:

- Well built user authentication methods, like multi-factors authentication (MFA), enhance the security of file storage systems. User management systems make sure that only authorized users gain access.

11. Auditing and Logging:- The implementation of auditing and lodging mechanisms helps monitor and track access and changes to files, providing transparency and facilitating security monitoring.

12. Security Updates and Patch Management:- Regularly updating and fixing software and systems is imp. to address security vulnerabilities and maintain the ongoing security of the file storage system.

13. Compliance and Regulation:- Depending on the industry and the nature of data being stored, compliance with specific standards and regulations is necessary to ensure data security and privacy.

By incorporating these strategies and techniques, a robust and secure file storage system can be developed using cryptography, whether through symmetric or hybrid encryption. This approach safeguards sensitive data from unauthorized access and upholds data integrity.

VI. METHODOLOGY

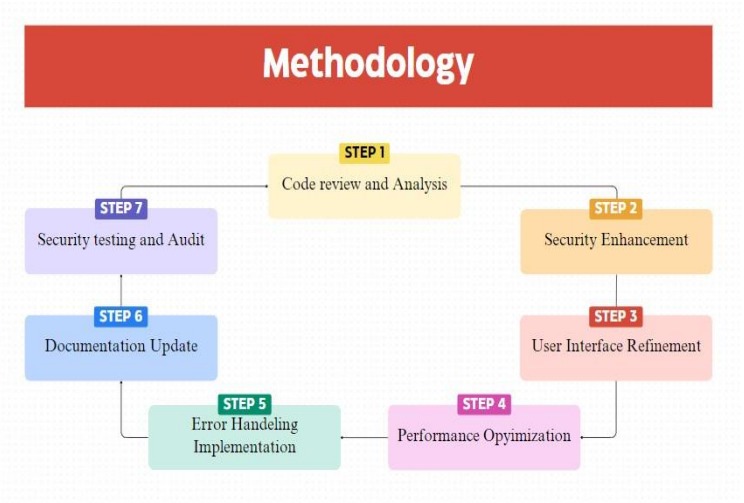

Figure 1: Methodology Steps

The methodology as described in figure 1 involves the following steps:

Code review and analysis: Thoroughly review the existing project codebase and understand its architecture, encryption methods, and user interface components

Security Enhancement: Integrate stronger encryption algorithms, update cryptographic libraries, and implement best practices for secure key management.

User Interface Refinement: Enhance the user interface design and navigation, ensuring a smoother and more intuitive user experience.

Performance Optimization: Analyze encryption and decryption processes, identifying bottlenecks and areas for optimization, and implement improvements.

Error Handling Implementation: Develop mechanisms to handle various error scenarios, providing users with informative and user-friendly error messages.

Documentation update: Update the project's README file and other documentation to provide clear instructions for installation, configuration, usage, and troubleshooting.

Security testing and Audit: Conduct thorough security testing, employing penetration tools and techniques to identify and rectify vulnerabilities.

A. ALGORITHM / FLOW CHART

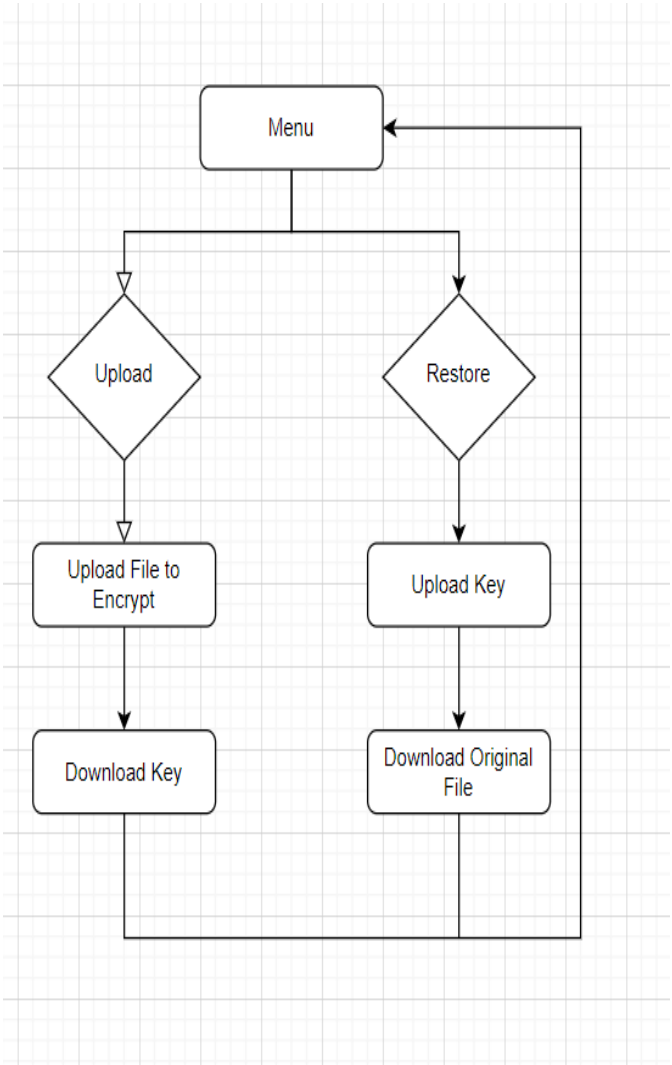

Figure 2: Working Flow Chart

The above presented flowchart represented in figure 2 gives us an accurate description of the working flow of the entire system. A user can either upload or restore the file according to its need. The program will then generate an encryption key for every upload and would allow the user to download the key which could be later used as an upload key to download the original file. In this way the entire flow of the system would work without any complications.

VII.RESULT

Figure 3: Home Page

Figure 4: Upload page

Figure 5: Uploading a File

Figure 6: Submitting the file

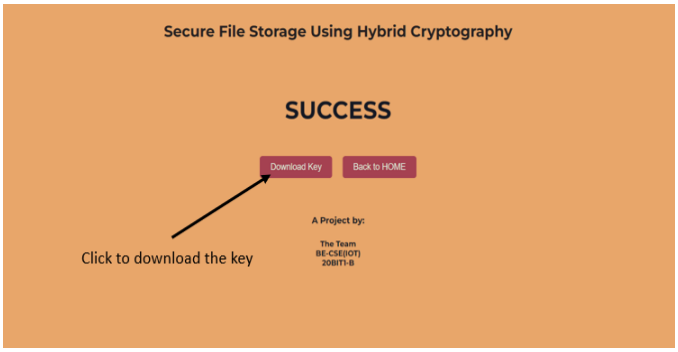

Figure 7: Downloading the cryptographic key

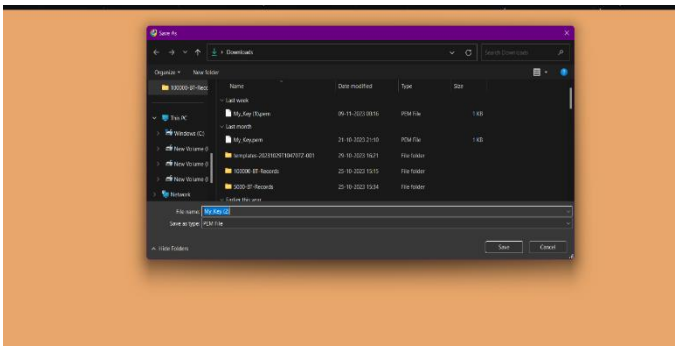

Figure 8: Selecting the download location

Figure 9: Restoring/decrypting the file

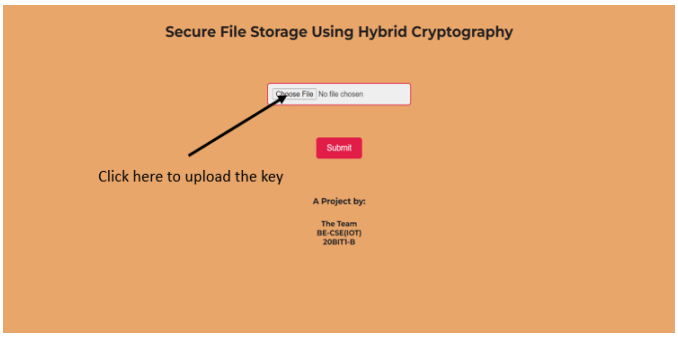

Figure 10: Uploading the downloaded key

Figure 11: Selecting the key

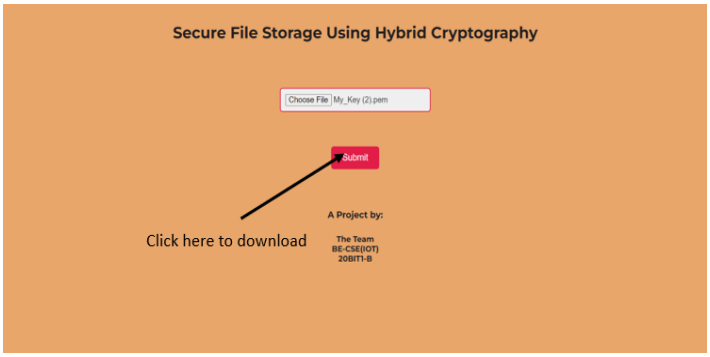

Figure 12: Submitting the key

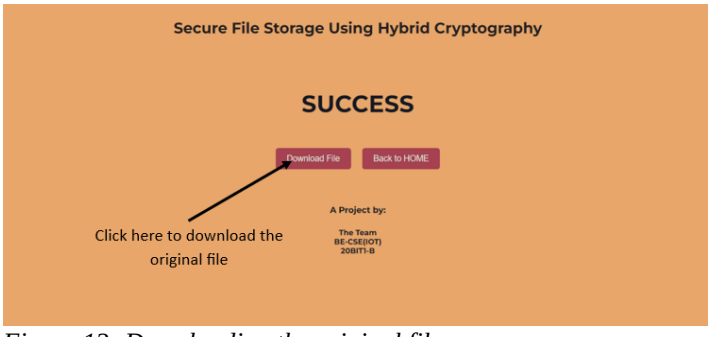

Figure 13: Downloading the original file

Figure 3 to *figure 13* demonstrates the working of the presented model. For instance *figure 3* gives the layout of

the home page where the user can select one of the to options (i.e either to upload the files or to restore the file). *Figure 4 to 8* shows how a file can be uploaded into the system and how a cryptographic key can be generated for the same.

Figure 9 to 13 shows the other half of the system where the original file could be obtained with the help of previously generated encryption key.

For reference, the initial uploaded file was the one that can be seen in the image below(*figure 14).*

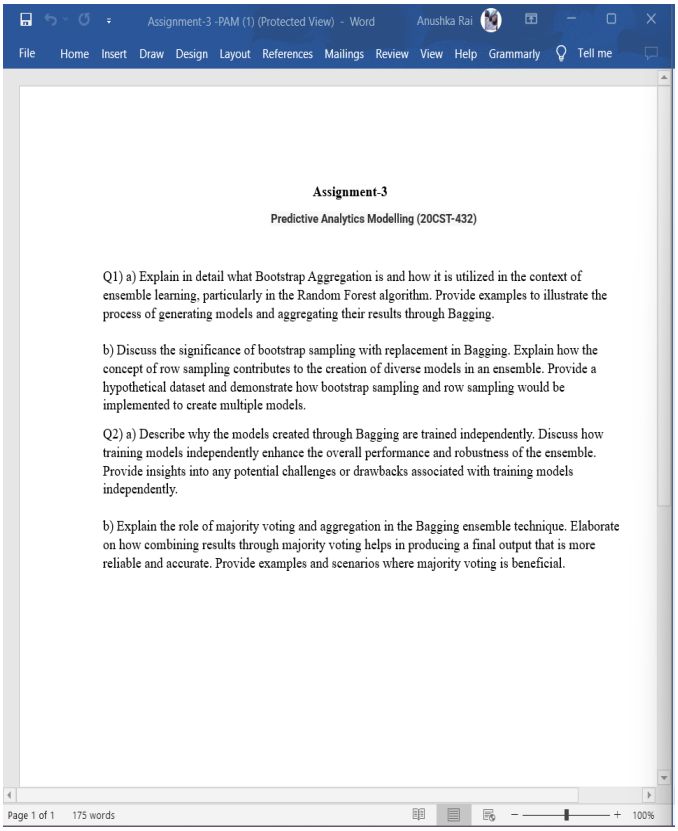

Figure 14: Initially uploaded file

After the decryption, the downloaded file is the one given below in *figure 15.*

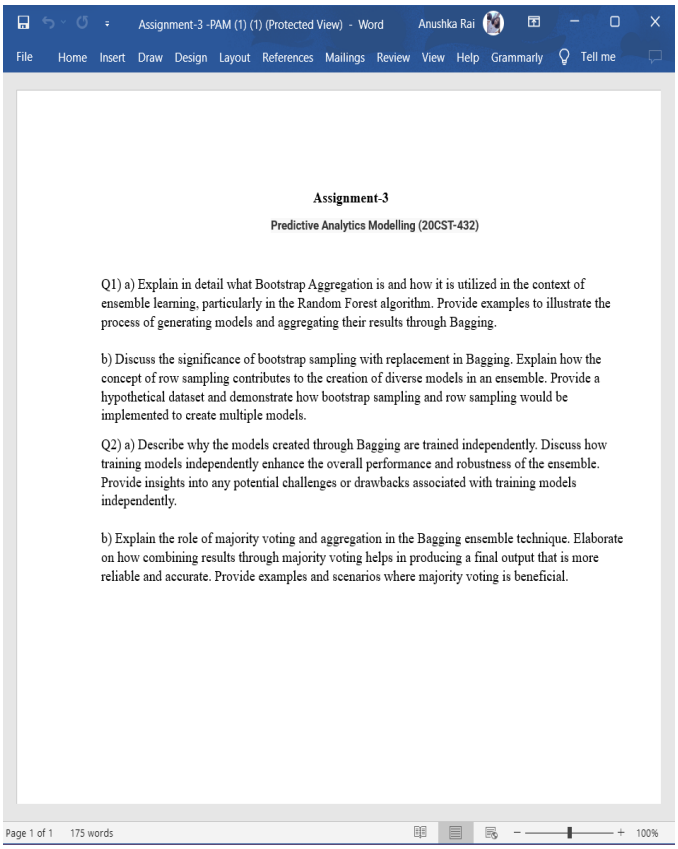

Figure 15: Downloading the decrypted file

In a real-world while using this encryption tool, the steps give in *figure 3 to 9* will be done by the sender and then the key will be shared by the sender to the receiver and then, upon receiving the key, the receiver will upload the key on the web page and decrypt it to download the original file, i.e. shown in *figure 10 to 13*.

VIII. CONCLUSION

The "File storage system using hybrid cryptography" project is a major advancement in the ongoing attempts to strengthen data safety in a society that is becoming more digitally linked and networked. It is clear from a thorough review of the literature and an investigation of important topics related to safe data storage that the use of hybrid cryptography in file storage systems presents a viable way to deal with urgent security issues.

By combining the benefits of symmetric and asymmetric encryption, this cutting-edge file storage solution offers a strong defence against contemporary online dangers. The system protects sensitive data from unauthorised access by using sophisticated key management techniques and intelligent data segmentation. Sophisticated auditing tools and access control systems improve security even further and make it easier to comply with legal obligations.

Furthermore, the focus on redundancy and scalability guarantees data availability and integrity even in the event of unplanned disruptions or hardware breakdowns. Not less crucially, the system keeps its interface easy to use, allowing a wide spectrum of people to use it without sacrificing security.

"Advanced Secure Storage" is a ray of hope as businesses and people struggle with the ever-increasing significance of data security and confidentiality. This solution not only tackles present weaknesses but also foresees potential future threats, providing consumers with piece of mind when it comes to protecting their most important digital assets.

To sum up, the creation and use of "Advanced Secure Storage" will represent a critical turning point in the continuous struggle to safeguard sensitive information, guaranteeing its privacy, integrity, and accessibility when required. With the help of this initiative, we may look forward to a more secure digital age where unauthorised access and data breaches are things of the past and data security is the new standard.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our supervisor Mrs. Bhavna Nayyer, for her critical guidance, insightful feedback, and unwavering support throughout the course of our research project. Her expertise and enthusiasm have been influential in casting this paper.

We would also like to thank our fellow colleagues for their contributions to this research, whether it be through providing resources, sharing their expertise, or offering encouragement. Their assistance has been invaluable.

Finally, I would like to acknowledge the support of my family and friends, who have provided me with unwavering love and encouragement throughout this journey.

REFERENCES

[1] Abadi, Daniel J., et al. "Scalable semantic web data management using vertical partitioning." Proceedings of the 33rd international conference on Very large data bases. 2007.

[2] Nandgaonkar, Suruchee V., and A. B. Raut. "A comprehensive study on cloud computing." International Journal of Computer Science and Mobile Computing, a Monthly Journal of Computer Science and Information Technology 3 (2014): 733-738.

[3] Ferraiolo, David F., and D. R. Kuhn. "Role-Based Access Controls." ArXiv, 2009, /abs/0903.2171.

[4] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843-859, Second Quarter 2013, doi: 10.1109/SURV.2012.060912.00182.

[5] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," in IEEE Access, vol. 9, pp. 107200-107223, 2021, doi: 10.1109/ACCESS.2021.3101218.

[6] Akyildiz, Ian & WY, Su & Sankarasubramaniam, Y. & Cayirci, E.. (2002). Wireless Sensor Networks: A Survey. Computer Networks. 38. 393-422. 10.1016/S1389-1286(01)00302-4.

[7] Barker, Elaine, et al. "NIST special publication 800-57." NIST Special publication 800.57 (2007): 1-142.

[8] Wang, Cong, et al. "Ensuring data storage security in Cloud Computing, Quality of Service, 2009. IWQoS." 17th International Workshop on, vol., no.

[9] Kanatt, Shruti, Amey Jadhav, and Prachi Talwar. "Review of secure file storage on cloud using hybrid cryptography." *International Journal of Engineering Research & Technology (IJERT)* 9.2 (2020): 16-20.

[10] Mahadevan, V., & Kumar, R. (2018). A Hybrid Cryptographic Approach for Secure File Transfer in Cloud Environment. In 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).

[11] Rajasekar, S., Priya, K., & Arun, S. (2018). Secure File Transfer Protocol Using Hybrid Cryptography Technique. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES).

[12] Mishra, A., Singh, S., & Shrivastava, R. (2018). A Secure File Transfer System Using Hybrid Cryptography and Steganography. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA).

[13] Shyamasundar, R. K., & Guruprasad, N. M. (2019). Hybrid Cryptography in File Transfer Protocols. Procedia Computer Science.

[14] Singh, S. K., & Kumar, S. (2016). Enhanced Security in File Transfer Using Hybrid Cryptography. In 2016 10th International Conference on Intelligent Systems and Control (ISCO).

[15] Gopikrishnan, R., & Babu, G. (2017). Secure File Transfer using Hybrid Cryptography Technique in Cloud Environment. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[16] Saranya, S., & Sundari, M. S. (2018). Hybrid Cryptography for Secure File Transfer in Cloud Computing. In 2018 International Conference on Communication and Signal Processing (ICCSP).

[17] Choudhary, A., Verma, P., & Varma, S. (2018). Secure File Transfer Protocol with Hybrid Cryptography. In 2018 4th International Conference on Recent Advances in Information Technology (RAIT).

[18] Kumar, S., & Goyal, P. (2017). Design and Implementation of Secure File Transfer Protocol using Hybrid Cryptography. In 2017 International Conference on Computing, Communication and Automation (ICCCA).

[19] Jain, S., & Mittal, P. (2018). Enhancing File Transfer Security Using Hybrid Cryptography in Cloud Environment. In 2018 International Conference on

Advances in Computing and Communication Engineering (ICACCE).

[20] Wang, H., & Zhang, X. (2019). Secure File Transfer Protocol Based on Hybrid Cryptography in Cloud Computing. In 2019 IEEE 5th International Conference on Computer and Communications (ICCC).

[21] Singh, R., & Sharma, A. (2018). Secure File Transfer Using Hybrid Cryptography in IoT Environment. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA).

[22] Patel, N., & Desai, K. (2019). Hybrid Cryptography-Based Secure File Transfer System for Healthcare Applications. In 2019 2nd International Conference on Communication, Computing and Digital Systems (CCODE).

[23] Li, L., & Zhang, Y. (2017). Enhanced Secure File Transfer Protocol Using Hybrid Cryptography in Mobile Networks. In 2017 IEEE International Conference on Computational Science and Engineering (CSE).

[24] Gupta, S., & Verma, P. (2018). Secure File Transfer Using Hybrid Cryptography in Wireless Sensor Networks. In 2018 3rd International Conference on Inventive Communication and Computational Technologies (ICICCT).