File storage system using hybrid cryptography - Advanced Secure Storage

A PROJECT REPORT

Submitted by

20BCS4614 Pardarshee Priya

20BCS6098 Harshal Chauhan

20BCS4622 Anushka Rai

20BCS6096 Saurav

in partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUER SCIENCE WITH SPECIALISATION

IN

INTERNET OF THINGS

Chandigarh University

November 2023

BONAFIDE CERTIFICATE

Certified that this project report **"File storage system using hybrid cryptography - Advanced Secure Storage"** is the bonafide work of "**Harshal Chauhan, Saurav, Pardarshee Priya and Anushka Rai"** who carried out the project work under my/our supervision.

SIGNATURE

Bhavna Nayyer (E15505)

SUPERVISOR

Professor

AIT-CSE

Submitted for the project viva-voce examination held on

INTERNAL EXAMINER **EXTERNAL EXAMINER**

TABLE OF CONTENT

i. List of Tables/Figures

ii. 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 and asymmetric encryption techniques. This method provides a robust 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.

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

1. INTRODUCTION

Sensitive data is more susceptible to breaches and unauthorised access in today's digital environment. Although encryption methods work well, they might not offer complete defence 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.

1.1 PROBLEM DEFINITION

The majority of file storage systems in use today use single-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 associated with data breaches and unauthorised access by utilising hybrid cryptography techniques, which combine symmetric and asymmetric encryption, to establish a resilient file storage system that ensures data confidentiality, integrity, and availability.

1.2 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 recognising the dynamic nature of data breaches and attempting to build a strong defence against unauthorised access.

1.3 Hybrid Cryptography

Hybrid cryptography is a cryptographic technique that blends two distinct encryption methods: symmetric-key encryption and asymmetric-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 same key is utilized for both 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 breach.

Asymmetric-Key Encryption: Asymmetric-key encryption, also known as public-key encryption, employs a pair of keys – a public key for encryption and a private key for decryption. This approach ensures secure 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 efficiency of symmetric encryption for data protection with the security 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

1.4 HARDWARE SPECIFICATION

Server Infrastructure:

A capable server with sufficient storage space to handle the uploaded and encrypted files.

1.4 SOFTWARE SPECIFICATION

Server-side Software:

Operating System: Linux (preferred for hosting applications)

Python: Version 3.11

Web Framework: Flask

Required Python Libraries:

Flask==1.1.1

werkzeug

cryptography==2.9.2

2. 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:

Hybrid cryptography is a technique that combines the benefits of both symmetric and asymmetric encryption schemes to enhance security and efficiency in data protection.

Symmetric encryption involves using a single secret key to both encrypt and decrypt data. It's fast and efficient but poses a challenge in securely sharing the key between communicating parties.

Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. This approach resolves the key-sharing issue but is computationally more intensive, especially for large volumes of data.

Hybrid cryptography leverages the strengths of both methods. It typically involves using asymmetric encryption to securely exchange a symmetric key, and then using that symmetric key for the encryption and decryption of the actual data. This approach maintains the security advantage of asymmetric encryption for key exchange while benefiting from the speed and efficiency of symmetric encryption for the bulk data.

Hybrid cryptography is widely used in various secure communication protocols, such as HTTPS, SSL/TLS, and PGP, as it provides a balance between security and performance, essential in protecting sensitive information in today's digital world.

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:

A safe file storage system refers to a platform, service, or methodology designed to securely store digital files, ensuring the protection, integrity, and confidentiality of the stored data. This type of system employs various security measures and protocols to safeguard files from unauthorized access, corruption, loss, or theft. Its key components include Encryption, access control, redundancy and backups, integrity verification, physical security, monitoring and auditing etc.

Creating a safe file storage system involves considering factors such as the sensitivity of the data, compliance requirements, accessibility needs, and scalability. Implementing a combination of encryption, access controls, redundancy, and monitoring helps create a robust and secure file storage environment.

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:

Key management involves the administration, control, and handling of cryptographic keys used in various security systems, particularly in encryption, authentication, and access control mechanisms. It encompasses the generation, storage, distribution, and destruction of cryptographic keys throughout their lifecycle to ensure the security of

sensitive data and systems. Its components include key generation, key storage, key distribution, key usage, key rotation, key revocation and deletion, key recovery.

Effective key management is crucial for maintaining the confidentiality, integrity, and availability of data. It's a fundamental aspect of secure communication, encryption, digital signatures, and access control systems. Poor key management can lead to security vulnerabilities, unauthorized access, and potential data breaches.

Various standards and best practices, such as the Key Management Interoperability Protocol (KMIP), exist to guide organizations in implementing robust key management strategies tailored to their specific security requirements.

"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.

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:

Access control refers to the security measures and policies implemented to regulate and manage who can access, view, modify, or use resources, systems, or physical areas within an organization or a digital environment. Its primary goal is to protect sensitive information, systems, and physical spaces from unauthorized access while ensuring that authorized users have appropriate access rights.

There are several types of access control:

- Physical Access Control: Governing entry to physical spaces like buildings, rooms, or data centers. This can involve locks, biometric scanners, key cards, or security personnel.
- Logical Access Control: Regulating access to digital systems, networks, and data. This includes user authentication, authorization, and various software-based controls.

1. Authentication: Verifying the identity of users through credentials such as passwords, biometrics, smart cards, or two-factor authentication.
2. Authorization: Granting specific permissions or rights to authenticated users based on their roles, responsibilities, or job functions. This includes determining what data or systems an individual or group can access and what actions they can perform.
3. Access Control Lists (ACLs): Lists associated with resources specifying who can access them and what operations they can perform.
4. Role-Based Access Control (RBAC): Assigning permissions based on predefined roles, simplifying management and ensuring that users have appropriate access based on their job roles.

- Mandatory Access Control (MAC): A strict, centrally controlled access model commonly used in highly secure environments where access rights are defined by a system administrator or security policy.
- Discretionary Access Control (DAC): A less restrictive access control model where users have more control over resources they own, allowing them to grant or revoke access to their resources.

Access control is a crucial component of information security, ensuring confidentiality, integrity, and availability of data and resources. It's implemented through a combination

of technological solutions, administrative policies, and user education to create a layered defense against unauthorized access and potential security breaches.

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:

Auditing and logging are essential components of cybersecurity and information systems management. They involve the systematic recording, monitoring, and analysis of events, activities, or changes within an IT environment or a system.

Logging: Logging refers to the process of capturing and recording events or activities that occur within a system or application. These events could include user logins, file accesses, system errors, configuration changes, or any other noteworthy occurrences. Logs are typically stored in files or databases and serve as a chronological record of system activities.

Auditing: Auditing involves the systematic review, analysis, and interpretation of logged data to assess the security, compliance, and operational efficiency of an organization's IT infrastructure. It includes examining logs and generating reports to identify patterns, anomalies, or potential security incidents. Auditing often involves comparing logged activities against predefined policies, security standards, or compliance requirements.

The purposes of auditing and logging include:

- Security Monitoring: Identifying and investigating security incidents or unauthorized access attempts by analyzing logs for suspicious activities or patterns.
- Compliance and Regulation: Ensuring adherence to industry standards, legal requirements, and internal policies by auditing system activities against established benchmarks.
- Troubleshooting and Diagnostics: Using logs to diagnose system errors, performance issues, or operational problems by analyzing the sequence of events leading to a particular issue.
- Forensic Investigations: During security incidents, logs serve as valuable sources of information for forensic analysis to understand the nature of the incident, its impact, and the actions taken by malicious actors.

To effectively use auditing and logging for security and management purposes, organizations often employ specialized tools and systems that automate log collection, storage, and analysis. Security Information and Event Management (SIEM) solutions, log management systems, and centralized logging platforms are examples of such tools that help organizations streamline the auditing and logging process.

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:

Scalability and redundancy are critical concepts in the design and management of systems, particularly in technology and infrastructure. They both play key roles in ensuring the reliability, performance, and availability of systems and services.

- Scalability: Scalability refers to a system's ability to handle an increasing amount of work or a growing number of users, transactions, or data without compromising performance or requiring a complete redesign. There are two primary types of scalability:

1. Vertical Scalability: Also known as scaling up, it involves increasing the resources (such as CPU, memory, or storage) of a single machine to handle higher workloads. For example, upgrading a server with more powerful hardware to accommodate increased demand.
2. Horizontal Scalability: Also known as scaling out, it involves adding more machines or nodes to distribute the workload across multiple devices. This approach often utilizes load balancing and clustering to ensure efficient distribution of tasks.

Scalability is crucial in modern systems as it allows businesses to accommodate growth, handle sudden spikes in demand, and maintain performance without experiencing bottlenecks or system failures.

- Redundancy: Redundancy is the inclusion of additional components or resources within a system with the goal of ensuring reliability and fault tolerance. Redundancy aims to mitigate the risk of system failure due to component malfunctions or other issues by providing backup mechanisms.

1. Hardware Redundancy: Involves duplicating critical hardware components (such as hard drives, power supplies, or servers) to ensure that if one component fails, another can take over seamlessly, preventing downtime.
2. Data Redundancy: Involves creating copies or backups of data to prevent loss in case of data corruption, accidental deletion, or hardware failure. RAID (Redundant Array of Independent Disks) configurations and backups are examples of data redundancy strategies.

Redundancy is essential for maintaining system availability, minimizing downtime, and ensuring continuous operation, particularly in mission-critical systems or services where any interruption can have significant consequences

Both scalability and redundancy are crucial elements of system design and maintenance, allowing systems to adapt to changing demands, maintain high availability, and enhance overall reliability and performance. Balancing these factors is key to building robust and efficient systems that can meet both current and future needs.

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:

User-friendly interfaces, often referred to as UI (User Interface) or UX (User Experience), are designed to create seamless and intuitive interactions between users and digital systems, software, or devices. A user-friendly interface aims to enhance usability, accessibility, and overall satisfaction for the end user.

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.

2.1 HISTORICAL DEVELOPMENTS

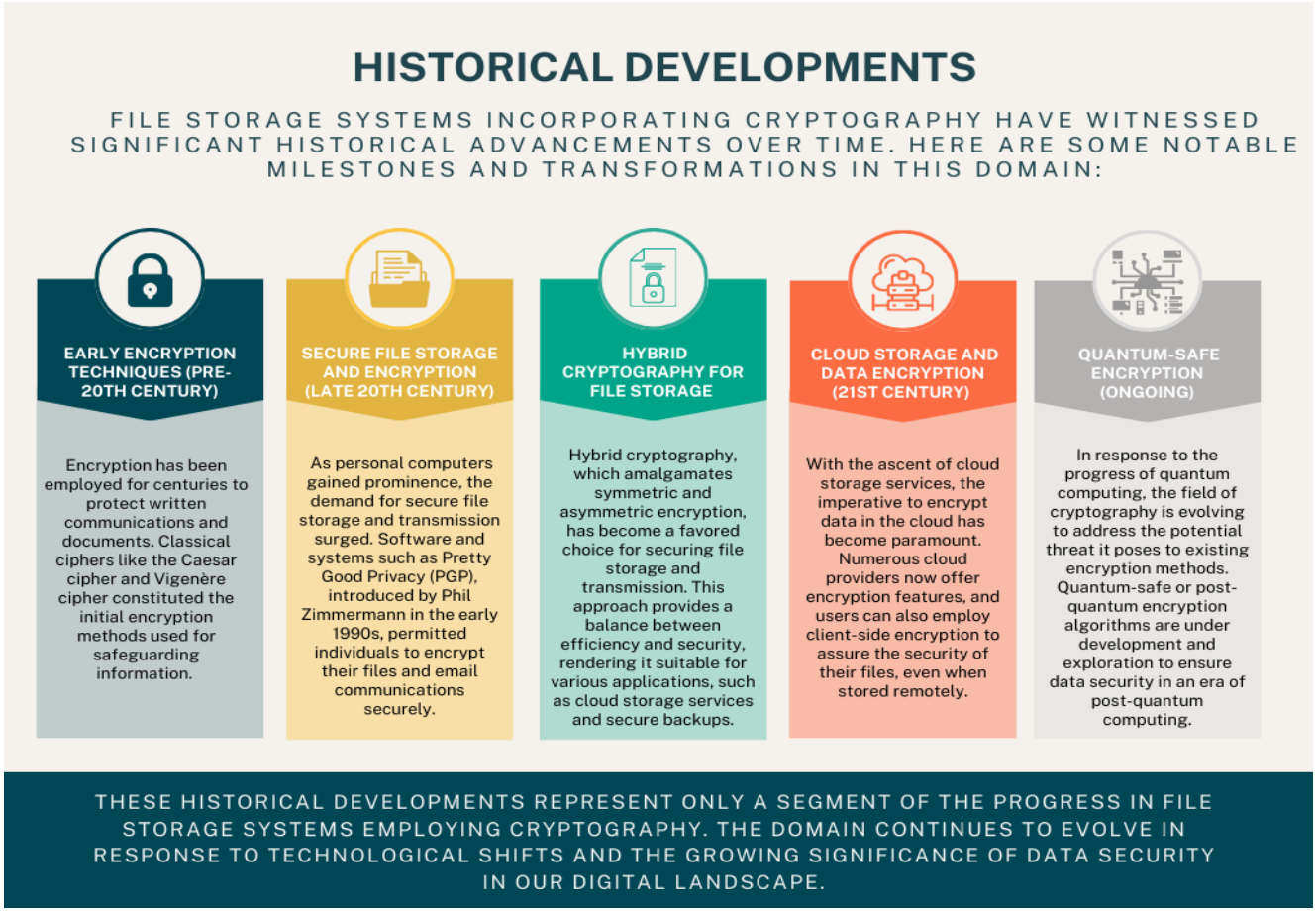

Fig 1: Historical Developments

File storage systems incorporating cryptography have witnessed significant historical advancements over time. Here are some notable milestones and transformations that can be seen in *fig 1* along with some additional information 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 Standards and Technology (NIST) designated the Advanced Encryption Standard (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 favoured choice for securing file storage and transmission. This approach provides a balance between efficiency and security, rendering it suitable 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.

2.2 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 symmetric and asymmetric 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.

3. 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.

4. 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 mentioned in *Fig 3* along with some additional applications:

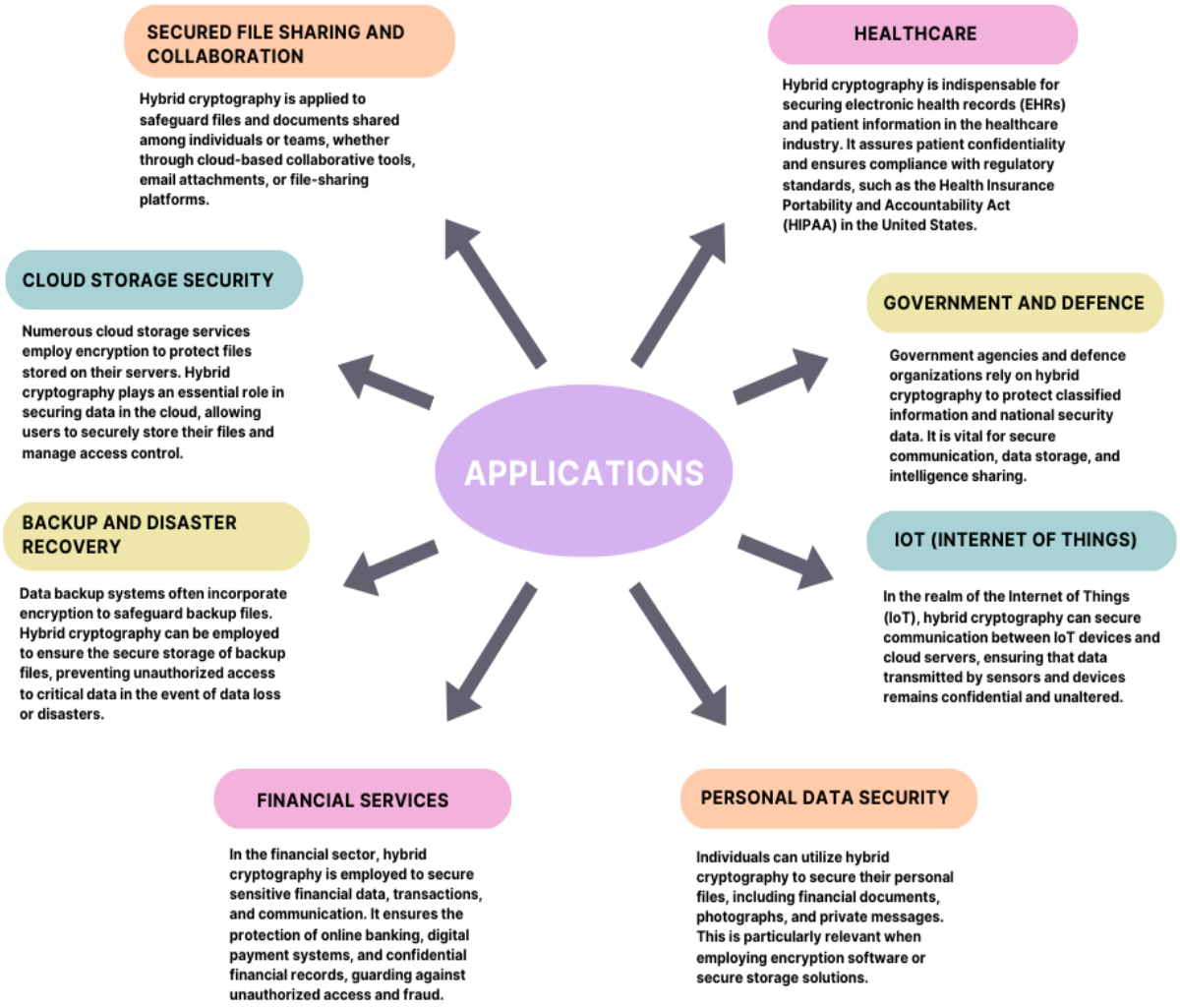

Fig 2: Applications

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 and Research Institutions: Educational and research institutions 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 the 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 suitable for a wide array of applications where data confidentiality, integrity, and authenticity are of utmost importance.

5. 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:

Data encryption is the process of transforming information (plaintext) into an unreadable format (ciphertext) using cryptographic algorithms and keys. This transformation ensures that even if unauthorized individuals access the encrypted data, they cannot understand or interpret it without the corresponding decryption key.

There are two primary types of encryption:

Symmetric Encryption: In symmetric encryption, the same secret key is used for both encryption and decryption of data. It's fast and efficient but requires secure key distribution since both parties need access to the same key. Examples include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

Asymmetric Encryption (Public-Key Encryption): Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. The public key is widely distributed and used to encrypt data, while the private key, kept secret by the recipient, is used for decryption. RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are common asymmetric encryption algorithms.

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:

For a file storage system employing hybrid cryptography, ensuring secure communication protocols is crucial to safeguard data during transmission. Here are some secure communication protocols that can be used in conjunction with hybrid cryptography for file storage:

- HTTPS (Hypertext Transfer Protocol Secure):

i. HTTPS encrypts data transmitted between a user's browser and the server, ensuring secure communication over the internet.

ii. It uses a combination of symmetric encryption (often negotiated via asymmetric key exchange) and digital certificates to establish a secure connection.

- SFTP (Secure File Transfer Protocol):

i. SFTP provides a secure channel for transferring files between systems, using encryption for data transmission.

ii. It's based on SSH (Secure Shell) and employs both symmetric and asymmetric encryption methods to secure file transfers.

- FTPS (File Transfer Protocol Secure):

i. FTPS combines FTP with TLS (Transport Layer Security) or SSL (Secure Sockets Layer) encryption for secure file transfers.

ii. It supports both implicit and explicit modes, providing encryption for data transmission.

- AS2 (Applicability Statement 2):

i. AS2 is a protocol used for secure and reliable data exchange over the internet, particularly in B2B (business-to-business) transactions.

ii. It incorporates digital signatures, encryption, and data compression for secure file transfer.

- IPsec (Internet Protocol Security):

i. IPsec operates at the network layer and provides security for IP communications by encrypting and authenticating each IP packet.

ii. It's commonly used for secure site-to-site VPNs (Virtual Private Networks) to protect data during transmission between networks.

- TLS/SSL (Transport Layer Security/Secure Sockets Layer):

i. TLS and its predecessor SSL are cryptographic protocols used to secure communication over the internet.

ii. They ensure data confidentiality, integrity, and authentication through encryption and digital certificates.

4. Authentication and Authorization:

- Access Control: Implementing access control mechanisms ensures that only authorized individuals can access and modify stored files. This encompasses user authentication and role-based access control (RBAC) systems. By combining strong authentication methods, granular authorization controls, and hybrid cryptography for data security, the file storage system can effectively protect sensitive data and limit access to authorized users or entities. Regular assessments, updates, and adherence to security protocols are essential to maintain the integrity and security of the system.

5. Integrity Verification:

- Hash Functions: Hash functions are employed to verify the integrity of files. By comparing hash values before and after storage, it is possible to detect any tampering with files. By combining integrity verification techniques like hash functions, digital signatures, and timestamping with hybrid cryptography, the file storage system can ensure that data remains unaltered during storage and transmission. Regular integrity checks and secure handling of verification data are essential to maintaining the overall integrity of the stored 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. By integrating data compression, duplication, and hybrid cryptography, the file storage system can effectively optimize storage space, maintain data integrity, and enhance security against unauthorized access. Regular monitoring, assessment, and adaptation of these strategies are essential to ensure an efficient and secure storage environment.

7. Secure Storage Protocols:

- Various storage protocols and file systems are designed with security in mind. Examples include Network Attached Storage (NAS) systems, Distributed File Systems (DFS), and cloud storage services that offer encryption at rest. Integrating hybrid cryptography with secure storage protocols ensures comprehensive protection for stored files, addressing encryption at rest, secure communication during transmission, and the integrity of the stored data. Regular assessments and adherence to best practices are crucial to maintaining a secure file storage system.

8. End-to-End Encryption:

- Implementing end-to-end encryption ensures 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.

By combining E2EE principles with hybrid cryptography, files are securely encrypted throughout their entire lifecycle, ensuring that only authorized parties with the appropriate decryption keys can access the data. This approach provides a high level of confidentiality and security for stored files, safeguarding sensitive information from unauthorized access or interception. Regular reviews and adherence to best practices are essential to maintain the effectiveness of this security framework.

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.

By integrating data backup, redundancy, and hybrid cryptography, the file storage system enhances data availability, protects against data loss, and maintains

confidentiality even in backup scenarios. Regular assessments, monitoring, and testing of backup and redundancy strategies are critical to ensuring the integrity and effectiveness of the overall data protection measures.

10. Secure Authentication and User Management:

Incorporating secure authentication and robust user management into a secure file system that utilizes hybrid cryptography is crucial for controlling access and ensuring the confidentiality of stored data.

Strong user authentication methods, such as multi-factor authentication (MFA), enhance the security of file storage systems. User management systems ensure that only authorized users gain access. By integrating secure authentication, robust user management practices, and proper key management with hybrid cryptography, the file storage system can ensure that only authorized users have access to sensitive data, maintaining confidentiality and security throughout the system. Regular audits, updates, and user education are essential for maintaining a secure environment

11. Auditing and Logging:

- The implementation of auditing and logging mechanisms helps monitor and track access and changes to files, providing transparency and facilitating security monitoring. By integrating robust auditing and logging mechanisms into the secure file storage system that utilizes hybrid cryptography, organizations can proactively monitor activities, detect security threats, and ensure compliance with regulations. Regular reviews, analysis, and adaptation of logging practices are crucial to maintaining the system's security posture.

12. Security Updates and Patch Management:

- Regularly updating and patching software and systems is essential to address security vulnerabilities and maintain the ongoing security of the file storage system.

By establishing a comprehensive security update management strategy, regularly applying patches, maintaining secure configurations, monitoring for threats, and keeping personnel educated and informed, organizations can significantly enhance the security posture of their secure file storage systems leveraging hybrid cryptography. Regular reviews and adjustments to update processes based on emerging threats and best practices are critical for maintaining a robust security stance.

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. Compliance with regulations is crucial to protect sensitive data, ensure privacy, and mitigate the risk of penalties or legal consequences resulting from non-compliance. Adhering to these standards helps build trust with customers, partners, and regulatory bodies while enhancing overall security measures within the file storage system.

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.

6. OBJECTIVES

Creating a project focused on a file storage system using hybrid cryptography involves pursuing a range of objectives, which can encompass:

- **Data Protection:** Implement a robust data protection strategy by employing a hybrid cryptography approach. This method involves using both symmetric and asymmetric encryption techniques to safeguard stored files. Symmetric encryption ensures efficient data handling by using a single key for both encryption and decryption, while asymmetric encryption enhances security by using a pair of keys for encryption and decryption. This combination maintains the confidentiality and integrity of sensitive data, preventing unauthorized access and ensuring that files remain unchanged during transmission or storage.
- **Efficiency in Data Management**: Achieving an optimal balance between stringent security measures and efficient data handling involves optimizing the file storage system. This optimization includes streamlining processes to ensure data security without compromising performance. By employing optimized encryption algorithms and efficient data transmission methods, the system ensures that files are securely stored while remaining practical for everyday use. This balance facilitates seamless user experience without sacrificing the system's security integrity.

- **Robust Key Management:** A comprehensive key management infrastructure is crucial for secure data handling. Establishing robust protocols for key generation, distribution, and storage is vital for both symmetric and asymmetric encryption components. This infrastructure ensures that cryptographic keys are securely managed throughout their lifecycle. It includes practices for secure key generation, secure storage mechanisms, key rotation policies, and stringent access controls to safeguard these critical elements of encryption.
- **Secure Data Exchange:** Developing mechanisms for secure data transmission and sharing involves implementing end-to-end encryption protocols. These protocols ensure that data remains encrypted from the sender to the recipient, protecting it against potential eavesdropping or interception. By utilizing strong encryption algorithms and secure transmission channels, the system facilitates secure data exchange, enabling users to share files confidently without compromising data security.
- **User Verification:** Implementing robust user authentication procedures guarantees that only authorized individuals can access stored files and decrypt data. This involves employing multifactor authentication, biometric verification, or strong password policies to ensure the legitimacy of user access. Proper user verification ensures that only authenticated users with the correct cryptographic keys can decrypt and access sensitive information, adding an extra layer of security
- **File Data Integrity Verification:** Deploying methods to verify file integrity during storage and retrieval is crucial for ensuring that files remain unchanged and uncorrupted. By using techniques such as checksums, digital signatures, or hash functions, the system can confirm that files have not been tampered with or altered. This verification process enables the detection of any unauthorized modifications to files, ensuring data integrity throughout the storage and retrieval processes.

- **Access Control Mechanisms:** Implement access control measures that govern user permissions meticulously. By employing role-based access control (RBAC) or attribute-based access control (ABAC), the system ensures that users access only the files they have explicit authorization to view or modify. This granular control enhances security by restricting unauthorized access to sensitive data, bolstering confidentiality.
- **Adherence to Regulations:** Aligning the project with relevant legal mandates and industry standards involves a thorough understanding of regulations such as GDPR, HIPAA, or other data protection laws. Compliance involves implementing specific measures within the system, ensuring data privacy, user consent management, data breach notification procedures, and other compliance requirements.
- **User-Friendly Interface:** Designing an intuitive user interface simplifies user interaction with the file storage system. This includes employing user-centric design principles, clear navigation, and easy-to-understand visual cues. Making secure practices seamless and convenient encourages users to adopt and adhere to secure file management practices.
- **Data Redundancy and Backups:** Implementing data redundancy mechanisms ensures data availability and resilience against system failures or data loss. Regular backups of stored files guarantee that even in the event of hardware failure or accidental deletion, data can be recovered, maintaining system reliability.
- **Auditing and Logging System:** Develop a robust auditing and logging system to monitor user activities and access. This system tracks user interactions within the file storage system, providing an audit trail for security and compliance purposes. Detailed logs enable administrators to trace any suspicious activities and ensure accountability.

- **Scalability and Versatility:** Constructing a scalable system enables it to accommodate increasing data volumes and adapt to various infrastructure environments seamlessly. Employing scalable storage solutions and flexible architecture allows for expansion without compromising performance or security.
- **Education and Awareness:** Providing comprehensive educational resources and documentation educates users about data security significance, encryption practices, and best security protocols. Training materials and guides empower users and administrators to utilize the system securely, fostering a culture of data security awareness within the organization.
- **Performance Enhancement:** Continuously optimizing the system involves fine-tuning processes to maintain a balance between robust security measures and high performance. Regular performance evaluations and optimizations ensure that security enhancements do not hinder the system's efficiency
- **Vulnerability Mitigation:** Identify and rectify potential vulnerabilities within the file storage system, including addressing emerging threats and weaknesses in cryptographic methods. Regular security audits and updates mitigate risks, ensuring the system remains resilient against evolving threats.
- **User Assistance and Training:** Offering support and training enhances user and administrator proficiency in utilizing the system securely. Providing resources, workshops, and help desks ensures users can navigate the system while adhering to security best practices.
- **Cost-Effective Solution:** Develop a solution that prioritizes robust security measures without significantly escalating costs. This involves cost-benefit analyses, optimizing resource utilization, and choosing efficient but secure technologies to ensure the project's financial sustainability.

- **Advancement and Research:** Contribute to ongoing research and innovation in data security, cryptography, and secure storage systems. Staying abreast of advancements allows for the integration of cutting-edge technologies, improving the system's security posture and resilience. Additionally, sharing insights and contributing to the field fosters advancements in the broader domain of data security.

The particular objectives of a project concentrated on file storage using hybrid cryptography can vary depending on the project's scope, target audience, and the specific requirements of the organization or users it seeks to serve.

7. SCOPE

The scope of a project focused on creating a file storage system using hybrid cryptography can be broad and encompass various aspects. Here's a comprehensive scope for this project:

- **System Architecture and Design:**

a. Define the architecture and design of the file storage system, outlining the components, their interactions, and data flow.
b. Specify the encryption algorithms and key management mechanisms used in the system.

- **Data Encryption and Security:**

a. Implement hybrid cryptography techniques to secure stored data, ensuring confidentiality and integrity.
b. Develop robust encryption and decryption processes to safeguard sensitive files.

- **User Authentication and Authorization:**

a. Implement user authentication mechanisms to verify user identities.

b. Set up access control and authorization systems to manage user permissions and roles.

- **Compliance and Regulatory Adherence:**

a. Ensure the project aligns with relevant data protection regulations and industry standards, considering privacy laws like GDPR, HIPAA, and others.

- **User Interface and User Experience:**

    a. Design an intuitive user interface for the file storage system that simplifies file management and encryption processes.

- **Performance Optimization:**

a. Continuously optimize the system to maintain a balance between security and performance.

- **User Support and Training:**

a. Offer user support and training resources to educate users about the importance of data security and best practices for utilizing the file storage system.

The scope of the project can be tailored to the specific goals and requirements of the organization or users for whom the file storage system is being developed. It should encompass all aspects necessary to create a secure, efficient, and user-friendly file storage solution using hybrid cryptography.

8. METHODOLOGY

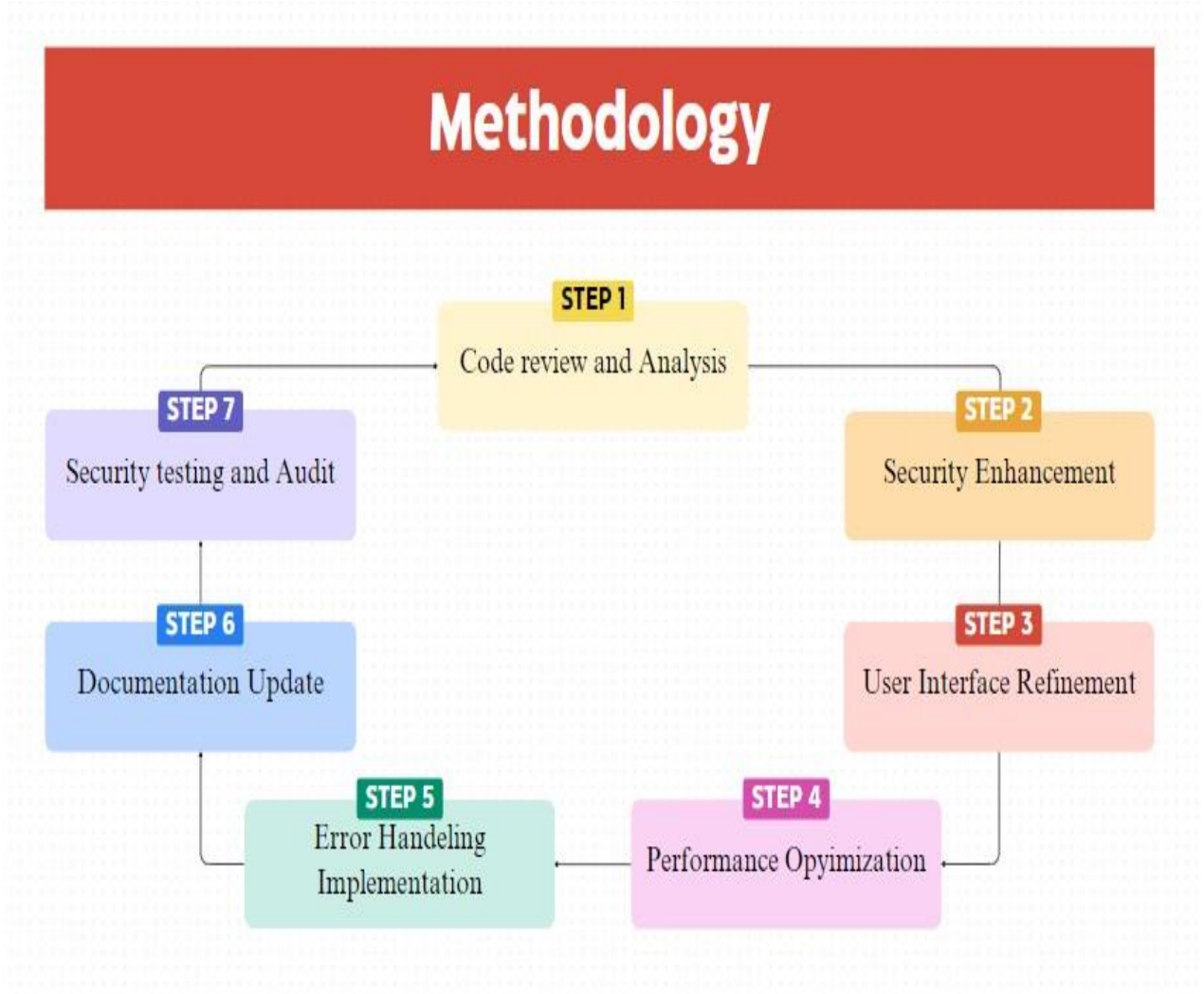

Fig 3: Methodology

The methodology involves the following steps:

Code review and analysis:

- Codebase Assessment: Scrutinize the existing project codebase, comprehensively examining its structure, modules, and functions.

- Architecture Understanding: Gain a deep understanding of the project's architecture, including its design patterns, frameworks, and overall flow.
- Encryption Methodology Evaluation: Analyze existing encryption methods, reviewing algorithms, key generation, and encryption/decryption processes.
- User Interface Component Examination: Explore the user interface components, evaluating design patterns, responsiveness, and usability across devices and platforms.

Security Enhancement:

- Stronger Encryption Integration: Integrate robust and modern encryption algorithms to fortify data security.
- Cryptographic Library Update: Update cryptographic libraries to the latest versions, addressing known vulnerabilities and leveraging new security features.
- Secure Key Management Implementation: Implement best practices for secure key management, including key generation, storage, rotation, and access control.

User Interface Refinement:

- UI Design Enhancement: Improve the user interface design by refining layouts, visual elements, and interactive components for a more appealing and intuitive user experience.
- Navigation Optimization: Streamline navigation pathways, ensuring smoother transitions and easier access to functionalities.

Performance Optimization:

- Encryption Process Analysis: Analyze encryption and decryption operations to identify performance bottlenecks and inefficiencies.
- Optimization Implementation: Implement optimizations to enhance the speed and efficiency of encryption/decryption processes without compromising security.

Error Handling Implementation:

- Error Scenario Identification: Identify potential error scenarios throughout the application.
- User-Friendly Error Messages: Develop mechanisms to handle errors gracefully, providing users with clear and informative error messages to facilitate troubleshooting and resolution.

Documentation update:

- README and Documentation Review: Revise and update project documentation, including the README file, installation guides, configuration instructions, usage manuals, and troubleshooting tips.
- Clarity and Completeness: Ensure that the documentation is comprehensive, clear, and easily understandable for both developers and end-users.

Security testing and Audit:

- Comprehensive Security Testing: Conduct rigorous security testing using penetration testing tools and techniques to uncover vulnerabilities.
- Vulnerability Rectification: Address identified security vulnerabilities promptly, implementing necessary fixes and security patches.

9. ALGORITHM/ FLOW CHART

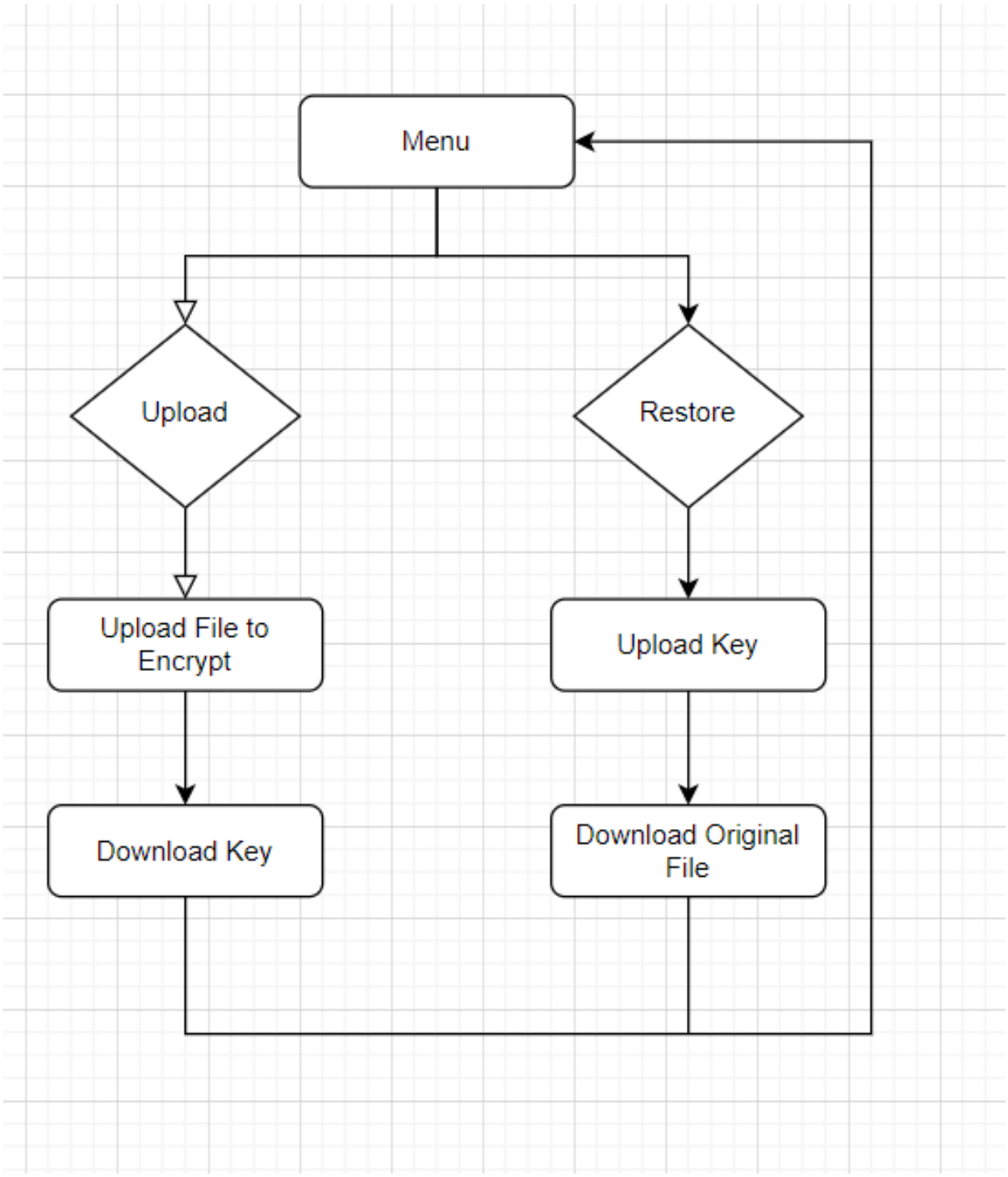

Fig 4: Flow Chart

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.

10. RESULT

Figure 5: Home Page

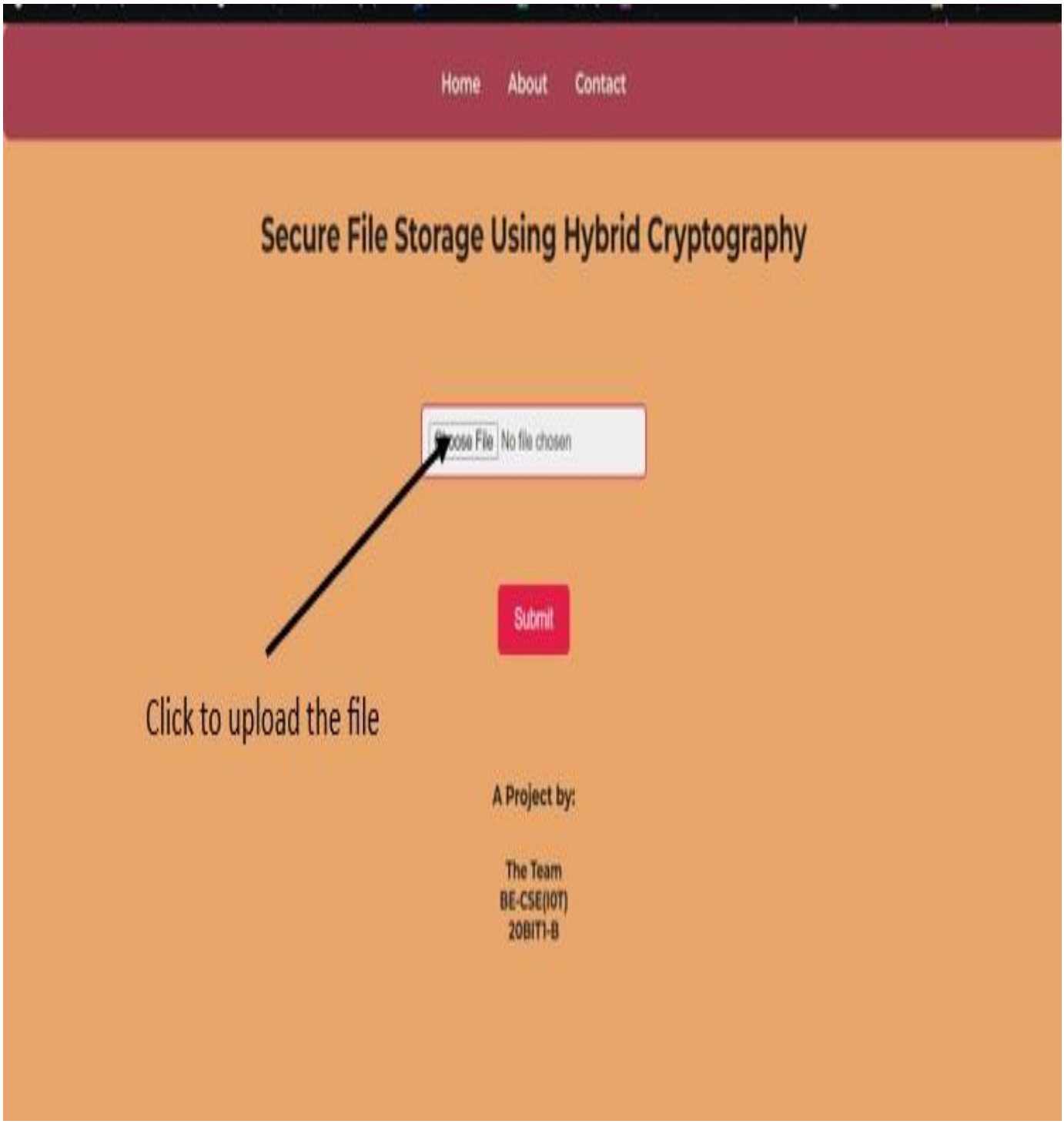

Figure 6: Upload page

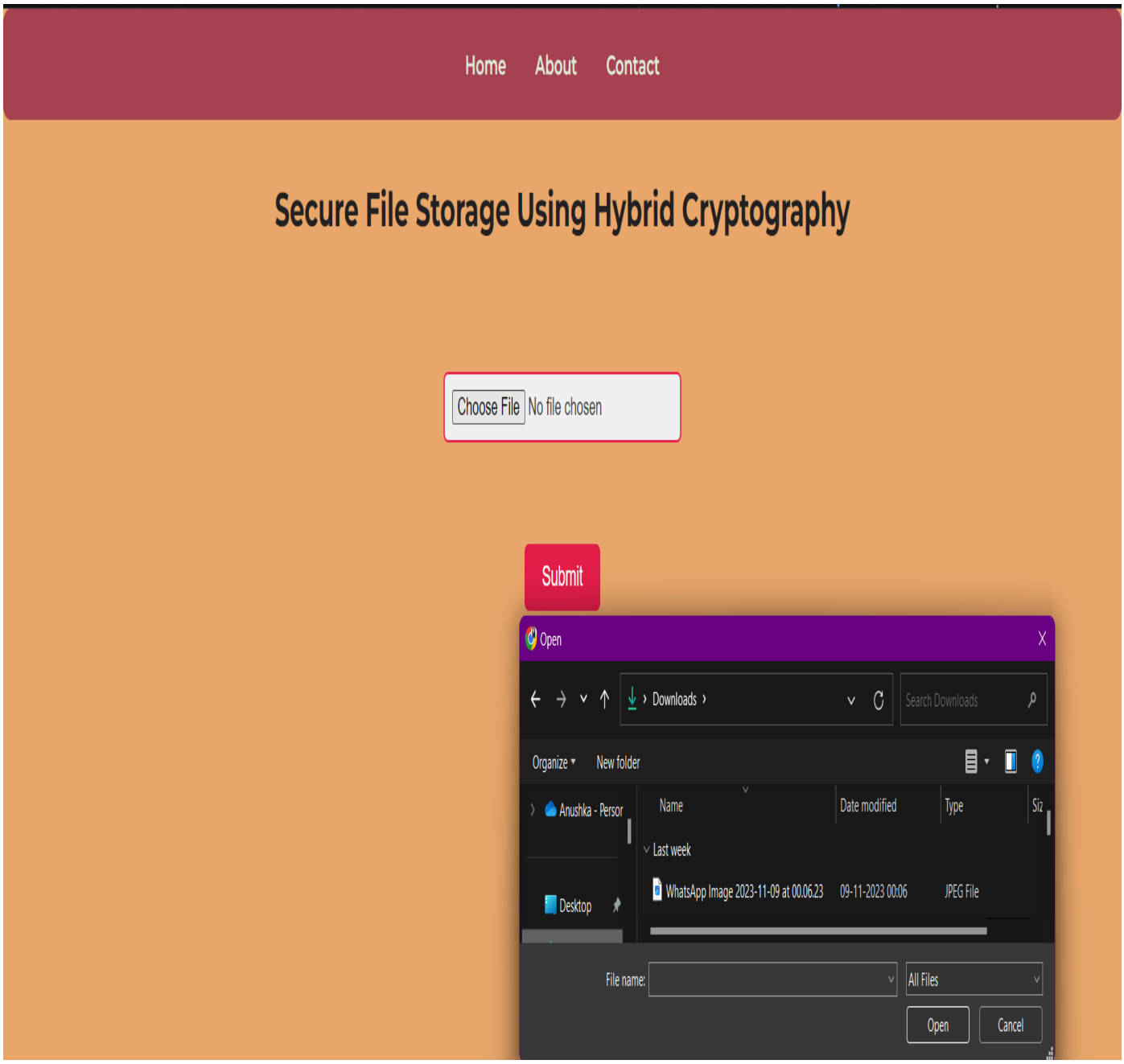

Figure 7: Uploading a File

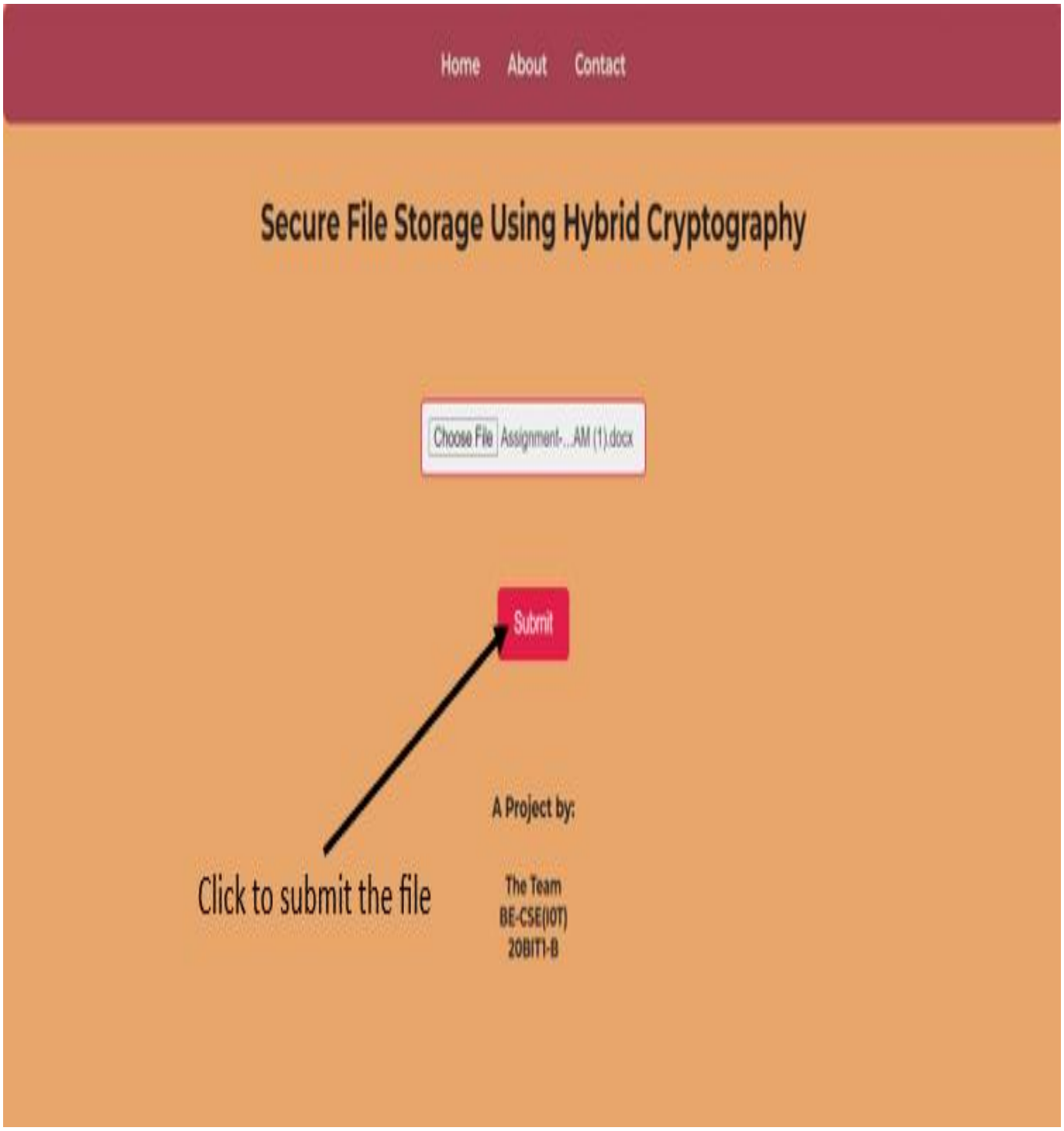

Figure 8: Submitting the file

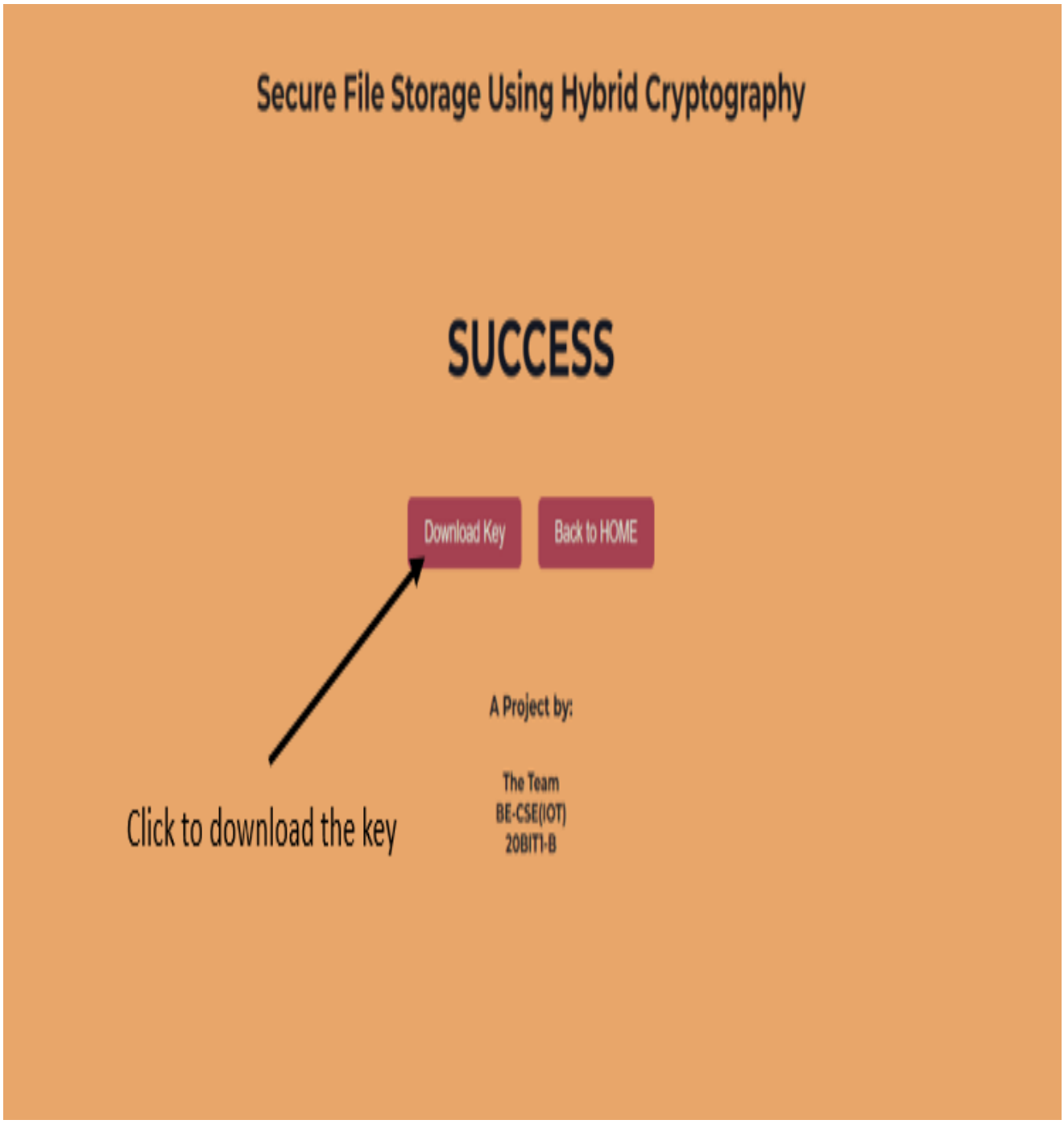

Figure 9: Downloading the cryptographic key

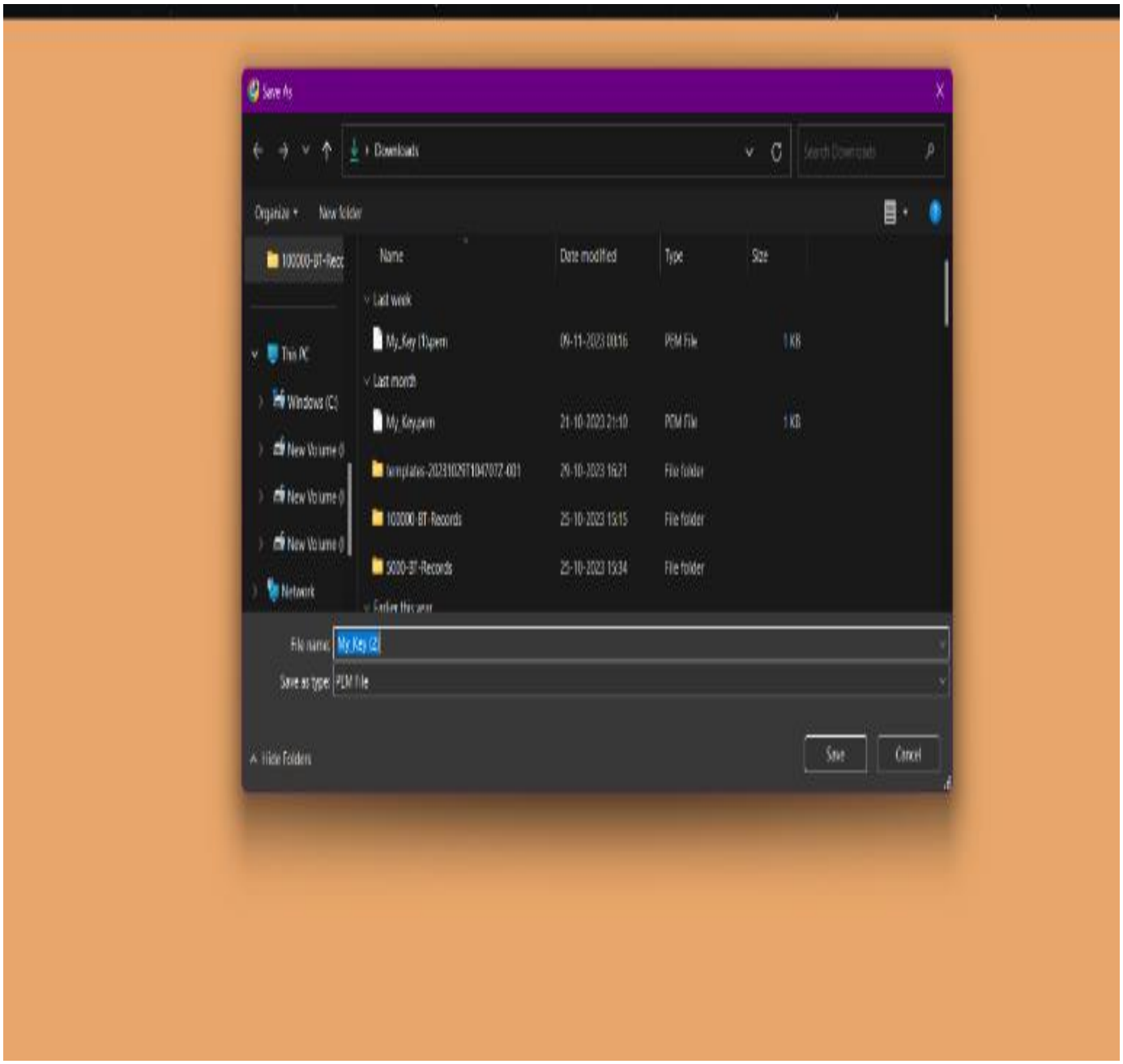

Figure 10: Selecting the download location

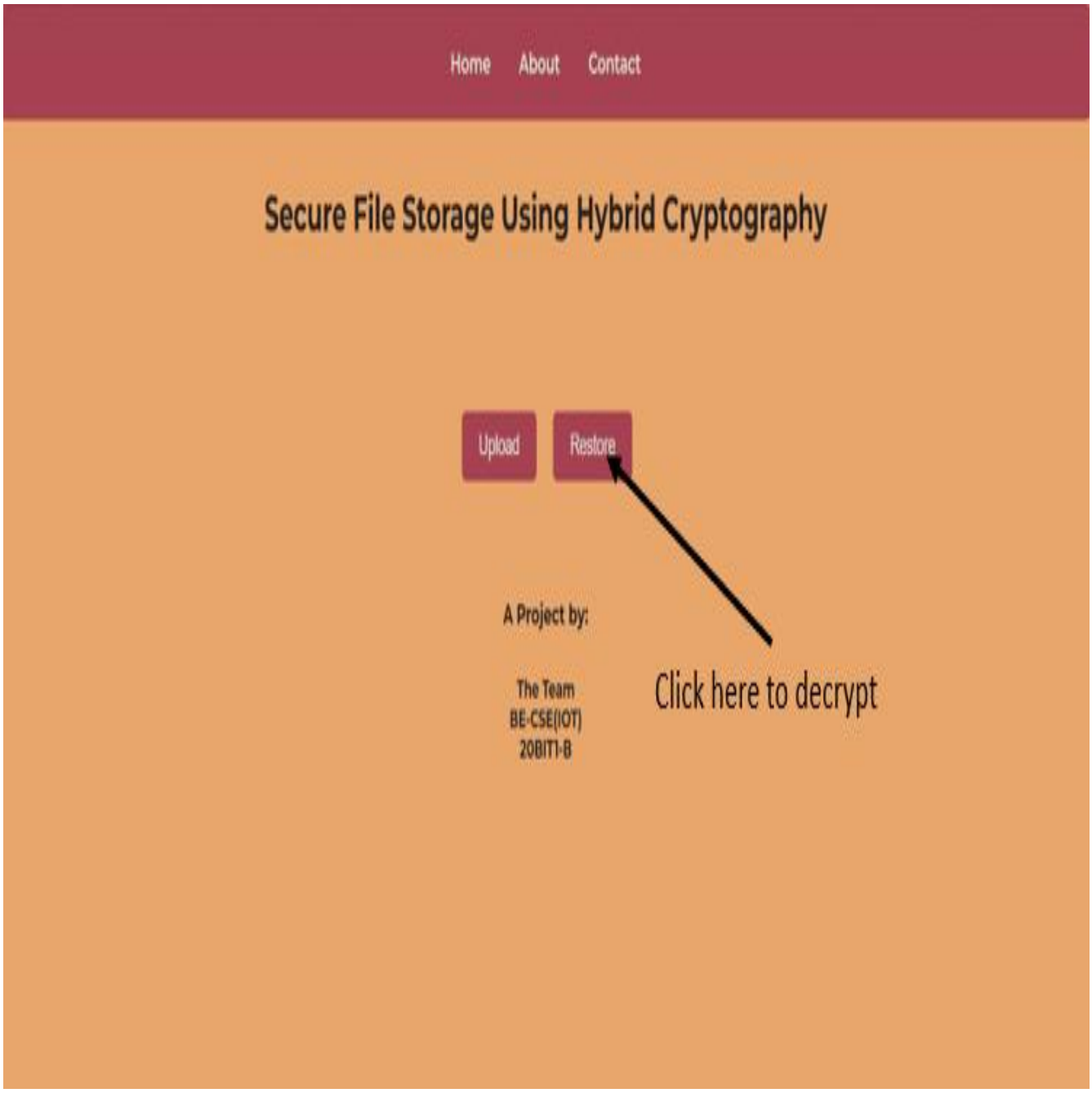

Figure 11: Restoring/decrypting the file

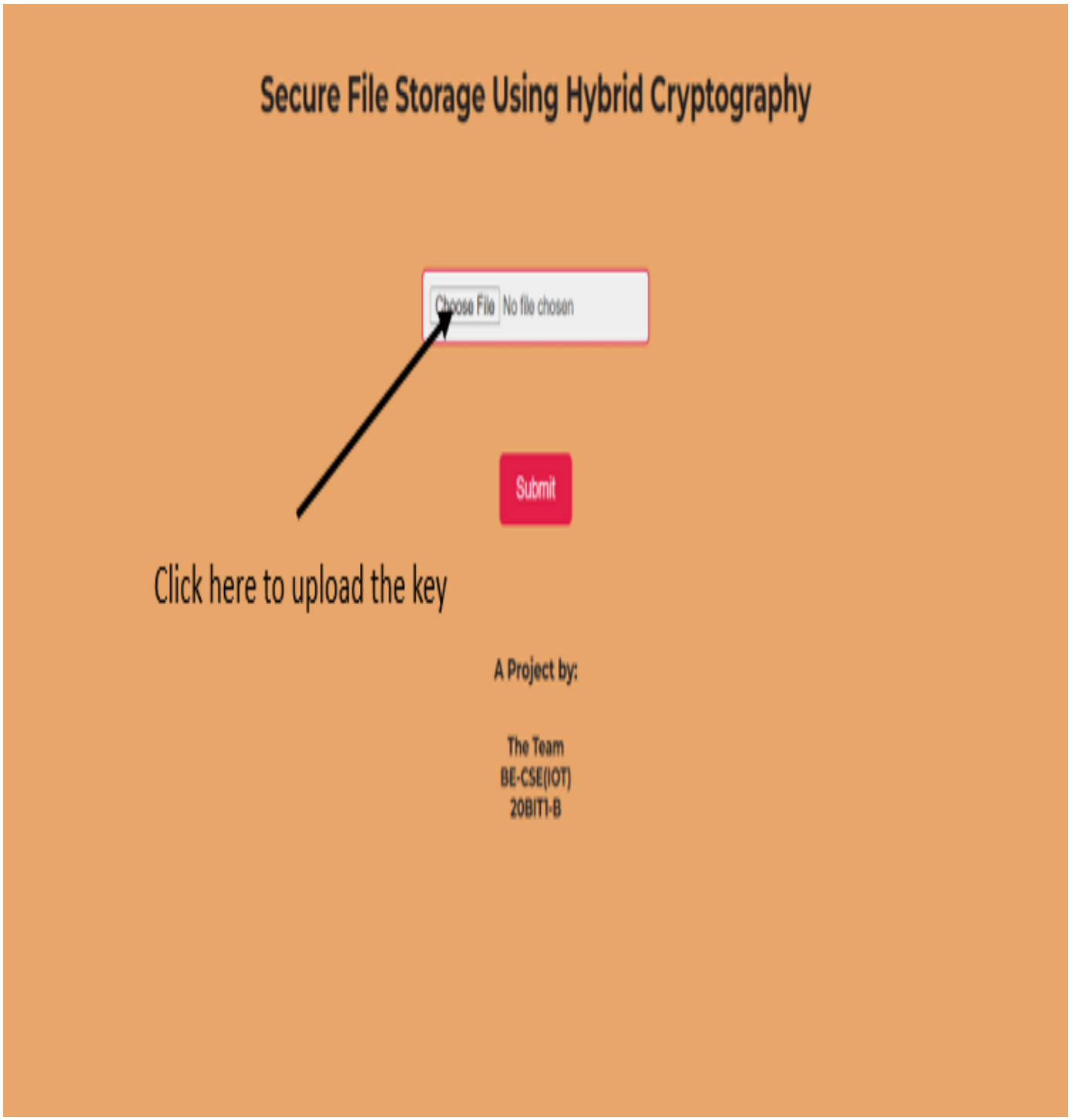

Figure 12: Uploading the downloaded key

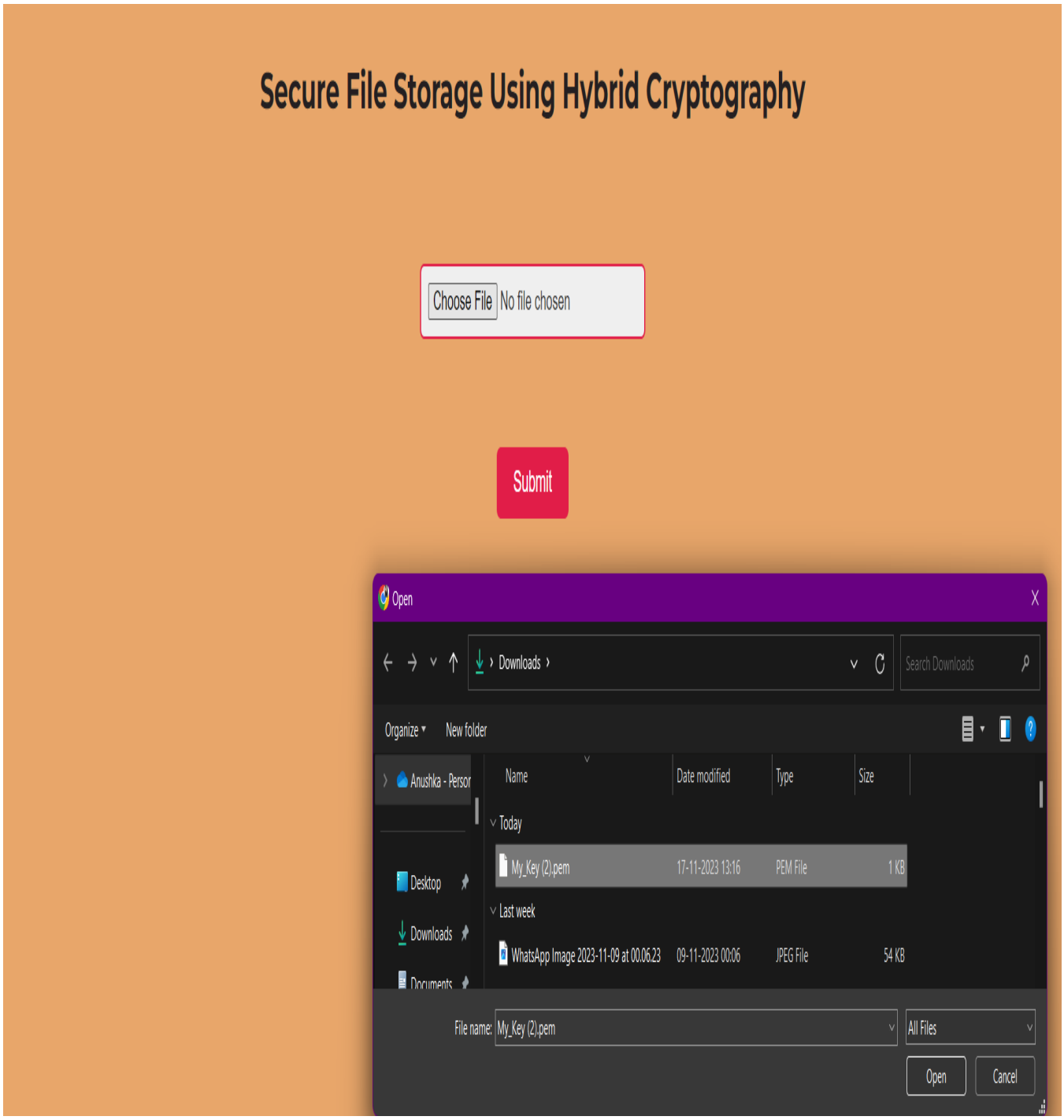

Figure 13: Selecting the key

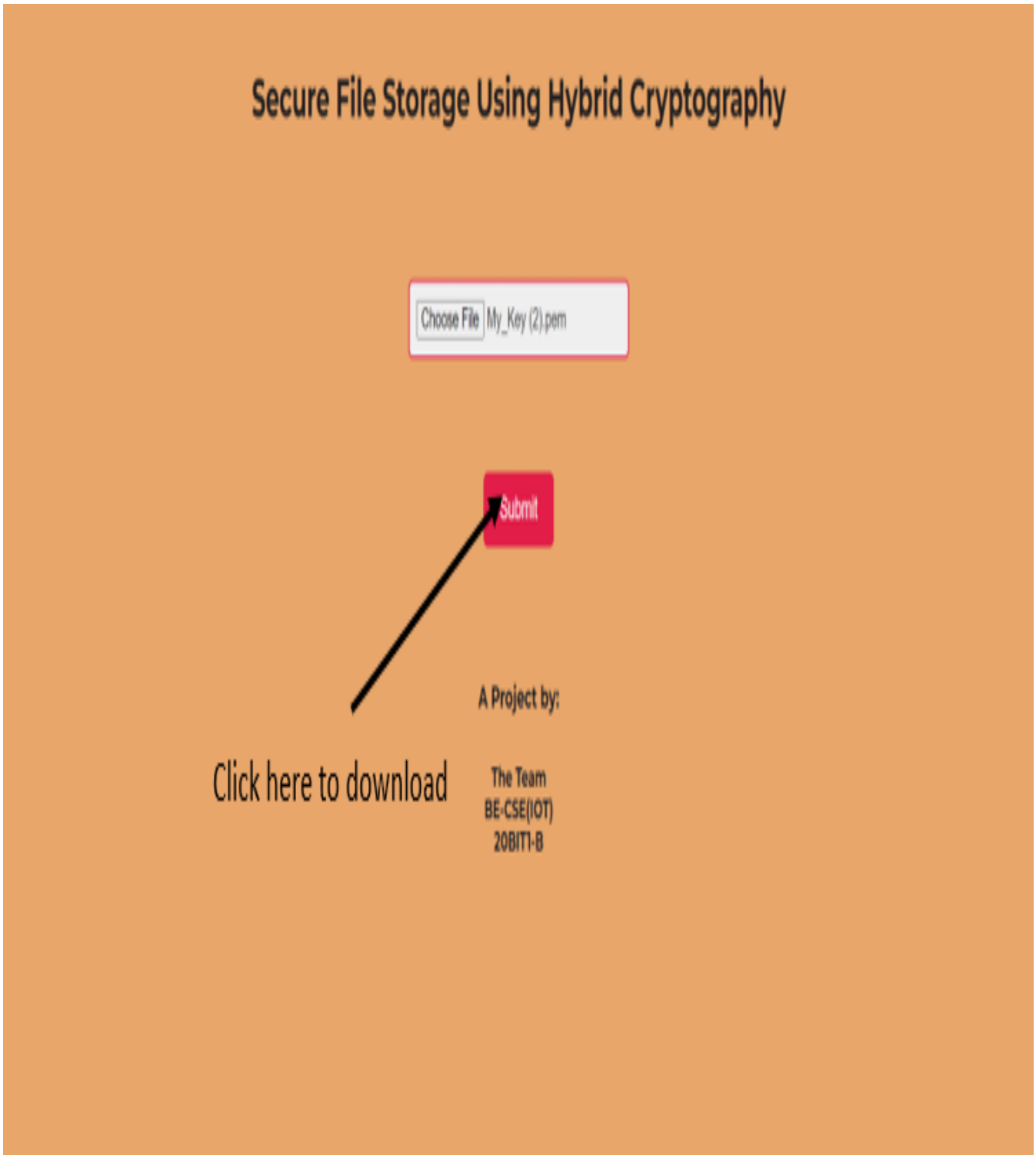

Figure 14: Submitting the key

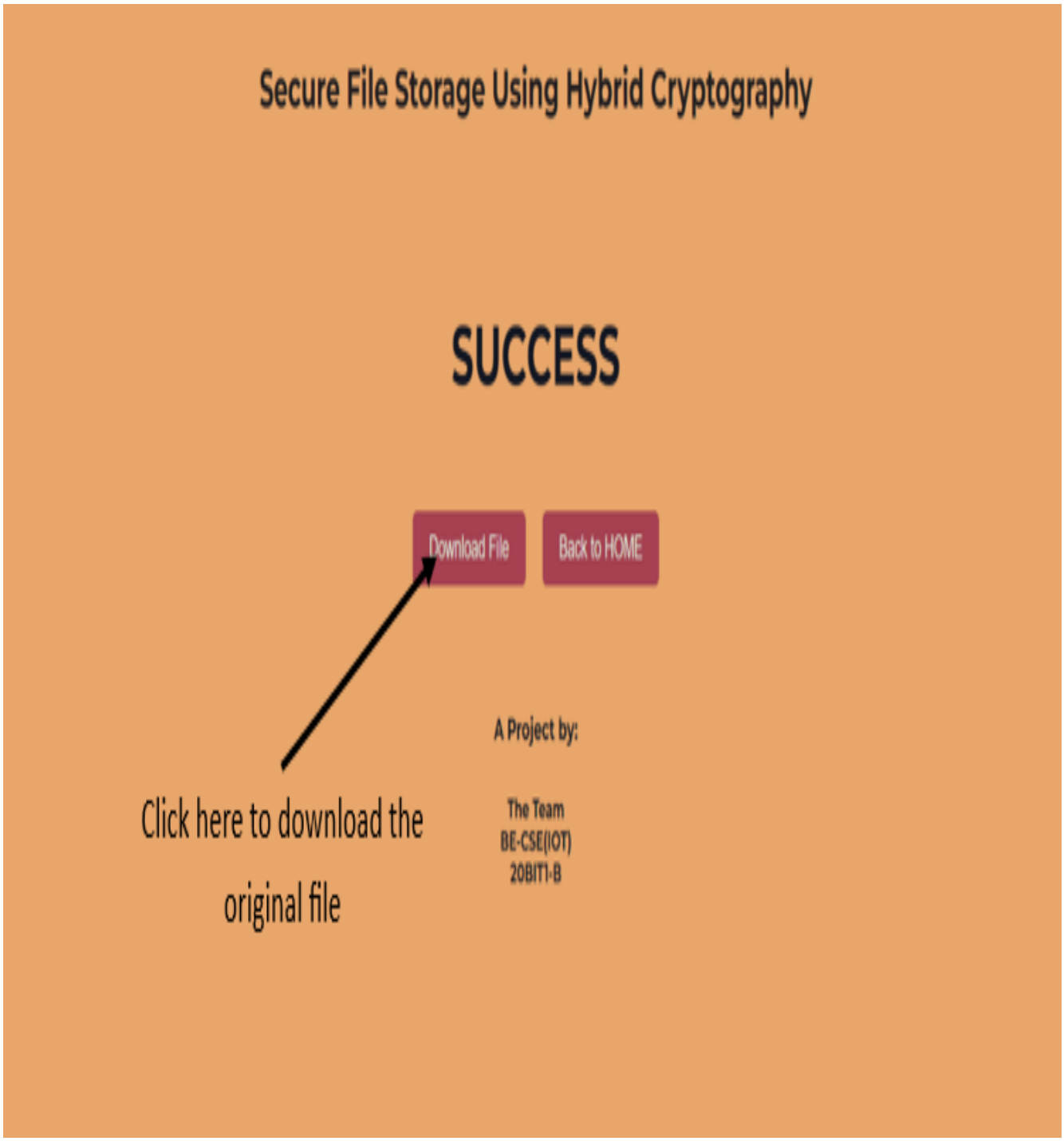

Figure 15: Downloading the original file

Figure 5 to *figure 15* demonstrates the working of the presented model. For instance *figure 5* 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 6 to 10 shows how a file can be uploaded into the system and how a cryptographic key can be generated for the same.

Figure 10 to 15 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 16).*

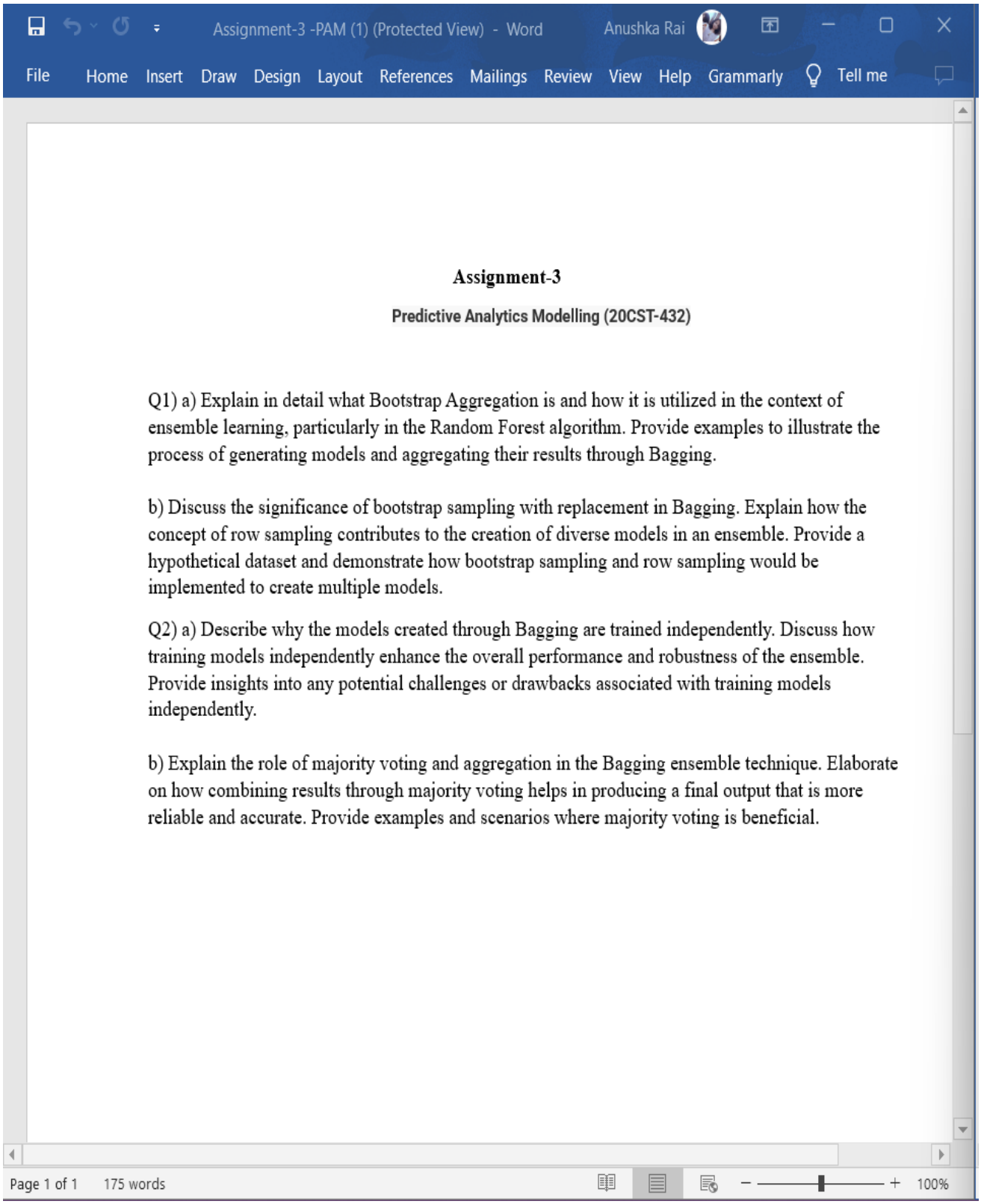

Figure 16: Initially uploaded file

After the decryption, the downloaded file is the one given below in *figure 17.*

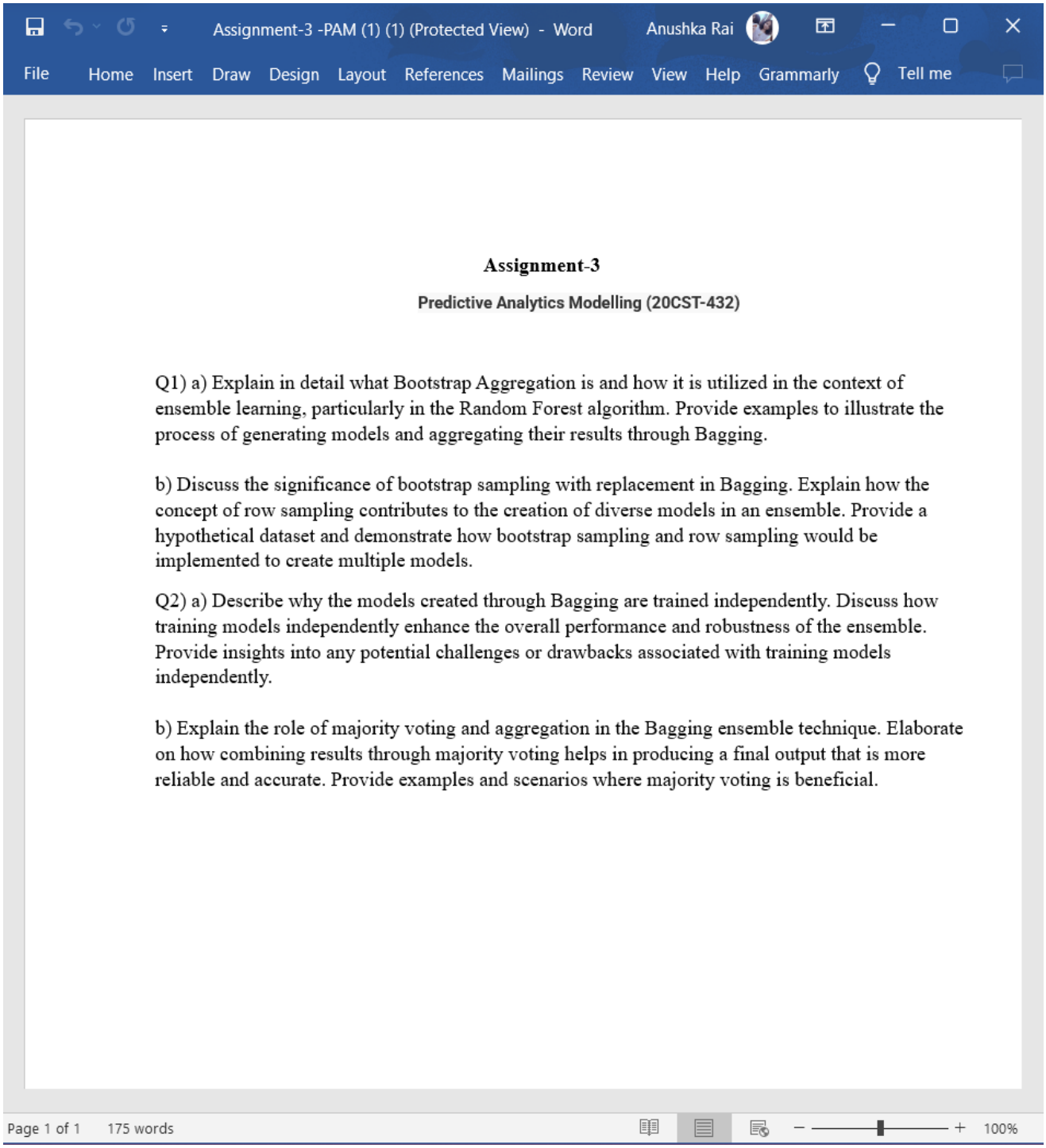

Figure 17: Downloading the decrypted file

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*.

11. 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 my supervisor Mrs. Bhavna Nayyer, for their invaluable guidance, insightful feedback, and unwavering support throughout the course of this research project. Their expertise and dedication have been instrumental in shaping 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).