Secret File Exchange Between Two Parties

Mr.K.V.SivaPrasadReddy [1], K.Naveen[2], J.Ganesh[3], T.Keshav[4] and SK.Masthan[5]
Assistant Professor[1] Student/Research Scholar[2],[3],[4],[5]

Department of Cyber Security
Malla Reddy University, Hyderabad
Maisammaguda, Dulapally,Hyderabad,500100, Telangana, India
k.v.sivaprasadreddy@mallareddyuniversity.ac.in [1]-
2111CS040059@mallareddyuniversity.ac.in[2] , 2111CS040031,@mallareddyuniversity.ac.in[3]
,2111CS040046@mallareddyuniversity.ac.in[4] , 2111CS040055@mallareddyuniversity.ac.in[5] ,

Abstract- The Secret File Exchange Between Two Parties is a sophisticated computational model designed to enable secure collaboration and computation among multiple parties while preserving data privacy and confidentiality. This project aims to develop a secure file exchange system facilitating confidential communication between two parties. In an era of escalating digital threats, ensuring the privacy and integrity of exchanged files is paramount. This report outlines the design and implementation of such a system. The system employs a client-server architecture with end-to-end encryption. Clients authenticate using secure credentials, establishing a trusted connection to the server. File exchange occurs through encrypted channels, safeguarding data from interception or tampering. Utilize strong encryption algorithms such as Advanced Encryption Standard (AES) to encrypt files before storage and transmission. Generate unique encryption keys for each file exchange session to enhance security. Implement secure key management practices to protect encryption keys from unauthorized access. using masking techniques is by applying data masking or obfuscation methods to conceal specific parts of the file content while still allowing authorized users to access the unmasked data.

Keywords: end-to-end encryption, data masking, Advanced Encryption Standard, client-server architecture

I.INTRODUCTION

This project aims to address the escalating digital threats by developing a secure file exchange system, where the privacy and integrity of exchanged files are paramount. In today's digital landscape, the exchange of sensitive information between parties demands a sophisticated solution that ensures both security and confidentiality. The Secret File Exchange Between Two Parties stands as a testament to such a need, offering a robust computational model designed to facilitate secure collaboration and communication while safeguarding data privacy. Employing a client-server architecture fortified with end-to-end encryption, users authenticate using secure credentials, establishing a trusted connection to the server. Through encrypted channels, file exchange occurs seamlessly, shielding data from interception or tampering·**[6]** By leveraging strong encryption algorithms like the Advanced Encryption Standard (AES) and generating unique encryption keys for each session, the system enhances security measures. Additionally, implementing secure key management practices ensures protection against unauthorized access. Additionally, masking techniques are employed to conceal specific parts of the file content, while allowing authorized users access to unmasked data**[5]**

II. LITERATURE SURVEY

The Secret File Exchange Between Two Parties addresses the critical need for secure collaboration and communication in today's digital landscape. In light of escalating digital threats, maintaining the privacy and integrity of exchanged files is imperative. With the proliferation of sensitive information being shared among multiple parties, a robust computational model is required to ensure data privacy and confidentiality**[6-7]** Various studies have emphasized the importance of implementing secure file exchange systems to protect against unauthorized access and interception. End-to-end encryption has emerged as a key strategy in securing data during transmission, ensuring that only authorized parties can access the information. Strong encryption algorithms like the Advanced Encryption Standard (AES) have been widely adopted due to their effectiveness in safeguarding data**[9]**

Additionally, the application of masking techniques, such as data masking or obfuscation methods, adds an extra layer of security by concealing specific parts of the file content while still allowing authorized users to access the unmasked data. This ensures that sensitive information remains protected even in the event of unauthorized access·**[8]** Introduces a cutting-edge computational model aimed at fostering secure collaboration and computation while preserving the confidentiality and privacy of exchanged files. In light of the increasing digital threats, the need to safeguard the integrity and privacy of shared data has become paramount. This project endeavors to develop a secure file exchange system specifically designed to facilitate confidential communication between two parties [1] .The literature underscores the critical importance of implementing robust security measures in file exchange systems to mitigate the risks associated with unauthorized access, interception, and tampering of sensitive information. End-to-end encryption emerges as a fundamental strategy in ensuring data security during transmission, guaranteeing that only authorized parties have access to the exchanged files [2-3] .The utilization of strong encryption algorithms, such as the Advanced Encryption Standard (AES), further enhances thesystem's resilience against cyber threats. Furthermore, the generation of unique encryption keys for each file exchange session significantly bolsters security measures by minimizing the likelihood of key compromise. Secure key management practices play a pivotal role in safeguarding encryption keys from unauthorized access, thereby mitigating the risk of data breaches and ensuring the confidentiality of exchanged files·[3] In addition to encryption, the application of masking techniques, such as data masking or obfuscation methods, provides an additional layer of security by concealing specific parts of the file content while still allowing authorized users to access the unmasked data[8-9] This ensures that sensitive information remains protected, even in the event of unauthorized access or interception. The importance of developing secure file exchange systems like the one proposed in this project. By employing a client-server architecture with end-to-end encryption, strong encryption algorithms, unique encryption keys, secure key management practices and masking techniques, the system aims to provide a robust and secure platform for confidential communication and collaboration between parties[6-7]

III. SYSTEM ANALYSIS

A. Existing System

This file exchange often lack comprehensive security measures, leaving sensitive data vulnerable to interception and unauthorized access. Traditional methods such as email attachments or unsecured file sharing platforms are commonplace but pose significant risks to data privacy and integrity[5] These systems typically rely on basic authentication mechanisms, which may be susceptible to breaches or unauthorized access by malicious actors. without end-to-end encryption, there is no guarantee of the confidentiality of exchanged files·[7] File exchange processes often occur over unencrypted channels, exposing data to potential interception or tampering during transmission·[10]

- ➢ Inadequate Key Management
- ➢ Weak Authentication Mechanisms
- ➢ Lack of End-to-End Encryption
- ➢ Scalability Issues

B. Proposed System

To address existing system limitations, we've developed a more efficient tool for a robust computational model that ensures data privacy and confidentiality. By employing end-to-end encryption, strong encryption algorithms like AES, and unique encryption keys for each session, the system enhances security measures. Secure key management practices and data masking techniques further fortify the system against unauthorized access, providing a trusted platform for confidential communication between parties A and B This comprehensive approach addresses the pressing need for secure collaboration amidst escalating digital threats, safeguarding sensitive information throughout the exchange process characters,and attack weight. -ese features were calculated for four different datasets CSIC 2010, HTTP

IV. METHODOLOGY

Secret File Exchange Between Two Parties project involves a combination of techniques to ensure secure collaboration and communication while preserving data privacy and confidentiality. Specifically, the project employs a client-server architecture, end-to-end encryption, strong encryption algorithms like AES, unique encryption keys for each session, secure key management practices, and masking techniques such as data masking or obfuscation·[6] These methods collectively contribute to the development of a secure file exchange system that facilitates confidential communication between two parties, safeguarding data from interception or tampering and protecting encryption keys from unauthorized access[10]·

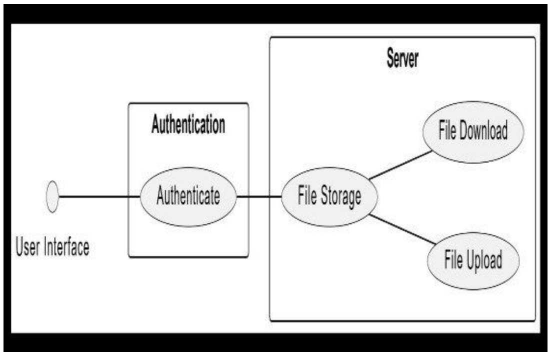
System Framework Integration:

File Exchange Between Two Parties encompasses a client-server architecture with end-to-end encryption·[9] This integration ensures secure authentication, encrypted file exchange through trusted connections, and the implementation of strong encryption algorithms like AES. Additionally, the generation of unique encryption keys for each session and the utilization of masking techniques further enhance security measures, safeguarding data privacy and confidentiality during file transmission and storage

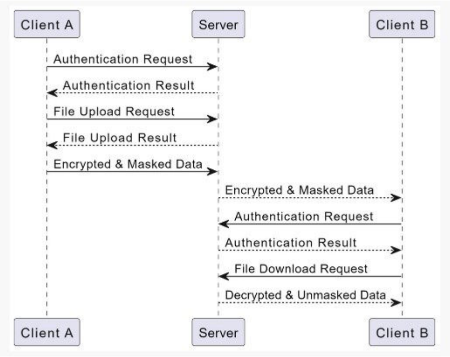
V. DATA FLOW OF THE PROBLEM

A Data Flow Diagram (DFD) is a visual tool used to analyze how data moves within a system, whether manual or automated. It shows processes, data storage, and any delays in the system. DFDs are essential as they form the basis for developing other parts of the system and provide a logical description of how data flows from input to output, regardless of the physical components involved. In system modeling, DFDs clarify the requirements for building a new system. During design, they are used to create structure charts for the system. Basic Notation in DFDs includes symbols like circles (for processes), arrows (for data flow), and rectangles (for data storage). 68 Sometimes called data flow graphs or bubble charts, DFDs offer a visual depiction of system functionality, aiding stakeholders in understanding and communicating requirements.[3] These diagrams help identify potential issues in data flow, allowing for process optimization and improved system performance. Overall, DFDs are integral in the software development lifecycle, providing a structured approach to designing and comprehending complex systems give differently[9-10]

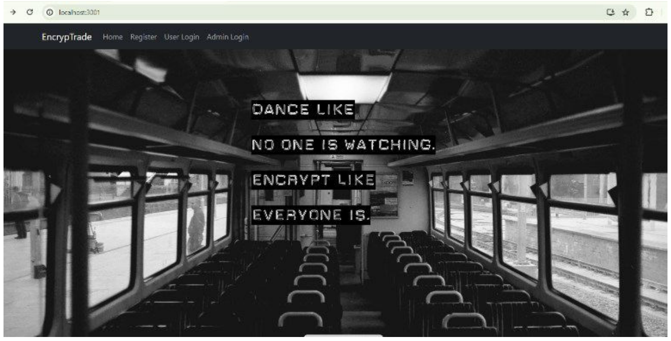
Level 1:

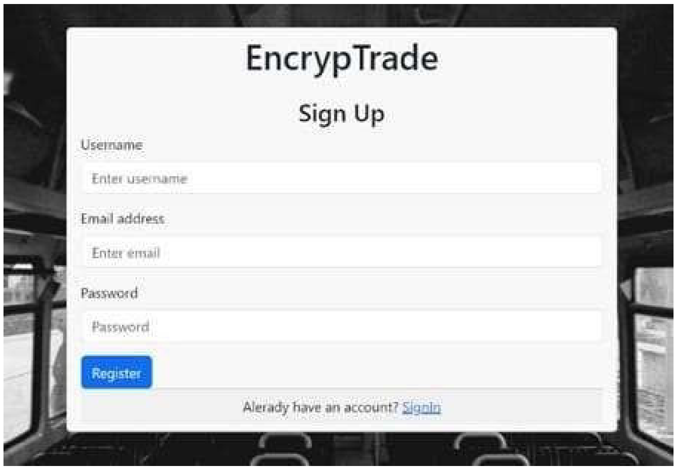


Level 2:



VI. RESULTS





EncrypTrade

Sign Up

Username

Enter username

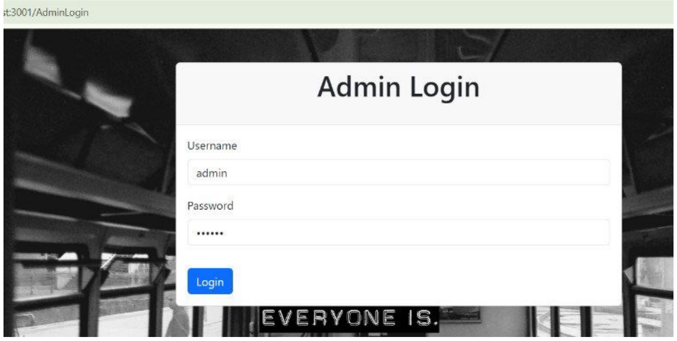
Email address

Enter email

Password

Password

Alerady have an account? Signin



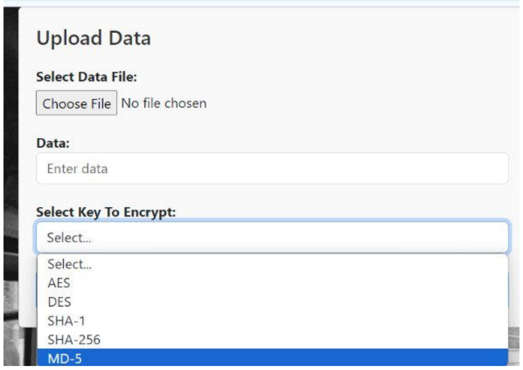
Admin Login

Username

admin

Password

••••••



Upload Data

Select Data File:

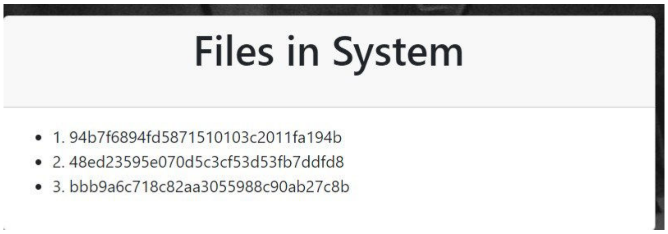
Choose File No file chosen

Data:

Enter data

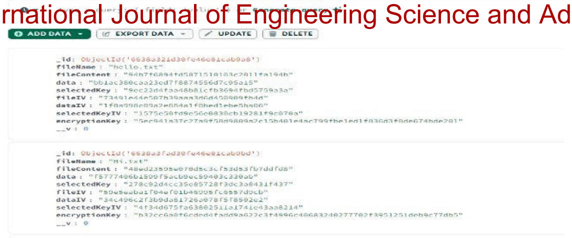
Select Key To Encrypt:

Select...

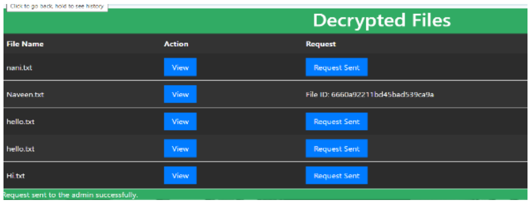


Files in System

- 1. 94b7f6894fd5871510103c2011fa194b
- 2. 48ed23595e070d5c3cf53d53fb7ddfd8
- 3. bbb9a6c718c82aa3055988c90ab27c8b



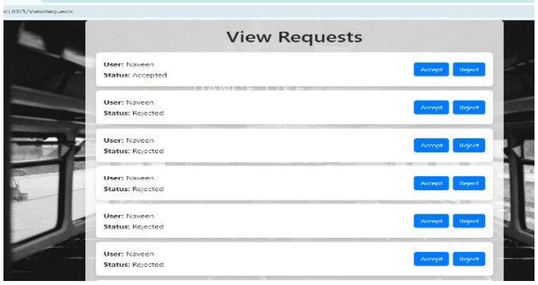
```
_id: ObjectId('6638a321d30fe46e81cab9a8')
fileName : "hello.txt"
fileContent : "94b7f6894fd5871518103c2811fa194b"
data : "bb1ac380caa23ed7f8874556d7c95a15"
selectedKey : "9ec22d4faa48b81cfb3694fbd5759a3a"
fileIV : "73491e44e507b39aaa3d6d450909fb4d"
dataIV : "1f0a998c09a2e684a1f0bed1ebe5ba06"
selectedKeyIV : "1575e50fd9e56e0830cb19281f9c070a"
encryptionKey : "5ec941a37c27a9f58d9809a2c15b401e4ac799fbe1ed1f836d3f0de674bde201"
__v : 0

_id: ObjectId('6638a3fad30fe46e81cab9bd')
fileName : "Hi.txt"
fileContent : "48ed23595e070d5c3cf53d53fb7ddfd8"
data : "f5777406b1599f5acb9ec59403c330ab"
selectedKey : "278c92d4cc35e85728f3dc3a8431f437"
fileIV : "59e5eaba1f04ef01b46995fc6557d9cb"
dataIV : "34c496c2f3b9da81726a078f5f8502e2"
selectedKeyIV : "4f34d675fa63802511a1741c43aa8214"
encryptionKey : "b32cc6a0f6cded4fadd9a622c3f4996c40683240277702f3951251deb9c77db5"
__v : 0
```



Decrypted Files

File Name	Action	Request
nani.txt	View	Request Sent
Naveen.txt	View	File ID: 6660a92211bd45bad539ca9a
hello.txt	View	Request Sent
hello.txt	View	Request Sent
Hi.txt	View	Request Sent

Request sent to the admin successfully.



View Requests

User: Naveen
Status: Accepted

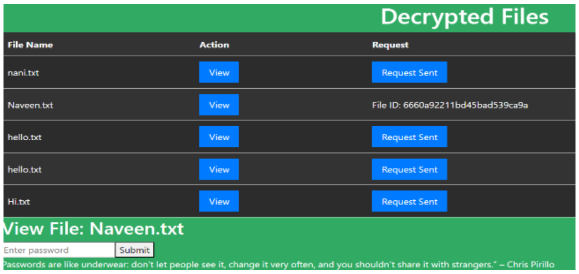
User: Naveen
Status: Rejected

User: Naveen
Status: Rejected

User: Naveen
Status: Rejected

User: Naveen
Status: Rejected

User: Naveen
Status: Rejected



Decrypted Files

File Name	Action	Request
nani.txt	View	Request Sent
Naveen.txt	View	File ID: 6660a92211bd45bad539ca9a
hello.txt	View	Request Sent
hello.txt	View	Request Sent
Hi.txt	View	Request Sent

View File: Naveen.txt

Enter password

Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers." – Chris Pirillo

VI. CONCLUSION

The Secret File Exchange Between Two Parties project successfully addresses the critical need for secure and confidential communication between parties A and B. By employing a client-server architecture with end-to-end encryption, the system ensures the privacy and integrity of exchanged files, mitigating risks associated with digital threats. Key achievements of the project include the implementation of strong encryption algorithms such as Advanced Encryption Standard (AES) and the generation of unique encryption keys for each file exchange session to enhance security measures. Additionally, the adoption of secure key management practices safeguards encryption keys from unauthorized access, further fortifying the system against potential breaches. Furthermore, the integration of masking techniques, including data masking and obfuscation methods, allows for the concealment of sensitive file content while enabling authorized users to access unmasked data, ensuring confidentiality without compromising usability. Overall, the Secret File Exchange Between Two Parties system represents a significant advancement in facilitating secure collaboration and communication while prioritizing data privacy and confidentiality in an era of escalating digital threats."

VII. FUTURE SCOPE

However, there are several avenues for future expansion and improvement it can be Extend the system to support secure collaboration among multiple parties beyond just two. This could involve enhancing the client-server architecture to accommodate multiple users and implementing robust access control mechanisms to manage permissions and data sharing. Focus on improving the user experience by developing user-friendly interfaces and Consider integrating blockchain technology to enhance data integrity and accountability. Using blockchain for file exchange and authentication can provide immutable records of transactions, reducing the risk of data tampering and ensuring the integrity of exchanged files.

VIII. REFERENCES

[1]https://www.researchgate.net/publication/48194690_Design_and_Implementation_of_a_Secure_Web Based_File_Exchange_ServerSpecification_Design_Document

[2]https://www.researchgate.net/publication/230639917_Design_of_Data_Masking_Architecture_and_Analysis_of_Data_Masking_Techniques_for_Testing

[3] KDnuggets , "Google Subpoena: Child Protection vs. Privacy," Accessed July 2006, from http://www.kdnuggets.com/polls/2006/google_subpoena.htm.

[4] Markoff, J. and Shane, S. 2006. "Government looks at ways to mine databases," New York Times (Late Edition, East Coast). February 25, 2006, p. C.1.

[5] Data Scrambling Issues A Net 2000 Ltd. White Paper.

[6]Sachin Lodha BY Data Privacy - TRDDC Silver Jubilee Commemoration Publication - SL Comments.doc

[7] F. You, C. Zhang, Y. Cao, H. Gong, C. Zhang, and J. Liao, ''Data maskingsystem based on ink technology,'' in Proc. 5th Int. Conf. Inf. Sci. ControlEng. (ICISCE), Jul. 2018

[8] T. Wei and V. Simko. (Mar. 15, 2022). R Package 'Corrplot': Visual-ization of a Correlation Matrix. [Online]. Available: https://github.com/taiyun/corrplot

[9] P. Cika and V. Clupek, ''Stress tester and network emulator inApache JMeter,'' in Proc. Photon. Electromagn. Res. Symp.-Spring(PIERS-Spring), Jun. 2019, pp. 3722–3726

[10] P. Probst, A. L. Boulesteix, and B. Bischl, ''Tunability: Importance ofhyperparameters of machine learning algorithms,'' J. Mach. Learn. Res.,vol. 20, p. 53, Feb. 2019