Xavier Institute of Engineering
Mahim, Mumbai 400016

Department of Computer Science and Engineering
(Internet of Things and Cyber Security Including Block Chain Technology)

CIPHER SHIELD

AAYUSH JADHAV
SAMEET JATHAN
SOHAM KADAM
ADITYA KADAV

Under the guidance of SUHAS SIR

OUTLINE

- Introduction
- Existing System
- Proposed System
- Hardware and Software Specification
- Result
- Conclusion
- Future Scope
- References

INTRODUCTION

Our File Encryption and Decryption mini project offers a secure process to protect your files, through advanced encryption & decryption techniques. During encryption, files are trams formed into unreadable formats and during decryption, files are transformed cipher text into readable format.

The primary aim of this project report is to delve into the features, functionality, and significance of Cipher Shield in the realm of data security. Cipher Shield is designed to offer an intuitive and secure solution for encrypting files of various formats, rendering them inaccessible to anyone lacking the proper decryption keys.

EXISTING SYSTEM

There are several websites and online tools that allow you to encrypt and decrypt files.

Websites :- Online-Convert.com

:- FileEncryptor.com

:- AxCrypt Online

:- Mega.nz

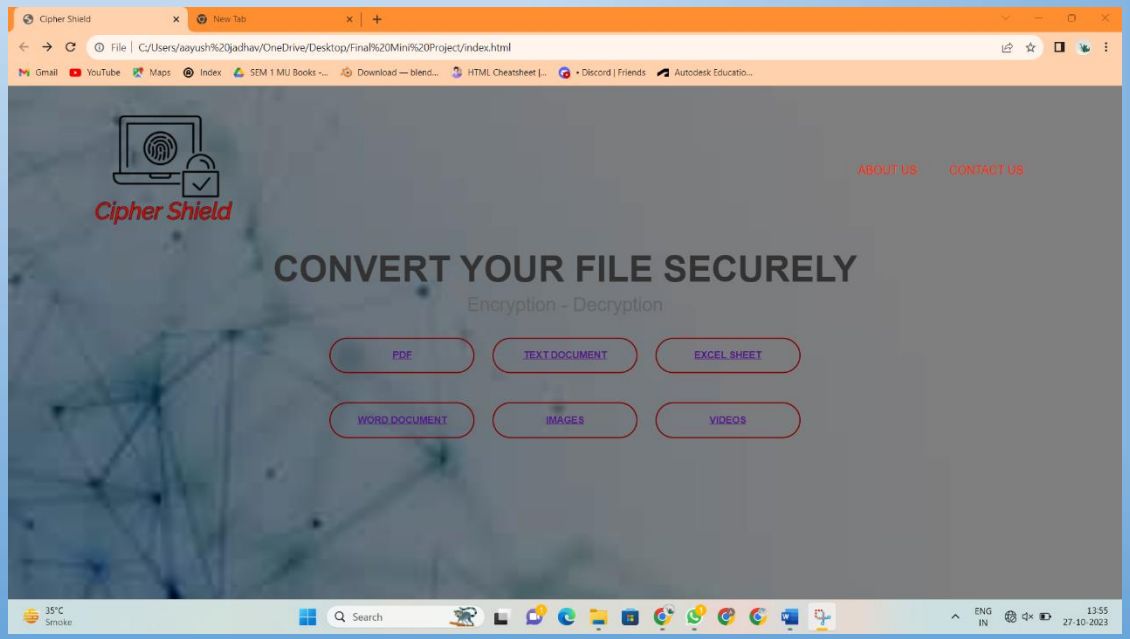
=>Drawbacks of Using Online Encryption Services:

- Security Concerns
- Lack of Control
- Limited Features
- File Size Limits
- Internet Connection

PROPOSED SYSTEM

Cipher shield provide one stop solution to convert all types of your file in one go whether it is plain text, pdf, word document, image, video, excel sheet.

Cipher Shield can Decrypt and Encrypt all types of your file in a seamless and easy way.



Home page of Cipher Shield

HARDWARE AND SOFTWARE SPECIFICATION

Hardware –

Cipher Shield is hosted on a dedicated server to ensure data security and performance. The server hardware includes:

- Intel i5 Processor
- 8 GB – 16 GB RAM
- 512 GB SSD Storage
- 10 MB/s Network

To enhance the security of the file encryption and decryption processes, Cipher Shield employs hardware security modules (HSMs). These HSMs provide cryptographic processing and key management.

User can use any type of PC or Laptop, the Cipher Shield's adaptive nature allows the website to run on any PC or Laptop needless of it's configuration.

HARDWARE AND SOFTWARE SPECIFICATION

Software –

The Frontend of the Cipher Shield website is made by using HTML programming language along with CSS programming language which is use to design the webpages of the Cipher Shield website.

The Backend of the Cipher Shield website is compiled using Java and JavaScript along with AES-GCM encryption algorithm which is use to encrypt the user's files

AES-GCM, which stands for Advanced Encryption Standard in Galois/Counter Mode, is a widely used encryption algorithm that provides both confidentiality and integrity for data. AES-GCM is a symmetric encryption algorithm that provides both encryption and authentication (integrity checking) of the data.

To encrypt the PDF and Text Documents we used the Web Crypto API to perform PDF and Text Document encryption, and it employs the "AES-GCM" (Advanced Encryption Standard in Galois/Counter Mode) encryption algorithm. Specifically, it utilizes the AES-GCM algorithm for encrypting the PDF file and Text document.

Here's a breakdown of the key parts in the code that involve AES-GCM encryption:

1. **Importing the Encryption Key:** The code generates a random encryption key of 128 bits (16 bytes) using crypto.getRandomValues(encryptionKey) and then imports this key using the Web Crypto API. The imported key is used for encryption.
2. **Encryption:** The code uses the imported AES-GCM key to encrypt the contents of the selected text file. This is done with the crypto.subtle.encrypt function, which uses the AES-GCM algorithm for encryption.

To decrypt the PDF and Text Document we used the the "AES-GCM" (Advanced Encryption Standard in Galois/Counter Mode) decryption algorithm.

Here's a breakdown of the key parts in the code that involve AES-GCM decryption:

1. **Importing the Decryption Key:** The code prompts the user to enter the encryption key, which should be a 32-character hexadecimal string (128 bits or 16 bytes). It then converts this hexadecimal string to a Uint8Array to represent the decryption key. The key is imported as a CryptoKey for decryption.
2. **Decryption:** The code uses the imported AES-GCM key to decrypt the contents of the selected encrypted file. This is done with the crypto.subtle.decrypt function, which uses the AES-GCM algorithm for decryption.

RESULT

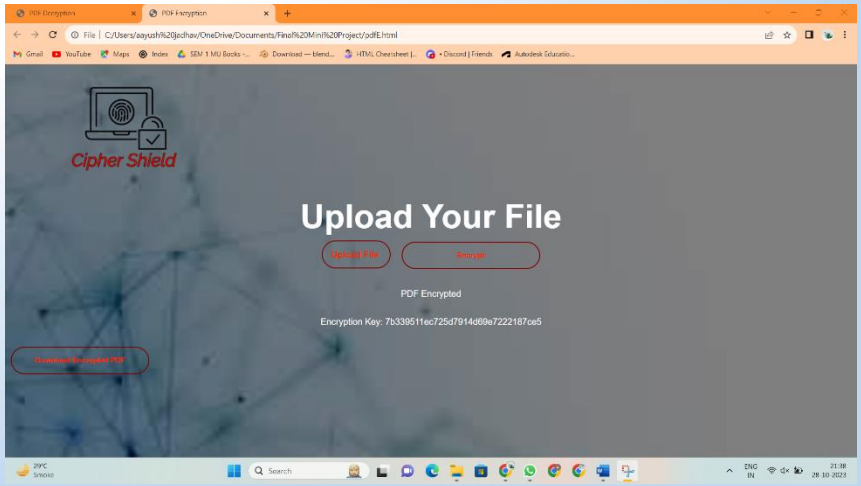
The Cipher Shield website encrypts and decrypts a user's file only and only by providing unique key which is generated by the website itself

If a user encrypts a file then the website will provide him with unique key and only by providing that key the user can decrypt the encrypted file thus safeguarding and protecting the users crucial information.

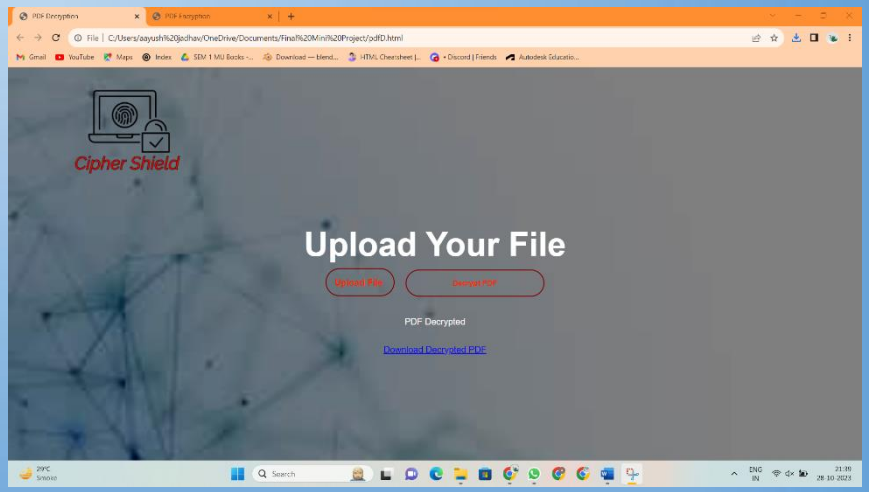
The user can encrypt and decrypt his Pdf and Text document using the website and can easily download the encrypted and decrypted file

The overall process is seamless and transparent thus safeguarding user's integrity and provides a overall user-friendly interface.

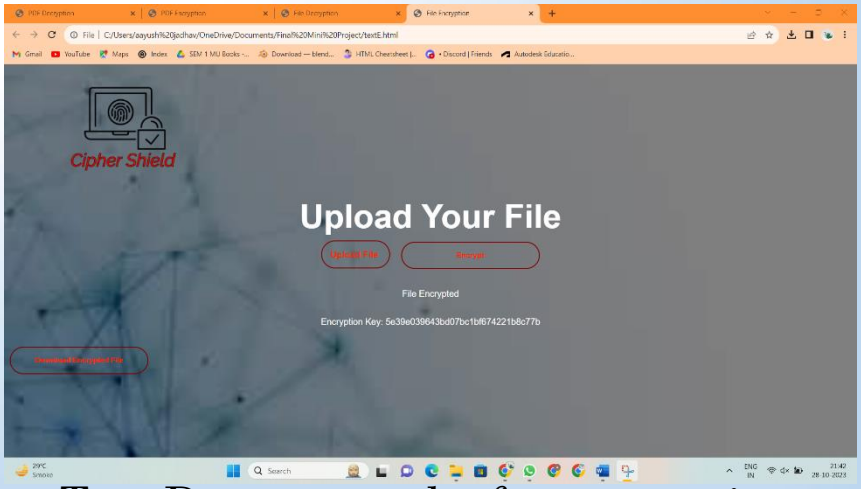
The results of the website are as follows :-



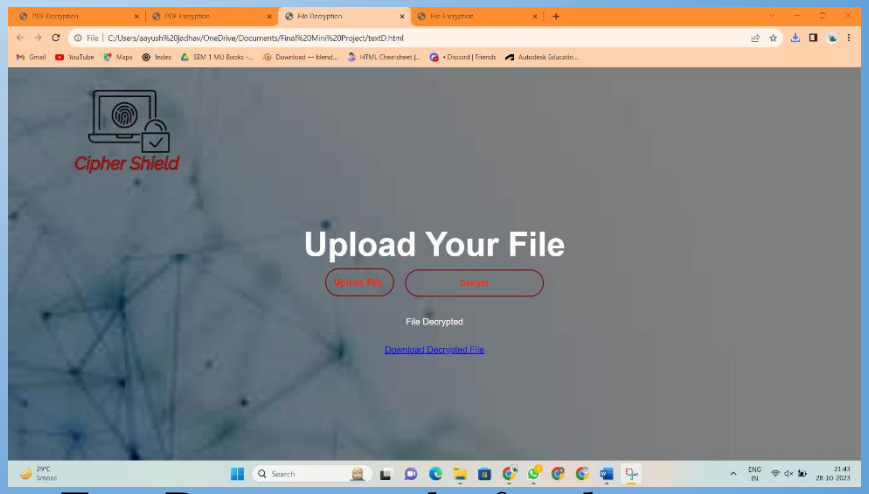
PDF tab after encrypting a pdf



PDF tab after decrypting a pdf



Text Document tab after encrypting a text file



Text Document tab after decrypting a text file

CONCLUSION

When it comes to encryption and decryption, it's important to understand the difference between the two.

Encryption is the process of transforming readable data into an unreadable format, while decryption is the process of transforming unreadable data into readable format.

Encryption is used to protect data from unauthorized access, while Decryption is used to restore data to its original format. Encryption and Decryption are essential for ensuring the security of data.

The File Encryption & Decryption mini-project conclude with successful output, providing user a reliable & user-friendly system to convert plain text into cipher text and vice-versa.

FUTURE SCOPE

The future scope of Cipher Shiled (Encryption and Decryption) mini project includes improving –

- Security Solutions
- Integrating with Cloud
- Mobile apps
- Enhancing IoT security
- Ensuring cross-platform compatibility
- User-friendly Interfaces
- Robust key management
- Compliance with Data Regulations
- Biometric Authentication

REFERENCES

- "Cryptography and Network Security" by William Stallings (book)
- Cryptography tutorials and articles on websites like GeeksforGeeks.
- Open-source encryption and decryption projects on platforms like GitHub for code examples and inspiration.
- YouTube videos on JavaScript code for File Encryption and Decryption.
- Various websites like Skiff, Stack Overflow, GitHub and Tutorialzine to understand the working of JavaScript code on File Encryption and Decryption.
- Logomaker to make various logos used in the Cipher Shield website.
- Extensive use of ChatGPT for various tech and literary supports (codes, information, instructions and reports)

THANK YOU