International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

CipherShare: CUSTOM KEY ENCRYPTION/DECRYPTION AND MESSAGING SYSTEM

[1]Abhinav Babu, [2]Abhinav Shaji, [3]Abhishek K, [4]Anirudh Babu, [5]Soumya T

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor (CSE)
Computer Science and Engineering Department,
Nehru College of Engineering and Research Centre (NCERC), Thrissur, India

---

Abstract - In an age where data security is crucial, the need for robust encryption systems has become increasingly necessary. This paper presents CipherShare, a Custom Key Encryption/Decryption and Messaging System, designed to provide enhanced security and flexibility for secure communication. The system employs a unique approach by allowing users to create custom encryption keys tailored to their specific requirements, ensuring a high level of data protection. The system uses Advanced Encryption Standard (AES) algorithm, due to which the proposed system offers several advantages over traditional encryption systems. Firstly, its custom key approach provides a higher level of security by reducing the risk of brute force attacks. Secondly, the system's flexibility allows users to adapt encryption keys according to their changing security needs. Thirdly, it is platform-independent, making it compatible with a wide range of devices and applications.

***Key Words*:** Custom Key, Encryption, Decryption, Security, Communication, Confidentiality.

1. INTRODUCTION

In today's digital world, the security of communication and data exchange has become a paramount concern. With the increasing reliance on digital platforms for sensitive information sharing, there is a growing need for robust encryption systems that can safeguard privacy and confidentiality. CipherShare emerges as a solution to this pressing demand, offering a custom key encryption/decryption and messaging system that ensures secure communication channels. At its core, CipherShare addresses the vulnerabilities inherent in conventional messaging systems by implementing customizable encryption techniques. By allowing users to generate their encryption keys, CipherShare provides an added layer of security, making it significantly harder for unauthorized parties to intercept and decipher messages.

One of the key features of CipherShare is its custom key encryption/decryption mechanism. Unlike traditional encryption methods, where a single algorithm or key is used for all communications, CipherShare empowers users to create their unique encryption keys. This approach enhances security by minimizing the risk of brute force attacks or key compromise, as each communication channel operates with its distinct encryption parameters. Moreover, CipherShare's messaging system integrates seamlessly with its encryption functionality, providing users with a secure platform for exchanging sensitive information. Whether it's text messages or images, CipherShare ensures that data remains encrypted throughout transmission, thereby safeguarding confidentiality. The versatility of CipherShare extends beyond individual users to encompass organizations and enterprises. CipherShare enables secure communication while sharing sensitive data within a closed environment. This capability is especially crucial for businesses operating in industries where data privacy and confidentiality are paramount, such as healthcare, finance, and legal sectors. Furthermore, CipherShare prioritizes user privacy by employing end-to-end encryption, ensuring that only the intended recipients can access message contents. By encrypting data at the sender's device and decrypting it at the recipient's device, CipherShare minimizes the risk of interception or eavesdropping by malicious third parties.

CipherShare's custom key encryption/decryption and messaging system represent a significant advancement in digital security. By empowering users with control over their encryption keys and ensuring end-to-end encryption for all communications, CipherShare provides a robust solution for protecting sensitive information in an increasingly interconnected world.

2. LITERATURE REVIEW

[1] The implementation of Intelligent Custom Dictionary Based Encryption/Decryption Scheme stores the new words and patterns used by the user in a database that is located in the System of the user itself , hence not sending any vulnerable information over the network. Even if a hacker tends to get hold of the data that is being transmitted over the network all he gets is encrypted data, which is useless without the custom dictionary that is used by the user for the encryption . The same dictionary is available with the recipient who then uses it to decrypt the sent string . The beauty of this security scheme is the custom dictionary which is enhanced and enriched in accordance to the users vocabulary. The scheme develops the encryption codes of new words on the go without any interference from the user hence providing a seamless way to encrypt and decrypt data. User can can use multiple dictionaries while communicating with different people whereas all the other users will only need to maintain only one dictionary that is specific to their conversation.

[2] Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem proposed two new cryptosystems, one of them called the hybrid cryptosystem using the Playfair cipher with the RSA square. The second is a hybrid cryptosystem using the Playfair with the RSA square and Chinese remainder theorem(RSASQ-CRT). These systems used two layers of encryption: First, encrypt with the Playfair cipher to obtain the first ciphertext. Second, it used RSASQ-CRT to obtain the final ciphertext. The hybrid cryptosystem Playfair with RSASQ provides high security and more complexity against hackers to find the private keys since it does not use the public key directly.

[3] A Cryptosystem Based On Vigenère Cipher By Using Multilevel Encryption Scheme is inspired by the Caesar Cipher in that it uses a "polyalphabetic substitution matrix" that combines two or more alphabetic tables. In this paper, a new method is proposed where an equivalent fixed length of plain text and a key is selected and applied in Vigenère table to get a new cipher text. This cipher text is act as a new key. With this new key, the cipher text is encrypted once again and sends the final cipher text to the receiver. Finally the receiver does the decryption in reverse way. This secured information can be transmitted once the users authenticate themselves by using Diffie Hellman Key Exchange Protocol. This proposed method is implemented in virtual private network (VPN) to show its efficiency in terms of authorization and secure data transmission.

[4] Sampurna Suraksha: Unconditionally Secure And Authenticated One Time Pad Cryptosystem has been proven to be actually unbreakable with the condition that the key is truly random, never reused, and is kept secret. If properly used, the system provides a formidable encryption and it will be practically impossible for any sniffer to decrypt or break one-time pad encrypted message by any type of cryptanalysis, without the proper key or even with infinite computational power. Since all plaintexts are equally probable in one time pad, it creates a strong notion of cryptanalytic difficulty. This paper explains how to use one-time pads, how to set up secure one-time pad communications, how to deal with its various security issues and also addresses the integration of other security techniques with one time pad, like a biometric finger print scanner for authentication.

[5] Hybrid Cryptosystem Based On Vigenère Cipher And Columnar Transposition Cipher performs its encryption by encrypting the plaintext using columnar transposition cipher and further using the ciphertext to encrypt the plaintext again using Vigenère cipher. It is implemented using java programming. This paper capitalized on the strengths and solved the weakness in the Vigenère cipher by using the strength of the columnar transposition. Here, the key is used to encrypt the plaintext using transposition cipher and then the resulting ciphertext is used as a key to encrypt the plaintext using Vigenère cipher.

[6] In Cryptographic Encryption Based On Rail-Fence Permutation, analog of Permutation and Rail Fence Cipher is used to develop a hybrid algorithm for Encryption and decryption. The Rail-fence permutation cipher is a transposition cipher where the plaintext is written in a zigzag pattern across several "rails" of an imaginary fence. Then, the ciphertext is generated by reading off the letters in the order of the rails. To decrypt, the matrix is reconstructed with the same key, and the original plaintext is obtained by reading off the characters row-wise.

[7] In Modified Playfair cryptosystem for improved data security, a modified Playfair (MPF) cryptosystem that is capable of handling different block sizes with high diffusion and confusion properties is developed. cryptanalysis of the developed cryptosystem was carried out and the results show that the MPF cryptosystem is resistant to known plaintext attack, chosen-plaintext attack, chosen ciphertext attack, frequency analysis attack, autocorrelation attack, differential cryptanalysis attacks, entropy attacks, brute force attack, and can handle variable block sizes.

[8] In A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted, the authors modify the Caesar cipher method that produces ciphertext that can be read. With the ciphertext that can be read, then cryptanalysis not suspicious of the ciphertext. Caesar cipher modification is done by replacing the alphabet into two parts, the vocals were replaced with the alphabet vocal too, and the consonant alphabet was replaced with a consonantal alphabet. However, there are some alphabet consonants are not replaced, this is because the frequency of the alphabet is rarely used in an Indonesian text. From the test results obtained ciphertext that can be read. With the ciphertext that can be read, then the cryptanalyst not suspicious of the message so that the cryptanalyst does not attempt to solve the ciphertext.

3. PROBLEM STATEMENT

In today's digital landscape, the security of sensitive communication and data exchange remains a critical concern. Traditional messaging systems often lack sufficient measures, leaving communications vulnerable to interception and compromise by malicious actors. Existing encryption solutions may not provide users with the level of control and customization needed to adequately protect their data. Therefore, there is a pressing need for a secure messaging platform that offers robust encryption techniques, customizable encryption keys, and seamless integration with messaging services to ensure the privacy and confidentiality of digital communications. The objective of CipherShare, a custom key encryption/decryption and messaging system, is to address these challenges and provide users with a secure means of communication in an increasingly interconnected world.

4. PROPOSED SYSTEM

The system aims to provide a secure and safe environment for effective data transfer, enhance user experience and optimize computational resources. The system is made more secure and preserves the integrity of data using AES algorithm, which is optimized for speed and can encrypt and decrypt data quickly, even for large amounts of data. User authentication is implemented within the system, as a custom key is required. The system also supports visual (image) data transfer with binary code encryption. A messaging system is implemented to provide a secure communication channel.

This paper presents a detailed overview of CipherShare: Custom Key Encryption/Decryption And Messaging System outlining its six key modules. They are given below:

1. Registration Module And Account Management Module: This module helps the students/staff to get registered from anywhere, if internet is present. After successful registration, the user can access the features of the proposed system.

2. User Management Module: This module handles user authentication, authorization, and management within the

system. It ensures that only authorized users can access the system and perform encryption, decryption, and messaging operations.

3. Encryption Module: The encryption module takes plaintext messages and encrypts them using the custom encryption key. It employs Advanced Encryption Standard (AES), an advanced encryption algorithm to ensure that the data is securely transformed into ciphertext, making it unreadable to unauthorized parties.

4. Decryption Module: The decryption module reverses the encryption process, taking ciphertext messages and decrypting them using the corresponding custom encryption key. This module ensures that only authorized users with the correct decryption key can access the original plaintext messages.

5. Messaging Module: The messaging module facilitates secure communication between users by integrating the encryption and decryption functionalities seamlessly. It allows users to exchange encrypted messages, ensuring confidentiality, integrity and authenticity of the messages.

6. Logging and Auditing Module: The logging and auditing module records all system activities, including number of times logged in, total messages sent and received.

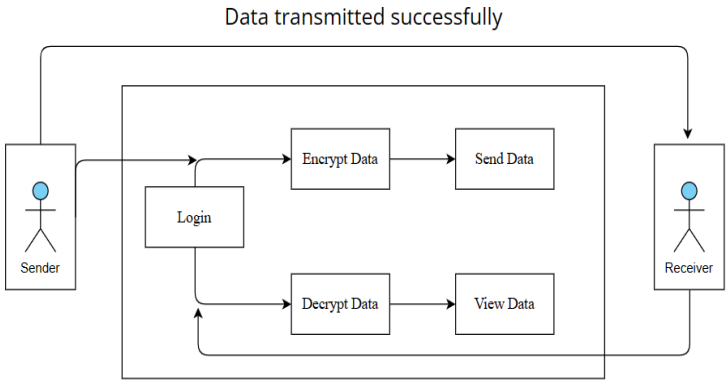

Fig 1: System Architecture

5. RESULTS AND DISCUSSION

The users interact with the system through a responsive web page developed using full stack development. The interface offers six primary options: Register, Log in, Encrypt data, Decrypt data,View Message and Send Message. The Register option allows new users to access the system with a username and a password. After registration, the users have to log in with their respective username and password which is stored in a database. Invalid users or users whose credentials have not been updated to the database will not be able to log in.

After successful log in, the user will be able to interact with the main page which has the menu for a dashboard, Image Encryption/Decryption, Text encryption/ Decryption, View Message and Send Message.

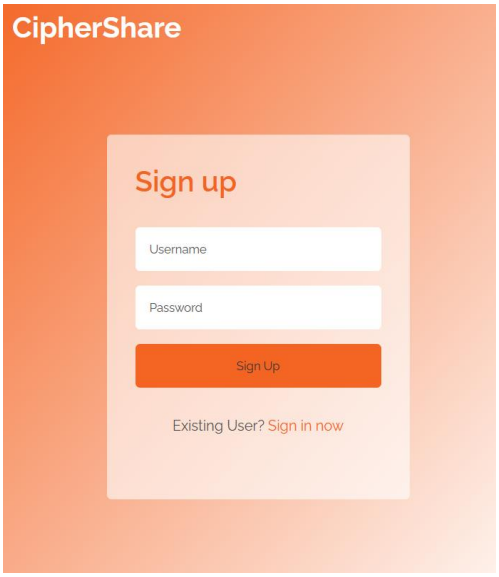

Fig 2: Sign Up Page

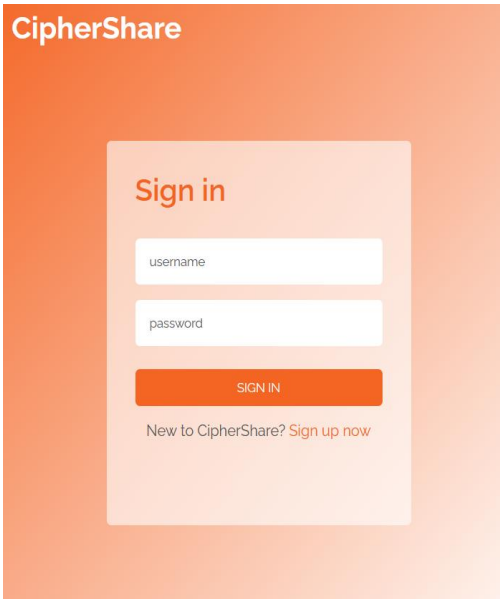

Fig 3: Sign In Page

In the dashboard section, users will be to see a history of their activities. They will be able to see the number of times they have logged in to the system,the total number of messages they have sent as well as the total number of messages they have received. This helps in auditing the user account to check for any unauthorized user access.

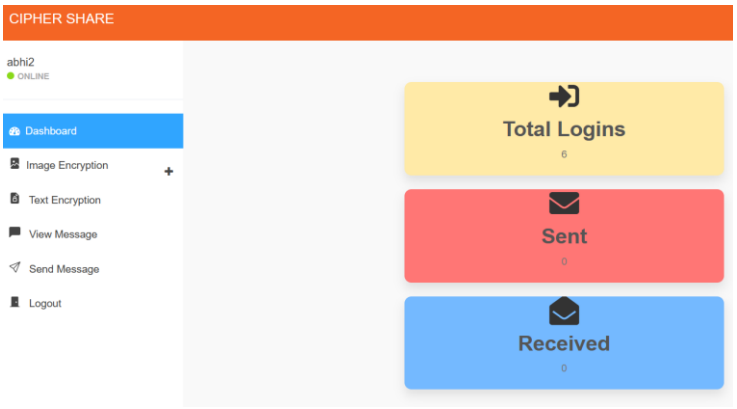

Fig 4: Dashboard Page

In the Encrypt Image section, the user can upload their image and convert it to binary code. The resultant binary code can be copied to the clipboard to be sent to other users.

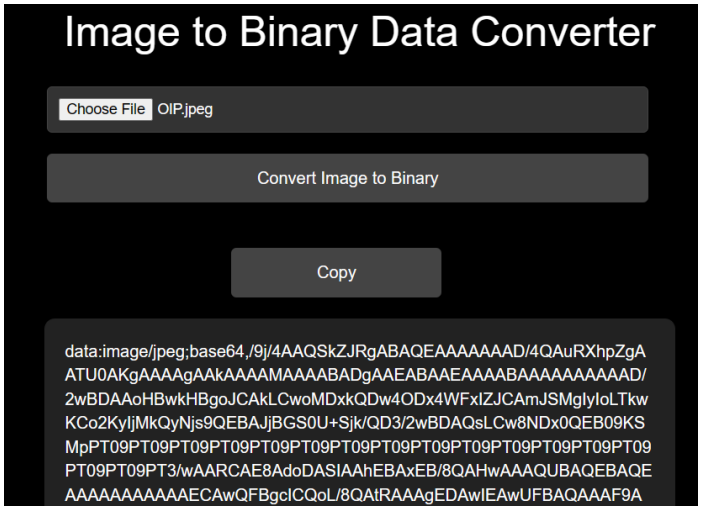

Fig 5: Encrypt Image Page

In the Decrypt Image section, the user can copy in binary code and obtain the decrypted image. The image can then be downloaded to be stored in the system.

Fig 6: Decrypt Image Page

The Text Encryption/Decryption section can convert the textual data of the user to a cipher or vice versa, using the implementation of Advanced Encryption Standard (AES) algorithm.

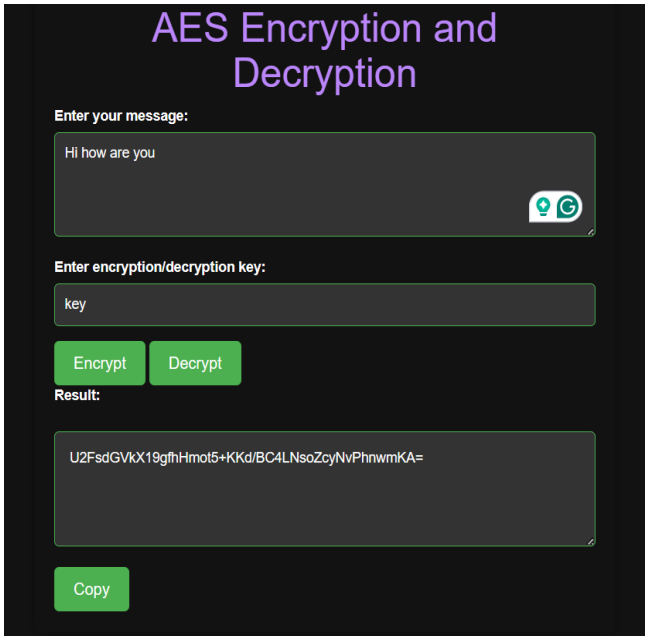

Fig 7.1: Text Encryption/Decryption Page

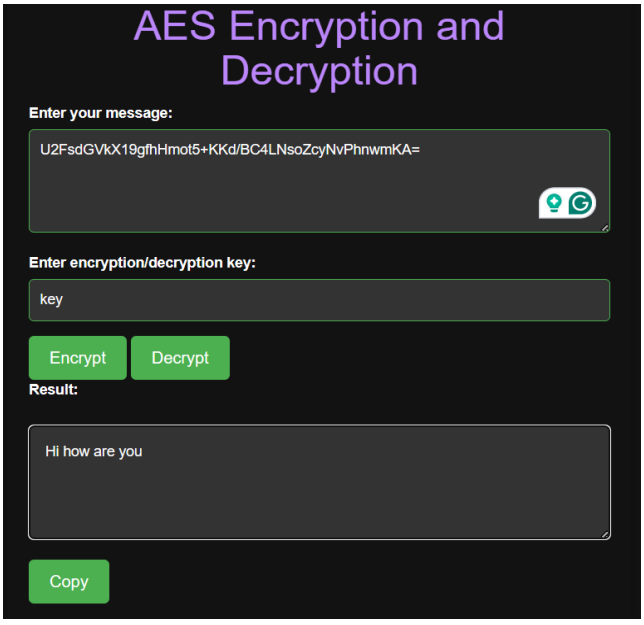

Fig 7.2: Text Encryption/Decryption Page

The Send Message section allows the users to send encrypted messages to different users, who are identified by their username.In the figure, the encrypted message was sent by user “abhi3” to “abhi2”.

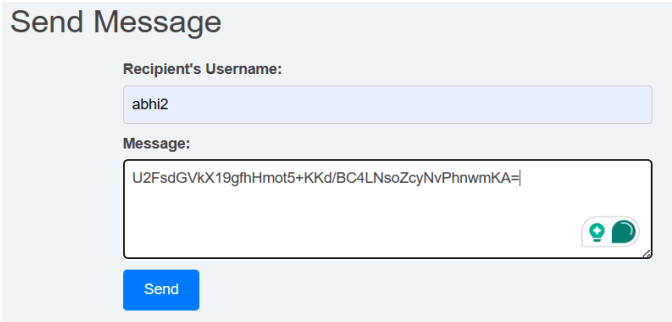

Fig 8: Send Message Page

The View Message section allows the users to view encrypted messages sent to them by different users .In the figure, the encrypted message was received by user “abhi2” from “abhi3”.

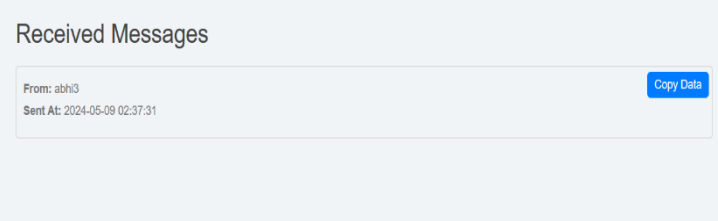

Fig 9: View Message Page

6. CONCLUSION

This system empowers users with control over their encryption keys and ensures end-to-end encryption for all communications, which makes it different from the traditional system of information sharing. The proposed system ensures that individuals and organizations can adopt secure communication practices without extensive technical expertise, thereby promoting widespread adoption of the platform. The platform's objectives of enhanced security, customizability, end-to-end encryption, and user-friendliness have been successfully achieved, making it a valuable tool for individuals and organizations seeking to safeguard their privacy and confidentiality. By integrating this system in areas of online communication, storage of sensitive data, online transactions, authorization and access control, users can ensure efficient and secure data transmission while accessing,sending and receiving it.

REFERENCES

[1] Intelligent Custom Dictionary Based Encryption/Decryption Scheme , Abhineet Anand , Ankur Dumka, Ravi Tomar and Ankit Khare, 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015), Dehradun, India, 4-5 September 2015

[2] Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem, Saja Mohammed Suhael, Zaynab Anwer Ahmed, Abir Jaafer Hussain, Baghdad Science Journal 2024, 21(1): 151-160 (P-ISSN: 2078-8665)

[3] A Cryptosystem Based On Vigenère Cipher By Using Multilevel Encryption Scheme, Sanjeev Kumar Mandal, A.R Deepti, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (4) , 2016, 2096-2099 (ISSN: 0975-9646)

[4] Sampurna Suraksha: Unconditionally Secure And Authenticated One Time Pad Cryptosystem, Rakesh Shukla, Hari Om Prakash, R.Phani Bhushan, S. Venkataraman, Geeta Varadan, ADRIN, Department of Space, Govt. of India, Secunderabad, Andhra Pradesh, 2013 International Conference on Machine Intelligence Research and Advancement

[5] A Hybrid Cryptosystem Based On Vigenère Cipher And Columnar Transposition Cipher, Quist-Aphetsi Kester, MIEEE, Lecturer Faculty of Informatics, Ghana Technology University College, International Journal of Advanced Technology & Engineering Research (IJATER) Volume 3, Issue 1, Jan. 2013 (ISSN No: 2250-3536)

[6] Cryptographic Encryption Based On Rail-Fence Permutation Cipher, Michael N. John, Ogoegbulem Ozioma, Udoaka Otobong. G, Boniface O. Nwala, Obi Perpetua Ngozi, International Journal of Mathematics Vol (06) Issue (11) (2023) (P-ISSN: 2795- 3274)

[7] Modified Playfair cryptosystem for improved data security, Esau Taiwo Oladipupo, Oluwakemi Christiana Abikoye, Institute of Advanced Engineering & Science Journal, Vol. 3, No. 1, March 2022, pp. 51~64 ISSN: 2722- 3221

[8] A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted, Benni Purnama, Hetty Rohayani.AH, International Conference on Computer Science and Computational Intelligence (ICCSCI 2015), Procedia Computer Science 59 (2015) 195 – 204