



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

Design and Analysis of Cryptographic Technique

Himashree R, Dr Sanjay K S

Student, Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India

HOD, Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: People are sharing more and more sensitive information online these days, and honestly, that's got a lot of folks worried about data security. It makes sense—no one wants their private stuff floating around for strangers to see. The best way to handle this is by using cryptography. Basically, you scramble the data, send it over the internet, and then unscramble it on the other side. This whole process goes way back, actually. People have been coming up with ways to hide messages for centuries. At its core, cryptography is all about making sure your data gets to the right person without anyone else snooping. Whether it's a secret message or just personal info, you want it hidden so only someone who knows how to decode it can read it.

KEYWORDS: Data security, encryption and decryption, RSA algorithm, AES encryption, hybrid cryptography, plaintext encryption, data integrity.

I. INTRODUCTION

In today's digital world—where technologies like IoT, 5G, and cloud computing dominate—cybersecurity risks have grown rapidly. As more systems become connected, the number of areas vulnerable to cyberattacks continues to expand. Traditional cryptographic techniques still form the backbone of secure communication, but they are increasingly challenged by advanced attack strategies, rising computational power, and the emerging threat of quantum computing. Because of this, everyday digital interactions—whether personal messages, business data exchanges, or government communications—are now more exposed to risks such as eavesdropping, tampering, and misuse. On the implementation side, the backend is developed using the **Flask** framework in Python. It supports secure authentication using JWT and bcrypt password hashing, provides encryption and decryption APIs, and enables safe message handling. All user information, keys, messages, threads, and audit logs are stored in **MongoDB Atlas**, with indexing applied to maintain high performance.

II. LITERATURE SURVEY

[1] Anuja Priyam." Extended Vicerent using double Transposition Cipher with One Time Pad Cipher." Intl J Engg Sci Adv Research(2015). The study presents the enhances text security through a multi-layered encryption process. The message is first encrypted using a One Time Pad (OTP) cipher and then rearranged with a transposition cipher. After adding logical bits, the data is encrypted again with a second OTP key and undergoes another transposition. This layered approach creates a highly secure cipher-text, and the original message is recovered by reversing these steps.

[2] Quist-Aphetsi Kester, "A cryptosystem based on Vicerent cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December (2012). This approach improves the Vigenere cipher using a dynamic key in encryption Rather than a single, constant key, each new key is obtained by transformation of the prior key using a function. This constant variation of the key makes the ciphertext significantly more resistant to frequency analysis attacks. The algorithm's effectiveness was demonstrated using a Java program and validated through cryptanalysis.

[3] O.E. Omolara. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication." Computer Engineering and Intelligent Systems ISSN 2222- 1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.5, (2014). This research represents the technique strengthens encryption by combining several methods. First, a random number is used as the shift for a Caesar cipher to modify a separate lettered key. This modified key is then used to encrypt the plain text with a Vigenere cipher. Finally, the resulting cipher-text undergoes a sequential binary XOR operation, starting with the random number key. This multi-step process produces a complex final ciphertext composed of letters, numbers, and symbols, making it more robust against frequency analysis.

[4] Garg, Saloni, Sonam Khera, Archana Aggarwal, and P. G. Scholar."Extended Vigenere Cipher with Stream Cipher." International Journal of Engineering Science and Computing (IJESC) 6, no. 5 (2016). Saloni Garg proposed to add stream cipher to vigenere cipher to enhance security. She also proposed to include all lowercase, numeric, and special characters on the cipher in order to make it flexible and capable to encrypt any kind of data, specifically not just uppercase letters. Stream ciphers work by one bit at a time encryption, or tweaking a bit of plaintext with a bit of keystream.

Proposed Methodology

The User Interface (UI) acts as the primary bridge between the user and the system. It provides a clean graphical environment where users can easily interact with the application—whether by entering data, selecting options, or navigating through different features. A well-designed UI ensures that users do not need technical expertise to operate the system; instead, they can communicate with it smoothly and intuitively. In this project, the interface is kept simple, responsive, and user-friendly, allowing users to perform tasks without confusion or unnecessary complexity. At the core of the architecture lies the Application Layer, which serves as the central processing unit of the system. While the UI handles the visual interaction, the Application Layer interprets every user action, processes it, and coordinates the appropriate system responses. This layer acts like the “brain” of the application: it receives inputs from the UI, triggers the required logic, communicates with backend services or databases, and returns meaningful outputs back to the user. It ensures that all operations—authentication, data handling, encryption, and message processing—run efficiently and consistently.

Proposed Model Diagram

The proposed model introduces an intelligent and secure communication framework that integrates hybrid cryptography with machine learning-driven analysis. At the core of the system is a multi-layer encryption pipeline where each message is sequentially processed through classical ciphers such as Caesar and Vigenère, followed by a strong modern cipher like AES. This layered approach ensures that even if one level is compromised, the remaining stages continue to safeguard the message. The model also incorporates a machine learning component that analyses communication patterns, detects anomalies, and predicts potential security risks in real time, thereby strengthening protection against emerging threats. The architecture begins with a user interface where messages are composed and submitted. These inputs are transferred to the application layer, which manages key generation, encryption operations, and communication flow. Encrypted data is then securely stored or transmitted over the network.

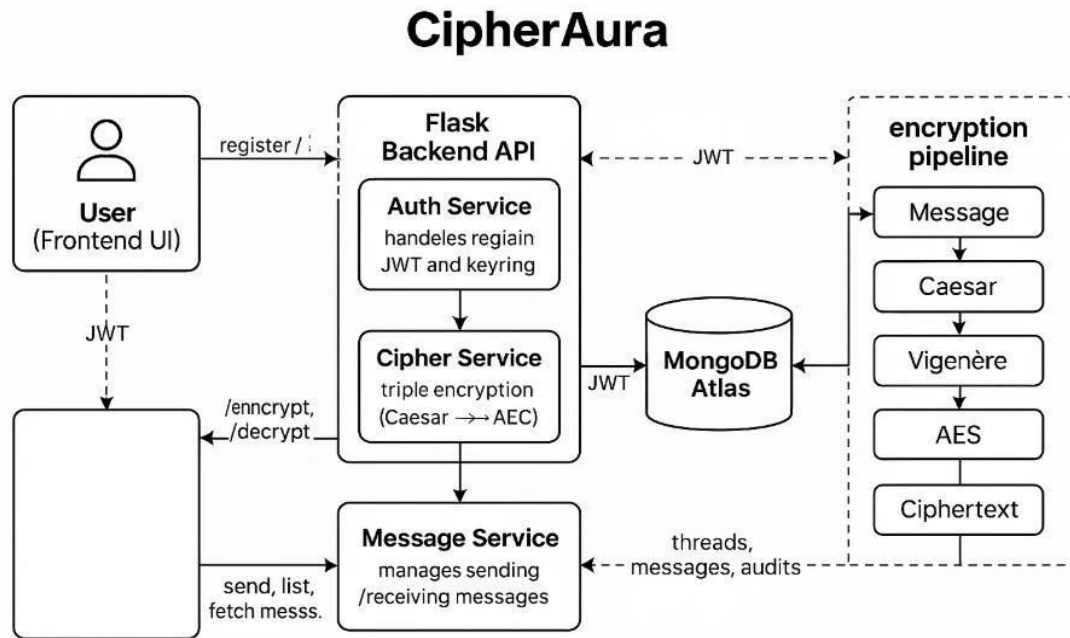


Figure 2.1.1: Block Diagram of Proposed System

Mathematical Formula

1) Caesar cipher (single shift)

Encryption (letter indices 0..25):

$$C = (P + k) \bmod 26$$

where PPP is the plaintext letter index, kkk is the shift key, and CCC is the ciphertext letter index.

Decryption: $P = (C - k) \bmod 26$; $P = (C - k) \bmod 26$

2) Vigenère cipher (key repeated over message)

For position iii:

$$C_i = (P_i + K_i) \bmod 26$$

where PiP_i is the plaintext letter index, KiK_i is the key letter index (key repeated or derived), and CiC_i is ciphertext.

Decryption: $P_i = (C_i - K_i) \bmod 26$

3) AES (block cipher, abstract form)

AES is best expressed as a black-box block function with keyed rounds:

$$C = \text{AESK}(P) \quad C = \text{AES}\{\text{K}\}(P) \quad C = \text{AESK}(P) \text{ and decryption}$$

$$P = \text{AES}^{-1}_K(C).$$

If you want the round-level view (128-bit block):

$$\text{Stater}+1 = \text{MixColumns}(\text{ShiftRows}(\text{SubBytes}(\text{Stater}))) \oplus \text{RoundKey}_r[\text{text}\{\text{State}\}_r + 1]$$

With the first round starting from $\text{State0} = P \oplus \text{RoundKey0}$, $\text{text}\{\text{State}\}_0 = P \oplus \text{RoundKey0}$. (No need to expand further unless you want S-box math.)

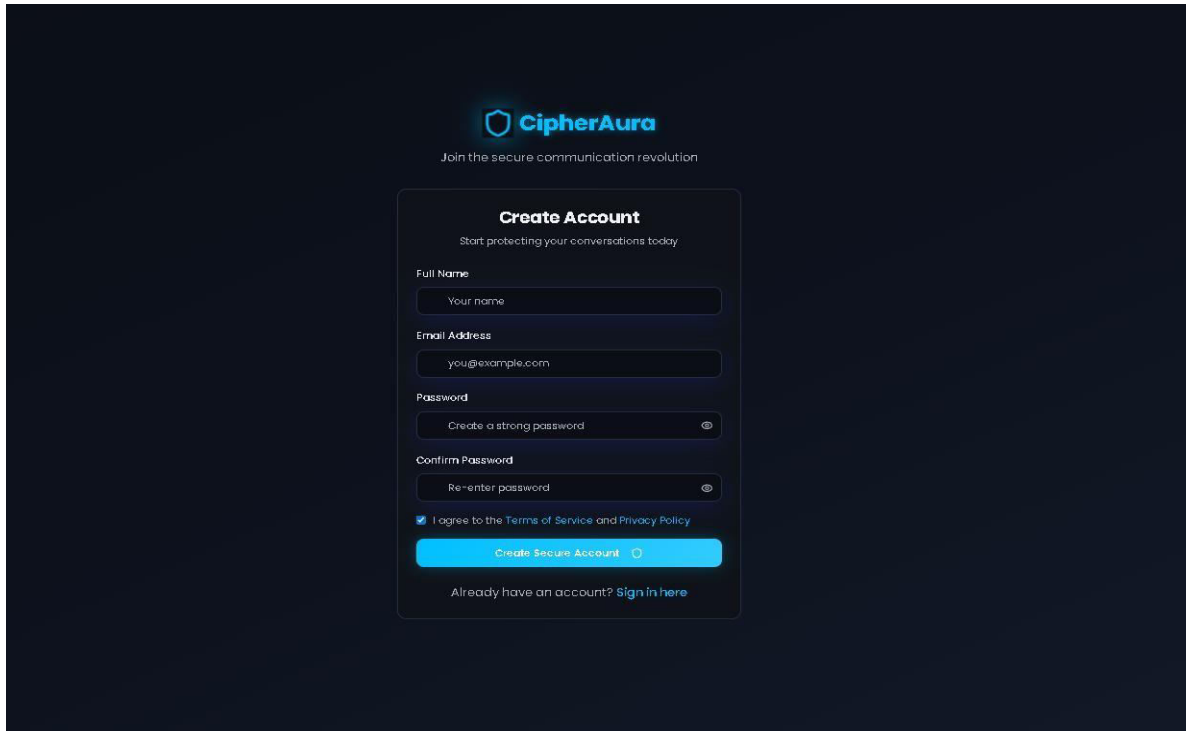
4) Hybrid pipeline (composition of the three stages)

Write the pipeline as nested functions so it's clear how data flows:

$$C = \text{AESK3}(\text{VigK2}(\text{Caesark1}(P))).$$

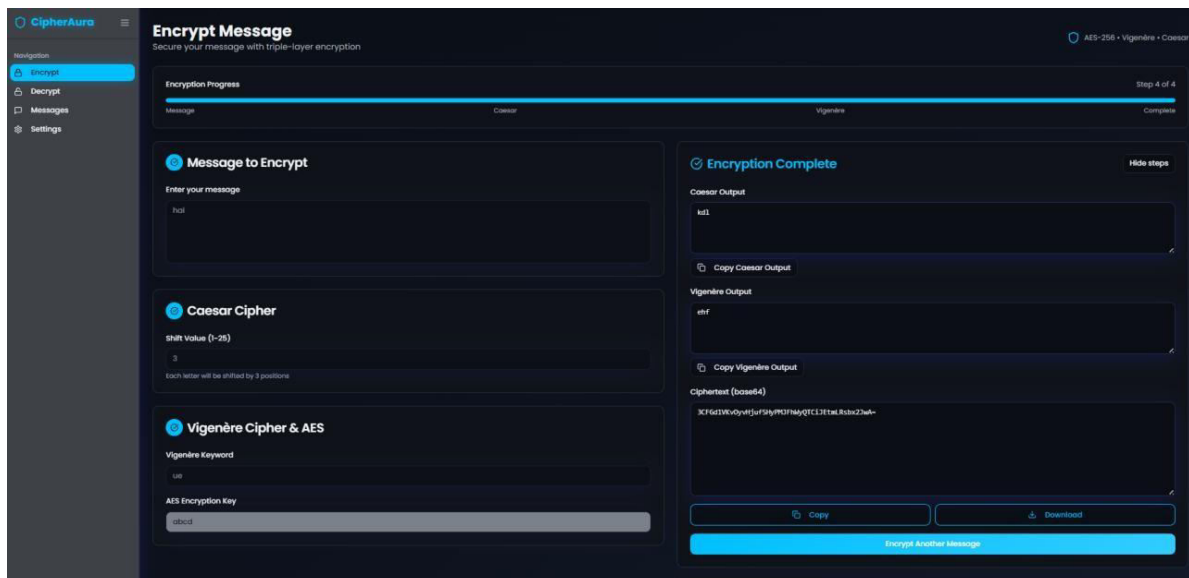
Decryption reverses the order:

$$P = \text{Caesar}_{k_1}^{-1}(\text{Vig}_{K_2}^{-1}(\text{AES}_{K_3}^{-1}(C))) \quad = \quad \text{Caesar}_{k_1}^{-1}(\text{Vig}_{K_2}^{-1}(\text{AES}_{K_3}^{-1}(C)))$$



The login page features a dark blue background with the CipherAura logo at the top center. Below the logo is a 'Create Account' form with the following fields: Full Name, Email Address, Password, and Confirm Password. There is a checkbox for 'I agree to the Terms of Service and Privacy Policy' and a 'Create Secure Account' button. A link for 'Already have an account? Sign in here' is located at the bottom of the form.

Fig 1 Login Page



The encryption page is titled 'Encrypt Message' and shows a progress bar with four steps: Message, Caesar, Vigenere, and Complete. The 'Message' step is active, showing a text input field with the message 'hdi'. The 'Caesar Cipher' step shows a shift value of 3. The 'Vigenere Cipher & AES' step shows a keyword 'cat' and an AES encryption key 'abcd'. The 'Encryption Complete' step shows the Caesar output 'kdl', the Vigenere output 'ehf', and the ciphertext 'XFGt1Wvdyv4tJuf5t4pRQF1wqQEC13t1w.Bdsu2w4n'. There are buttons for 'Copy', 'Download', and 'Encrypt Another Message'.

Fig 2 Encryption on Page

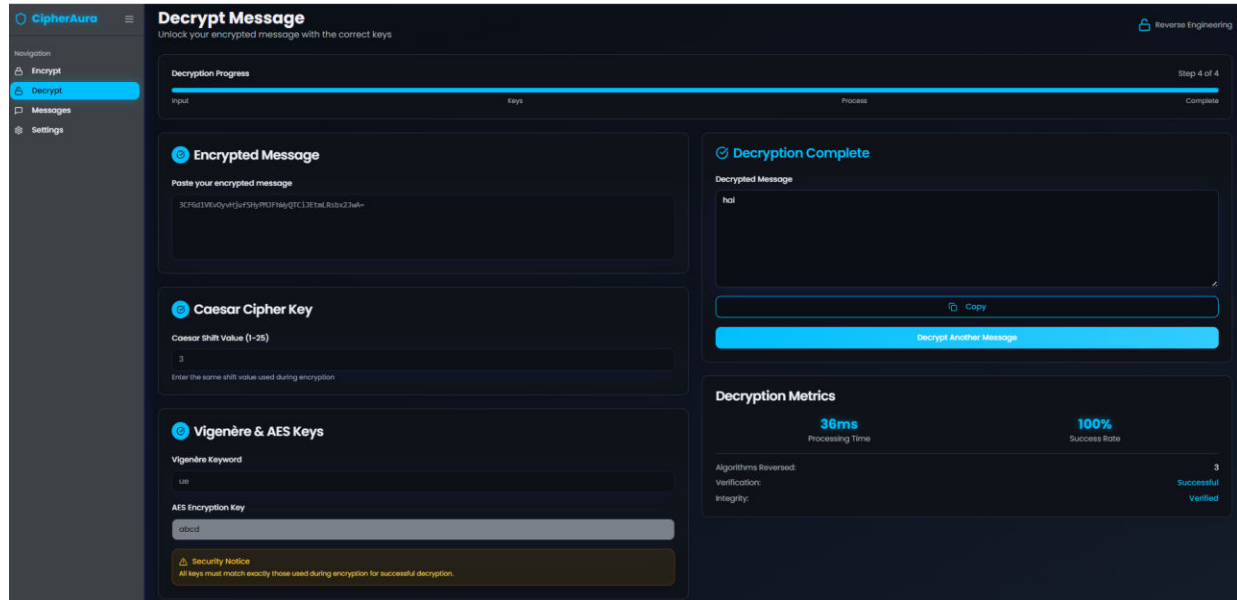


Fig 3 Decryption on page

III. CONCLUSION

The Cipher Aura Hybrid Encryption System addresses the increasingly difficult problem of ensuring the security in the digital communication by taking advantage of a structured cryptography. It incorporates Caesar Cipher, Vigenere cipher and AES encryption along a single pipeline. Even when either of the encryption layers is compromised through this design Confidential information is secured and this combination technique increases the privacy , integrity as well as brute force and advanced attacks. In addition to the encryption pipeline, the system is securely user authenticated, manages keys, logs audit and thread messages within a well -d enveloped web based platform. It is being backed by Flask and MongoDB Atlas that offer a high degree of scalability and reliability. The frontend is user friendly and is built in React and Tailwind CSS. Together these factors form a viable and workable form of safe communication.

IV. FUTURE ENHANCEMENT

Cipher Aura Hybrid Encryption System is a sturdy and secure polishing system that takes a cross between Caesar, Vigenere and AES codes. Nevertheless, it can be enhanced to be friendlier to users, scalable enough, and resilience. Possible enhancements include providing an asymmetric cryptography mechanism such as RSA or Elliptic Curve Cryptography (ECC) to be introduced. This would enable that secure key exchange is possible without handing over pre-s hared keys. Such modifications will render the system more realistic to be used in actual -l ife communications networks with distributed systems. In addition, incorporation of quantum -r esistant cryptography may safeguard the system against impending attacks caused by quantum computers; this may involve introducing lattice -based cryptography or hash -based cryptography. Besides the upgrade in algorithm, the site might also have file and multimedia encryption. This would ensure that not only text messages can be secured but also images, documents and audio/video communication. The potential of Cipher Aura being used as an end -to- end communication tool, features such as group messaging, secure file transfer and end -t o- end encryption of chat, could make Cipher Aura a household name.

REFERENCES

- [1] Anuja Priyam." Extended Vigenère using double Transposition Cipher with One Time Pad Cipher." Intl J Engg Sci Adv Research 2015 June; 1(2):62-65.
- [2] Quist -A phetsi Kester, "A cryptosystem based on Vigenère cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012.
- [3] O.E. Omolara. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for SecureData Communication." Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222- 2863 (Online) Vol.5, No.5, 2014.
- [4] Garg, Saloni, Sonam Khera, Archana Aggarwal, and P. G. Scholar. "Extended Vigenere Cipherwith Stream Cipher." International Journal of Engineering Science and Computing (IJESC) 6, no. 5 (2016).
- [5] Aized Amin Soofi, Irfan Riaz, and Umair Rasheed. "An Enhanced Vigenere Cipher for DataSecurity." International Journal of Scientific & Technology Research 5, no. 03 (2016). [6] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar a nd Vigenere cipher." In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International
- [6] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." InComputationalIntelligenceandComputingResearch(ICCIC),2013IEEEInternational Conference on, pp. 1 -3 . IEEE, 2013.
- [7] Sanjeev Kumar Mandal, "A Cryptosystem Based On Vigenere Cipher By Using Multilevel Encryption Scheme." (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (4) 2016, 2096 - 2099.
- [8] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341 –2345, 2016.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details