International Research Journal of Education and Technology

Peer Reviewed Journal, **ISSN: 2581-7795**

Cyber security: Data Protection using Hybrid Encryption & Steganography

Suresh Poojala[1], Mr. A Rajesh[2]

[1]M Tech student of LINGAYAS INSTITUTE OF MANAGEMENT AND TECHNOLOGY, Madalavarigudem-521212, Andhra Pradesh
[2]Assistant Professor, Department of Computer Science &Engg, LINGAYAS INSTITUTE OF MANAGEMENT AND TECHNOLOGY, Madalavarigudem-521212 Andhra Pradesh.

Abstract -*In the evolving landscape of digital communication and data storage, cyber security remains a paramount concern. This project proposes a hybrid security framework that combines Hybrid Encryption (AES + ECC) with Image-based Steganography to provide enhanced protection for user data stored on centralized or decentralized servers. The hybrid encryption approach ensures that data cannot be decrypted even if malicious actors obtain partial keys, as it uses both symmetric and asymmetric algorithms. Additionally, Steganography conceals sensitive messages within image files, enabling covert data transmission while maintaining the appearance of innocuous media. To further ensure data integrity, the system generates a unique hashcode for each uploaded file, allowing verification at any time.*

Access control is fortified through multi-factor authentication, combining traditional credentials with OTP-based email verification. Beyond security operations, the platform also includes user education tools, providing learning materials and real-time cybersecurity news updates. Developed using Python and MySQL, the application empowers users to encrypt files, hide data in images, retrieve decrypted files, and stay informed about modern threats—all through a secure and interactive web interface.

1.INTRODUCTION

With the rapid advancement of digital technology, user data is increasingly transmitted and stored across centralized cloud platforms and decentralized systems like P2P and blockchain networks. Despite widespread adoption of encryption techniques by these platforms, sensitive data remains vulnerable—especially when stored remotely—due to the risk of unauthorized access by malicious insiders or compromised servers.

To combat these threats, this project introduces a novel cyber security approach by combining Hybrid Encryption and Steganography to offer a dual layer of protection for user data. Hybrid Encryption integrates both symmetric (AES) and asymmetric (ECC) encryption techniques. AES provides fast and efficient data encryption, while ECC offers secure key distribution. This combination ensures that even if a server is compromised, it becomes virtually impossible to decrypt the data without access to both encryption keys.

Complementing this, Image-based steganography is employed to conceal encrypted messages within digital images, allowing users to upload protected content that appears visually unchanged to outsiders. This form of security-through-obscurity adds another dimension to safeguarding user information. Although video and audio steganography offer similar benefits, they demand high computational resources and are therefore not used in this implementation.

To further ensure data integrity and prevent tampering, a cryptographic hash function is generated for every uploaded file. Users can verify the file's authenticity at any time by rechecking its hash code.

In addition to data protection, the platform features multi-factor authentication (MFA) using email-based OTP verification to prevent unauthorized account access. Users must provide a valid email during registration, strengthening account security against intrusion attempts.

The application also serves as an educational tool, featuring modules such as "Learning Tools" and "News Updates", designed to raise awareness about modern cybersecurity threats and solutions.

This hybrid system not only empowers users to encrypt, hide, and verify their data independently but also promotes cyber hygiene

2. Literature Survey:

1. Data Vulnerability in Centralized and Decentralized Systems

With the widespread use of centralized (cloud-based) and decentralized (P2P, blockchain) systems, user data often resides on third-party servers, exposing it to risks from insiders and external threats. Even when encrypted, if key management is weak, data remains vulnerable (Zhou et al., 2010).

2. Hybrid Encryption for Enhanced Security

Hybrid encryption combines the efficiency of symmetric encryption (like AES) with the security of asymmetric encryption (like ECC). This dual-layer strategy ensures that even if one key is compromised, the complete decryption

3. Steganography for Concealed Communication

Steganography hides the existence of a message, making it more secure than encryption alone. Image-based steganography is particularly useful because images are common file types and do not raise suspicion. Tools like LSB (Least Significant Bit) embedding are effective and computationally less intensive (Johnson & Katzenbeisser, 2000).

4. Hashing for Data Integrity Verification

Hash functions such as SHA-256 are used to verify the integrity of stored files. Any modification in the data results in a completely different hash, helping to detect unauthorized changes (Preneel, 1999).

5. Multi-Factor Authentication (MFA) for User Access Control

Combining traditional credentials (username/password) with a second factor like email OTP enhances account security. MFA drastically reduces the risk of unauthorized access, especially in web-based systems (Aloul, 2009).

Existing System:

In current digital ecosystems, user data is frequently stored on centralized cloud platforms or decentralized servers like peer-to-peer (P2P) networks and blockchain. These platforms provide standard encryption protocols, but they remain vulnerable because the data is stored away from the user's control. Malicious insiders or attackers with access to server infrastructure can potentially retrieve encryption keys and decrypt sensitive information. Furthermore, conventional security systems rely on single-factor authentication, which can be easily compromised. Most systems also lack an effective mechanism to verify the integrity of stored files. These limitations pose serious threats to data confidentiality, integrity, and authenticity, making user data susceptible to breaches, unauthorized access, and tampering.

Proposed System:

The proposed system enhances cybersecurity through a multi-layered approach combining hybrid encryption and image steganography. Hybrid encryption leverages both symmetric (AES) and asymmetric (ECC) algorithms, ensuring that no single party, including server administrators, can access the full set of keys required to decrypt the file. For additional secrecy, sensitive messages can be embedded within images using image-based steganography, making the data appear innocuous to unauthorized viewers. To maintain file integrity, a hashcode is generated and stored with each file, allowing users to verify that their data has not been altered. The platform incorporates multi-factor authentication (MFA) through email OTPs, ensuring that only verified users can access the system. Educational modules like Learning Tools and Cybersecurity News Updates are included to keep users informed about modern threats and tools. Together, these features provide a self-secured, tamper-proof environment for data protection.

Problem Statement

Modern servers, although encrypted, can be vulnerable to malicious internal actors who can access encryption keys. Cloud-stored user data is particularly at risk of unauthorized decryption.

3. Proposed Solution

To combat this, the system:

Encrypts files using Hybrid Encryption:

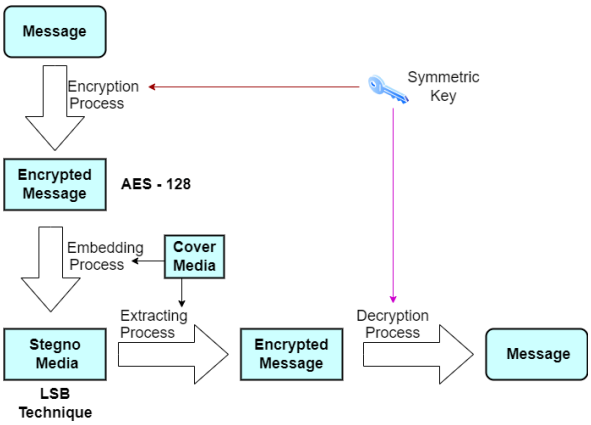
AES (Symmetric) for fast encryption.

ECC (Asymmetric) to protect the AES key.

Embeds hidden messages using Image-based Steganography.

Verifies file integrity using SHA-based Hashing.

Enforces Multi-Factor Authentication (MFA) via email OTP. Educates users through Cybersecurity learning tools and news feeds.



System Architecture

4. System Implementations:

With the increasing risk of data breaches through both centralized and decentralized platforms, this system proposes a robust solution that combines Hybrid Encryption (AES + ECC) with Image Steganography to ensure end-to-end data security and integrity. It also features multi-factor authentication, hash-based verification, and cybersecurity awareness modules.

4.1 Dual Approach Solution

As data continues to move across cloud and decentralized servers, there is a growing concern over internal threats such as malicious employees who may access encryption keys. Existing encryption mechanisms are vulnerable when both encryption and decryption processes are controlled by the same server. This work introduces a dual-approach solution:

- Hybrid Encryption: Uses symmetric (AES) and asymmetric (ECC) encryption to separate encryption keys, making unauthorized access nearly impossible.
- Image Steganography: Hides encrypted messages within images, making sensitive information indistinguishable from regular content.

Additionally, multi-factor authentication (MFA) using email OTPs ensures that only genuine users can access the system.

System Modules

3.1 New User Sign-Up

Users register by filling a form. Valid email addresses are required for OTP authentication.

4.2 User Login and OTP Verification

Upon login, an OTP is sent to the registered email. Users must input this OTP to continue.

4.3 Hybrid Encryption Module

Users upload any file.

The file is encrypted using AES (for speed) and ECC (for secure key exchange).

A hash is generated to ensure file integrity.

Encrypted files are stored on the server.

4.4 Image Steganography Module

Users type a secret message and upload a cover image.

The system embeds the encrypted message into the image using LSB or similar steganographic techniques.

The image is saved as a regular file, obscuring the presence of any secret message.

4.5 Access Data Module

Lists all previously uploaded files.

Displays:

Encryption type (Hybrid/Steganography)

Hash code

Download options (Decrypted file or extracted hidden message)

4.6 Learning Tools Module

Provides information about:

Latest cybersecurity tools

Best practices for data protection

4.7 News Updates Module

Fetches and displays current cybersecurity-related news and trends to keep users informed.

5. Implementation Environment

Backend: Python 3.7.2

Database: MySQL (initialized using provided database.txt)

Frontend: HTML-based UI hosted on a local Python server

Security Libraries: AES (from pycryptodome), ECC, Hashlib

Steganography: Image-based using Python image processing libraries

6. SCREEN SHOTS

Growing technologies making user data to be float in network universe with the help of centralized servers like Clouds and Decentralized servers like P2P or Blockchain. All servers providing heavy encryption for user data security but data store away from user hands always vulnerable to 3rd party malicious server employees who can easily get database keys and can decrypt user data.

To avoid above data leakage we are employing Hybrid and steganography based self-data protection algorithms to provide more security to user's data. In propose work as Hybrid encryption we are encrypting file with symmetric (AES) and asymmetric (ECC) algorithms and this Hybrid Encryption will not allow Server employees to know keys of both algorithms and file will not be decrypted.

In Steganography process user can hide messages in images and upload to network like plain image and malicious users aware of hidden message and user data will be secured. Note: you ask for video and audio steganography also but this required heavy computation so we are employing Image based Steganography.

To further check file integrity we are generating hashcode on uploaded file so file content will be verify anytime with the help of hashcode.

To allow only genuine user to access account we are employing Multi Factor based authentication where user has to authenticate with normal login and then must be authenticated via EMAIL OTP. So give valid Email ID during registration.

To aware user about Cybersecurity issues we are allowing user to know about latest tools and learning materials by accessing modules like 'Learning Material and News Updates'.

To implement this project we have designed following modules

1) New User Sign up: user can sign up with the application

2) User Login: user can login to system and then authenticate via OTP process

3) Hybrid Encryption: using this module user can upload any file which will get encrypted using Hybrid Encryption process and file integrity process will be done with hashcode.

4) Image Steganography: using this module user can enter some message and then upload image and then system will hide encrypted message in image.

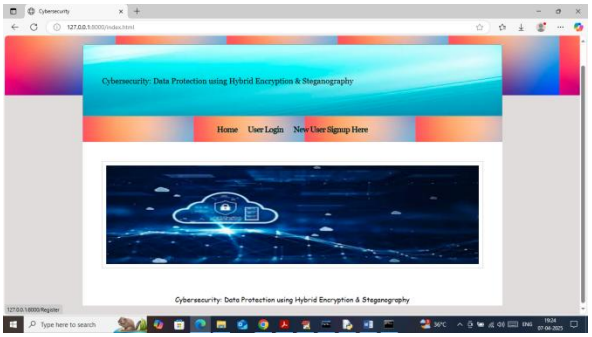


Figure 1. screen click on 'New User Sign up' link to get below page

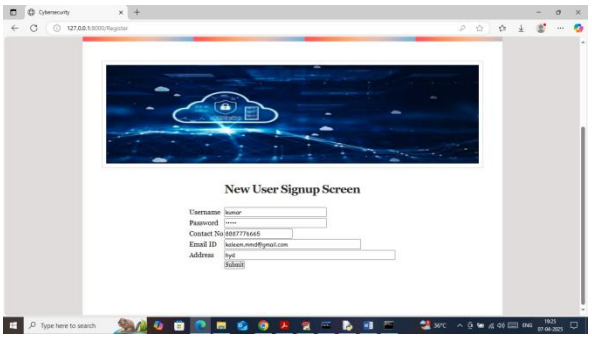


Figure 2. user is entering sign up details and then press button to get below page

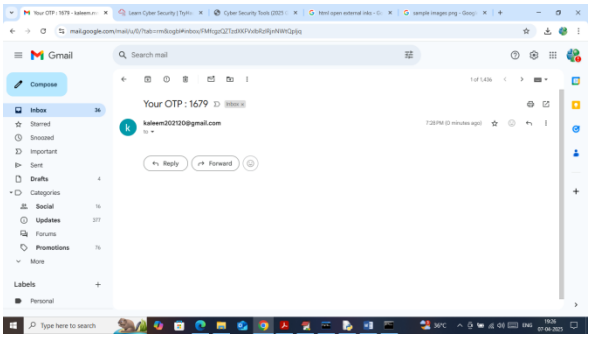


Figure 3 : OTP received to email and enter to application to continue authentication process

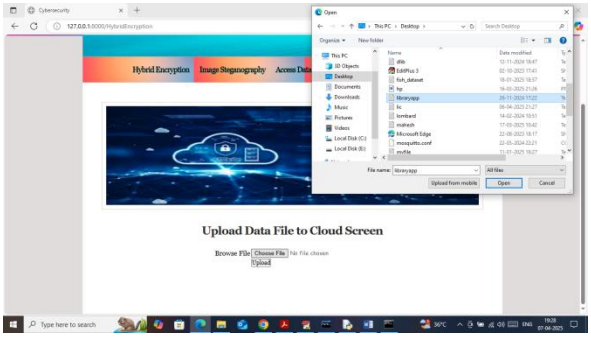


Figure 4 : select and upload any file and then click on 'Open and upload' buttons to saved file in encrypted format

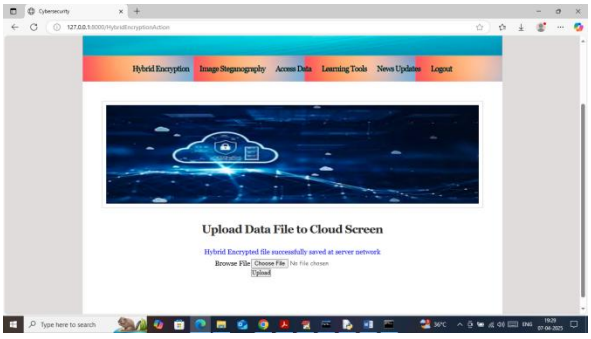


Figure 5 : file saved at server and in below screen can see file content in encrypted format

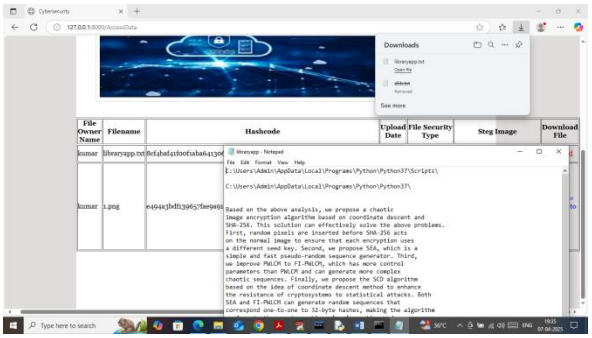


Figure 6 : Hybrid Encryption' then user can click on red 'Download' link download file in decrypted format

7. Conclusion:

In this project, we successfully implemented a cybersecurity solution that integrates hybrid encryption (AES + ECC) and image-based steganography to provide robust protection for user data. The system ensures that even if data is intercepted or accessed by unauthorized parties, it remains indecipherable due to the dual-layered encryption. Additionally, image steganography provides an extra layer of obscurity by hiding sensitive information within image files, making it unrecognizable to potential attackers. To verify the integrity of data, hashcodes are generated for all uploaded files, enabling reliable verification of data authenticity at any time. The inclusion of multi-factor authentication via email OTP adds another layer of user security, preventing unauthorized access to the platform. Supporting features such as cybersecurity learning tools and news updates further enhance user awareness and platform usability. Overall, the platform demonstrates a secure, user-friendly, and practical approach to modern data protection needs.

8. Future Work:

While the current implementation achieves a high level of data security, several improvements and expansions can be considered in future work. First, the integration of audio and video steganography could significantly broaden the applicability of the system, especially for multimedia data, although

this would require more advanced computational resources and optimized algorithms. Additionally, migrating from local server deployment to a cloud-based or blockchain-based backend could improve system scalability, resilience, and decentralization. Implementing real-time anomaly detection and AI-driven threat analytics would provide dynamic protection against evolving cybersecurity threats. Lastly, expanding the system to include mobile platforms and cross-platform encryption compatibility could enhance accessibility and practical use in real-world scenarios. Continued user feedback and security audits will also be essential in identifying vulnerabilities and evolving the platform to meet future cybersecurity demands.

9. References

1.Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209.

2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.

3. Eastlake, D., & Jones, P. (2001). US Secure Hash Algorithm 1 (SHA1). RFC 3174.

4. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding — A survey. Proceedings of the IEEE, 87(7), 1062–1078.

5. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

6. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information Hiding: Steganography and Watermarking — Attacks and Countermeasures. Springer.

7. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C (20th Anniversary ed.). Wiley.

8. Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2019). The Tangled Web of Password Reuse. In Proceedings of the Network and Distributed System Security Symposium.

9. Bhattacharyya, D., Kim, T. H., & Pal, K. (2011). A comparative study of symmetric and asymmetric cryptography. Proceedings of the 2011 International Conference on Information and Communication Technology.

10 Provos, N., & Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy, 1(3), 32–44.

11. Mallikaarachchi, K. S., Huang, J. L., Madras, S., Cuellar, R. A., Huang, Z., Gega, A., Rathnayaka-Mudiyanselage, I. W., Al-Husini, N., Saldaña-Rivera, N., Ma, L. H., Ng, E., Chen, J. C., & Schrader, J. M. (2024, April 6). *Sinorhizobium meliloti BR-bodies promote fitness during host colonization*. *bioRxiv*. https://doi.org/10.1101/2024.04.05.587509

12. Gowda, D., Annepu, A., Kulkarni, S. V., Madras, S. S., & Rao, B. K. (2026). *AI and IIoT enabling smart connectivity and automation in healthcare*. In *Cybersecurity and privacy in the era of smart technologies* (pp. 1–30). IGI Global Scientific Publishing.

13. Singh, A., Patil, S., Wilson, R., Dixit, P. R., & Madras, S. S. (2025). *Chemical toxicology of drug metabolites: Implications for human health*. *Journal of Applied Bioanalysis, 11*(3), 328–335. Green Publication.

14. Madras, S. S. (2024, December). *Unlocking novel hydrocolloids: Purification and characterization of exopolysaccharides from rhizobia*. *European Journal of Molecular & Clinical Medicine, 11*(5), 302–316. EJMCM, International House.

15. Madras, S. S. (2022, May). *Comparative analysis of aerobic and anaerobic bacterial culturing methodologies*. *African Journal of Biological Sciences (South Africa), 4*(2), 226–247. Institute for Advanced Studies.