CYBERSECURITY: DATA PROTECTION USING HYBRID ENCRYPTION & STEGANOGRAPHY

Sk. AnjaneyuluBabu[1], P.Rama Krishna[2]
Assistant Professor [1], PG Scholar [2]
Department of Master of Computer Applications
QIS College of Engineering & Technology (Autonomous), Ongole
Prakasam Dist., AP

ABSTRACT

In the evolving landscape of digital communication and data storage, cybersecurity 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.

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 cybersecurity 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 and awareness—ensuring privacy and trust in a digitally connected world.

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).

Reference: Zhou, Z., & Huang, D. (2010). Efficient and secure data storage operations for mobile cloud computing. Proceedings of the 8th International Conference on Network and Service Management (CNSM).

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 remains infeasible (Menezes et al., 1996).

Reference: Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography.CRC Press.

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).

Reference: Katzenbeisser, S., &Petitcolas, F. A. P. (2000). Information hiding techniques for steganography and digital watermarking.Artech House.

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).

Reference: Preneel, B. (1999). Analysis and design of cryptographic hash functions. Doctoral dissertation, KU Leuven.

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).

Reference: Aloul, F. A. (2009). Two factor authentication using mobile phones. IEEE/ACS International Conference on Computer Systems and Applications.

6. Limited Robustness Against Image Compression

Steganographic data embedded in spatial domain images may be destroyed during compression or resizing operations, reducing reliability in real-world transmission (Barni&Bartolini, 2004).

Reference: Barni, M., &Bartolini, F. (2004). *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*. Marcel Dekker.

7. Key Exchange Vulnerabilities in Public-Key Cryptography

Public-key encryption relies on secure key exchange mechanisms. Man-in-the-middle attacks can intercept keys if proper authentication protocols are not implemented (Rivest et al., 1978).

Reference: Rivest, R., Shamir, A., &Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems.*Communications of the ACM*, 21(2), 120–126.

8. Detection Risks in Transform-Domain Steganography

Although more robust than LSB, transform-domain methods like DCT can still be detected using advanced statistical models and machine learning-based steganalysis (Katzenbeisser&Petitcolas, 2000).

Reference: Katzenbeisser, S., &Petitcolas, F. A. P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*.Artech House.

9. Scalability Issues in Large-Scale Secure Systems

Hybrid encryption systems deployed in large distributed networks may face scalability challenges in managing keys and

maintaining encryption efficiency (Gupta & Jain, 2018).
Reference: Gupta, S., & Jain, A. (2018). A hybrid approach for secure cloud data storage.*International Journal of Computer Applications*, 179(5), 1–6.

10. Emerging Threats from AI-Based Steganalysis

Recent advancements in deep learning have enabled automated detection of hidden messages within digital media, challenging traditional steganography techniques (Hayes &Danezis, 2017).
Reference: Hayes, J., &Danezis, G. (2017). Generating steganographic images via adversarial training.*Advances in Neural Information Processing Systems (NeurIPS)*.

SYSTEM ANALYSIS

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.

Disadvantages of Existing Systems:

Centralized Encryption	Data stored in the cloud is often only encrypted using a **single algorithm**(e.g., AES). If server admins access the key, they can decrypt the data.
NoSteganography	Sensitive messages are stored visibly in files or databases, easily targeted.
Single Factor Authentication	Most platforms rely on just a password, which is vulnerable to brute-force or phishing attacks.

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.

Advantages of the Proposed System

Feature	Proposed System Implementation
Hybrid Encryption	Uses both **AES (symmetric)** and **ECC (asymmetric)**Encryption. Knowing one key alone cannot decrypt data. Screenshots show files encrypted and saved on the server.
Image Steganography	Hides encrypted messages inside images. Steganographic images appear normal, avoiding suspicion. Screenshot shows message successfully embedded in the image.
Multi-Factor Authentication	Users log in with a password and verify with an **Email OTP**. Shown in login and OTP entry screens.

IMPLEMENTATION

The implementation of the Cybersecurity Data Protection System focuses on securing sensitive information using Hybrid Encryption and Steganography techniques. The system combines cryptographic algorithms with hidden data embedding methods to provide multiple layers of security for confidential data transmission and storage.

The proposed system protects sensitive information from unauthorized access, cyberattacks, interception, and data leakage by encrypting data and concealing it within digital media files such as images, audio, or video.

1. Data Collection and Input

The first stage involves collecting confidential data that needs protection.

The input data may include:

- Text documents
- Personal information
- Financial records
- Passwords
- Medical records
- Business files
- Images and multimedia data

The user uploads or enters the data into the secure system for protection.

2. Hybrid Encryption Implementation

Hybrid Encryption combines symmetric and asymmetric encryption techniques to improve both security and efficiency.

Symmetric Encryption

Used for fast encryption of large amounts of data.

Algorithms Used

- AES (Advanced Encryption Standard)
- DES / Triple DES
- Blowfish

The plaintext data is converted into encrypted ciphertext using a secret key.

Asymmetric Encryption

Used for secure key exchange and authentication.

Algorithms Used

- RSA
- ECC (Elliptic Curve Cryptography)

The symmetric encryption key is encrypted using the receiver's public key.

This combination provides secure and efficient communication.

3. Data Encryption Process

The encryption workflow includes:

1. User selects confidential data
2. Generate symmetric encryption key
3. Encrypt data using AES or similar algorithm
4. Encrypt secret key using RSA/ECC
5. Generate encrypted output

This ensures confidentiality and secure key management.

4. Steganography Implementation

Steganography is used to hide encrypted data inside digital media files.

Cover Media Used

- Images
- Audio files
- Video files

The encrypted ciphertext is embedded into a cover file without visibly changing the original media.

5. Steganography Techniques

Different steganography techniques can be applied based on media type.

Image Steganography

- Least Significant Bit (LSB)
- Pixel Value Differencing
- DCT-based embedding

Audio Steganography

- Echo hiding
- Phase coding
- Frequency masking

Video Steganography

- Frame-based embedding
- Motion vector embedding

These methods improve hidden data security and invisibility.

6. Secure Data Transmission

The stego file containing hidden encrypted data is transmitted through communication channels such as:

- Email systems
- Cloud platforms
- Messaging applications
- File transfer systems

Even if intercepted, attackers cannot easily detect or decrypt the hidden data.

7. Data Extraction and Decryption

At the receiver side:

1. Extract hidden encrypted data from the stego file
2. Decrypt the symmetric key using private key
3. Decrypt ciphertext using symmetric key
4. Recover original plaintext data

This restores the confidential information securely.

8. Security Monitoring and Integrity Verification

The system verifies:

- Data integrity
- Unauthorized modification attempts
- Tampering detection
- Authentication validity

Hashing algorithms may be used:

- SHA-256
- MD5
- SHA-3

This improves data integrity protection.

9. System Deployment

The final cybersecurity protection system can be deployed as:

- Secure File Sharing Platform
- Cloud Security System
- Enterprise Data Protection Solution
- Secure Messaging Application
- Digital Forensics Security Tool

Deployment platforms may include:

- AWS
- Microsoft Azure
- Google Cloud Platform

METHODOLOGY

The methodology of the proposed Cybersecurity Data Protection System follows a hybrid cryptographic and steganographic security approach.

Step 1: Problem Identification

Sensitive digital information is vulnerable to cyberattacks, unauthorized access, and data interception during communication and storage. Traditional encryption alone may expose the presence of confidential data. The proposed system aims to improve cybersecurity by combining encryption and steganography.

Step 2: Requirement Analysis

The following requirements are analyzed:

- Confidential data protection requirements
- Encryption algorithm requirements
- Steganography media requirements
- Secure communication requirements
- Integrity verification requirements

Step 3: Data Preparation

Sensitive information is collected and prepared for encryption.

The system selects:

- Appropriate encryption algorithms
- Cover media for steganography
- Secure key generation methods

Step 4: Hybrid Encryption Implementation

The methodology includes:

1. Generate secret encryption key
2. Encrypt data using symmetric encryption
3. Encrypt secret key using asymmetric encryption
4. Produce secure ciphertext

This provides confidentiality and secure key exchange.

Step 5: Steganography Embedding

The workflow includes:

1. Select cover image/audio/video
2. Embed encrypted data into cover media
3. Generate stego file
4. Verify embedding invisibility

This conceals the existence of confidential information.

Step 6: Secure Communication

The stego file is transmitted securely through communication channels while maintaining confidentiality and hidden data protection.

Step 7: Extraction and Recovery

The receiver:

1. Extracts hidden encrypted data
2. Decrypts secret key
3. Recovers original plaintext data

This ensures secure information retrieval.

Step 8: Performance Evaluation

The system is evaluated based on:

- Encryption security strength
- Steganography invisibility
- Data integrity protection
- Transmission security
- Computational efficiency

Step 9: Result Generation

The system generates outputs such as:

- Encrypted data files
- Stego media files
- Integrity verification reports
- Secure communication logs
- Data recovery reports

Step 10: Conclusion and Future Enhancement

The final stage evaluates the effectiveness of the system and suggests future improvements such as:

- AI-powered adaptive encryption systems
- Blockchain-secured data sharing
- Quantum-resistant cryptographic algorithms
- Real-time intrusion detection integration
- Cloud-native cybersecurity frameworks
- IoT-based secure communication systems

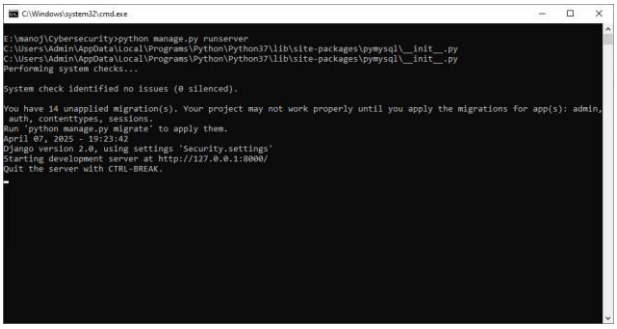
Technologies Used

- Python
- Cryptography Libraries
- AES / RSA Algorithms
- OpenCV
- Steganography Techniques
- Hashing Algorithms
- Flask / Django
- MySQL / MongoDB

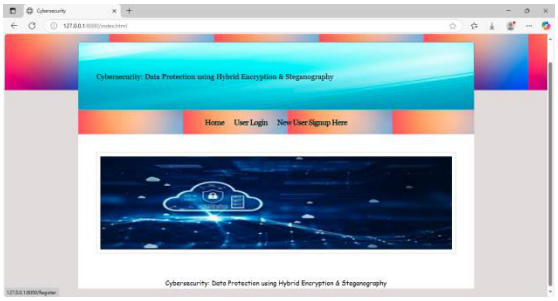
RESULTS

To run project install python 3.7.2 and then install all packages given in requirements.txt file. Install MYSQL and then copy content from 'database.txt' file and paste in MYSQL console to create database.

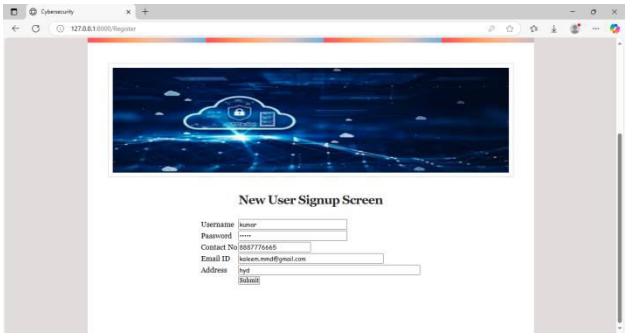
Now double click on 'run.bat' file to start python web server and then will get below page



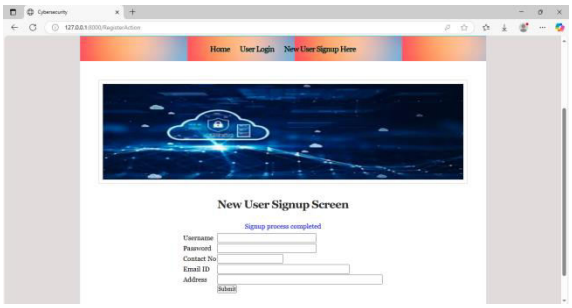
In above screen python server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and then press enter key to get below page



In above screen click on 'New User Sign up' link to get below page

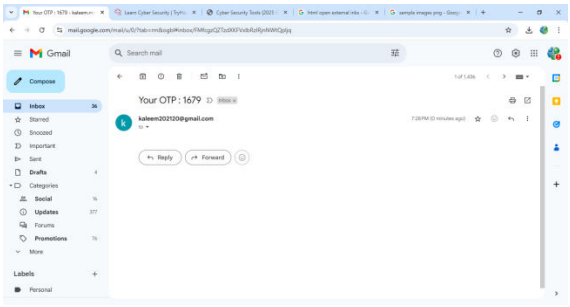


In above screen user is entering sign up details and then press button to get below page

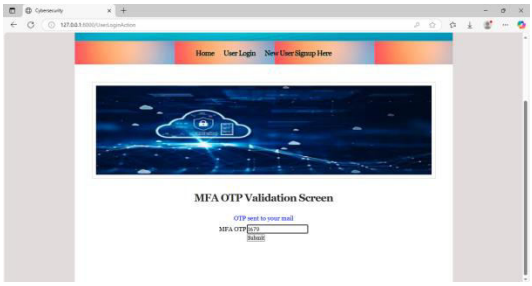


In above screen sign up process completed and now click on 'User Login' link to get below page

In above screen user is login and after login will get OTP in email like below page



In above screen OTP received to email and enter to application to continue authentication process



In above screen enter OTP and then press button to get below page

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.

REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987. [1, 2]

[2] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*.CRC Press, 1996. [1]

[3] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," RFC 3174, 2001.

[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding — A survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking — Attacks and Countermeasures*. Springer, 2001.

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

[8] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The Tangled Web of Password Reuse," in *Proceedings of the Network and Distributed System Security Symposium*, 2019.

[9] D. Bhattacharyya, T. H. Kim, and K. Pal, "A comparative study of symmetric and asymmetric cryptography," in *Proceedings of the 2011 International Conference on Security Technology*, 2011.

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

AUTHORS PROFILES

Mr. SK.ANJANEYULU BABU is an Associate Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. His Specialization is AI&ML.

Mr P.RAMA KRISHNA is a postgraduate student pursuing an MCA in the Department of Master of Computer Applications at QIS College of Engineering & Technology, Ongole an Autonomous college in Prakasam dist. He completed his undergraduate degree in B.Sc (Computers) from Acharya Nagarjuna University. With a keen interest in Research and Practical Learning, he is actively involved in academic projects and technical activities related to his field