International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Cybersecurity: Data Protection Using Hybrid Encryption and Steganography

Saripilli Sarika
Reg. No. 24Q71F0060
Saripillisarika0705@gmail.com
Department of Master of Computer Applications
Avanthi Institute of Engineering and Technology (Autonomous)
Vizianagaram, Andhra Pradesh, India
Under the guidance of Mrs. T. Varalakshmi, MCA, Assistant Professor
laxmivara588@gmail.com

***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 hash code 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 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. By layering encryption, steganography, hashing, and multi-factor authentication, the proposed system provides a self-secured, tamper-resistant environment that addresses insider threats and the limitations of single-layer protection.*

Keywords*—*Cybersecurity; Hybrid Encryption; AES; Elliptic Curve Cryptography; Image Steganography; Hash-Based Integrity; Multi-Factor Authentication; Data Protection.

I. INTRODUCTION

In today's digital world, the amount of data shared through the internet is increasing rapidly. Personal information, financial records, business documents, healthcare reports, and confidential files are continuously transmitted through centralized cloud servers and decentralized platforms such as blockchain and peer-to-peer networks. Although these technologies provide convenience and accessibility, they also introduce serious cybersecurity challenges, as cybercriminals, malicious insiders, and unauthorised users constantly attempt to gain access to sensitive information, leading to data breaches, identity theft, financial loss, and privacy violations.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Traditional security systems mainly depend on single-layer encryption methods and password-based authentication, which are no longer sufficient because attackers have developed advanced methods to crack passwords, steal encryption keys, and exploit server vulnerabilities. Even when encryption is applied, the encryption keys may still be accessible to system administrators or attackers who compromise the server infrastructure. A stronger approach is therefore required in which information is both encrypted and hidden from attackers.

This project introduces an advanced security framework that combines multiple protection techniques: hybrid encryption combining AES for fast, efficient file encryption and ECC for secure key exchange and key protection; image-based steganography using Least Significant Bit (LSB) embedding to hide encrypted messages within images without noticeable visual change; hash-based integrity verification using SHA to detect any modification of stored files; and multi-factor authentication that combines credentials with OTP-based email verification. The platform also includes user-education tools and cybersecurity news updates, providing multi-layered security against modern cyber threats.

II. LITERATURE SURVEY

With the rapid growth of cloud computing, peer-to-peer networks, and blockchain technology, a large amount of user data is stored on centralized and decentralized servers where users have limited control. In centralized systems, providers manage encryption keys and storage infrastructure, so malicious insiders or attackers who gain access to the server environment may retrieve keys and decrypt confidential files; decentralized systems face risks related to unauthorised node access, weak authentication, and data exposure. Researchers have emphasised that traditional storage systems cannot fully guarantee confidentiality, integrity, and privacy, so stronger security mechanisms are required.

Hybrid encryption is considered one of the most effective approaches for securing sensitive information because it combines the advantages of symmetric and asymmetric cryptography—AES provides high-speed encryption for large files, while ECC ensures secure key exchange with smaller key sizes—so that an attacker cannot decrypt the complete data even if one key is compromised. Steganography conceals secret information within digital media, hiding the very existence of the message; image-based steganography using LSB embedding is widely used because images can carry hidden information without noticeable change. Cryptographic hashing such as SHA produces fixed-length values that change completely with any modification, making hash-based verification highly effective for detecting tampering. These findings motivate combining encryption, steganography, hashing, and multi-factor authentication into a unified system.

TABLE I. SECURITY TECHNIQUES AND THEIR ROLE

S.No	Technique	Role in the System	Key Property
1	AES (symmetric)	Fast encryption of file content	High-speed, strong for large data

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

S.No	Technique	Role in the System	Key Property
2	ECC (asymmetric)	Secure key exchange and key protection	Strong security with small keys
3	Image steganography (LSB)	Hides encrypted message within an image	Conceals existence of data
4	SHA hashing	File-integrity verification	Detects any modification
5	Multi-factor authentication	Access control via credentials + OTP	Resists password attacks
6	Learning / news modules	User cybersecurity awareness	Improves usability and awareness

III. EXISTING SYSTEM AND PROPOSED SYSTEM

A. Existing System

In current digital ecosystems, user data is frequently stored on centralized cloud platforms or decentralized servers such as peer-to-peer networks and blockchain. These platforms provide standard encryption protocols but remain vulnerable because 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. Most systems rely on single-factor authentication, generally use a single encryption mechanism such as AES or RSA with keys managed by the same server, lack data-hiding techniques, and provide no effective mechanism to verify file integrity.

Disadvantages of the existing system:

- Single-layer encryption: one compromised key exposes all data.
- Lack of data-hiding techniques, so valuable data is easy to target.
- Weak authentication based only on username and password.
- Poor data-integrity verification, with no reliable tamper detection.
- Vulnerability to insider threats when one server manages all keys.

B. Proposed System

The proposed system enhances cybersecurity through a multi-layered approach. Hybrid encryption leverages both AES (symmetric) and ECC (asymmetric) so that no single party, including server administrators, can access the full set of keys required to decrypt a file. Sensitive messages can be embedded within images using image-based steganography, making the data appear innocuous. A hash code is generated and stored with each file so users can verify that data has not been altered, and multi-factor authentication through email OTPs ensures only verified users can access the system. Educational modules such as learning tools and cybersecurity news updates keep users informed about modern threats.

Advantages of the proposed system:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Enhanced security through dual-layer AES + ECC hybrid encryption.
- Secure hidden communication using image-based steganography.
- Strong multi-factor authentication via email OTP verification.
- Improved data-integrity verification using cryptographic hashing.
- Protection against insider threats through separated key management.
- User-awareness modules improving security knowledge and usability.

IV. SYSTEM ANALYSIS AND DESIGN

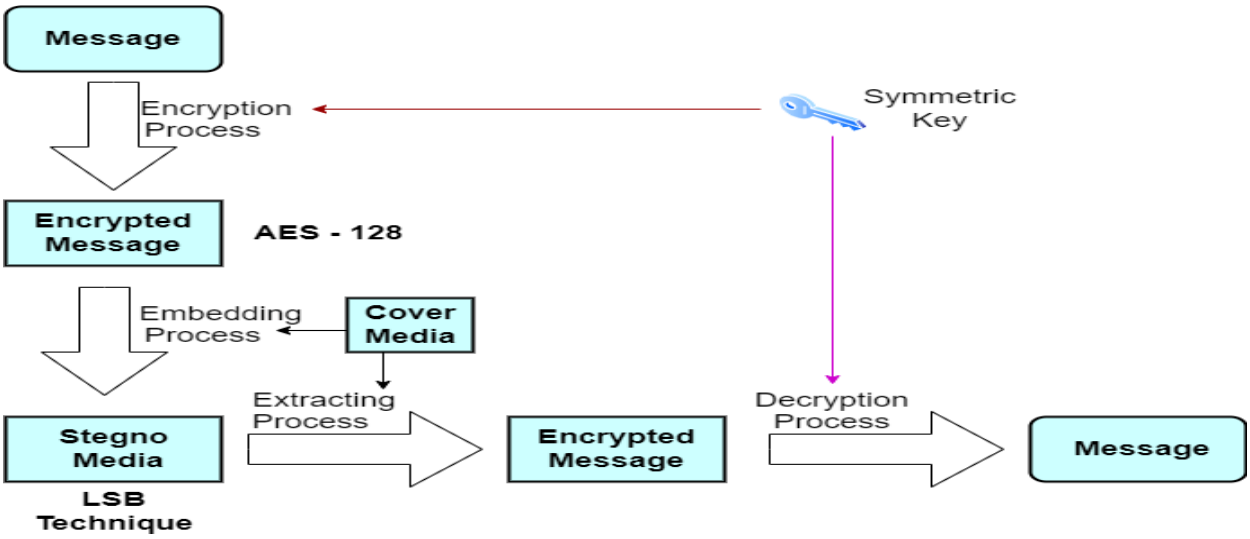
A. Requirements

Functionally, the system must allow new users to sign up with a valid email for OTP verification, authenticate users through multi-factor authentication, encrypt uploaded files using the hybrid AES + ECC mechanism, embed a secret message within a cover image using steganography, generate and store a hash code for every uploaded file, list and retrieve previously uploaded files with decrypted output or extracted hidden messages, and provide learning-tool and cybersecurity-news modules. Non-functionally, the system should ensure confidentiality, integrity, and authenticity of data, resist insider and brute-force attacks, and provide a usable web interface. The application is developed in Python with MySQL and runs on a standard Windows environment.

B. System Architecture

The architecture is organised around a secure web interface through which the user interacts with the encryption, steganography, integrity-verification, authentication, and education modules. Encrypted files and steganographic images are stored securely in the database. When the user requests access to stored information, the system retrieves the corresponding data, verifies integrity using hash codes, and provides decrypted output or extracted hidden messages. The learning-tools and news-update modules interact with the user by providing cybersecurity knowledge and current security information, while the authentication module enforces credential plus OTP verification before any operation.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



V. SYSTEM IMPLEMENTATION

A. Technology Stack

TABLE II. TECHNOLOGY STACK

Component	Technology / Tool
Programming Language	Python
Database	MySQL
Symmetric Encryption	AES (Advanced Encryption Standard)
Asymmetric Encryption	ECC (Elliptic Curve Cryptography)
Steganography	Image-based LSB embedding
Integrity Verification	SHA-based hashing
Authentication	Multi-factor authentication (email OTP)
Operating System	Windows

B. Core Modules

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The implementation realises the design as cooperating modules. The sign-up module registers users with a valid email required for OTP verification. The hybrid-encryption module lets users upload any file, encrypts the content with AES, and protects the encryption key with ECC. The image-steganography module lets users type a secret message and upload a cover image, embedding the (encrypted) message within the image using LSB embedding. The access-data module lists previously uploaded files and, after verifying the hash code, provides decrypted output or extracts the hidden message. The learning-tools and cybersecurity-news modules provide educational content and current threat information.

C. Security Workflow

A user authenticates through credentials and an email OTP. To protect a file, the content is encrypted with AES and the AES key is protected using ECC, so an attacker who obtains one key still cannot decrypt the data. For covert communication, an encrypted message is embedded into a cover image using LSB steganography, hiding its existence. A SHA hash is generated for every uploaded file and stored, allowing later verification—any modification produces a different hash, revealing tampering. This layered workflow combines confidentiality, obscurity, integrity, and strong access control.

VI. RESULTS AND DISCUSSION

Testing was conducted at the unit and functional levels, validating the internal logic of each module and the requirement-focused behaviour of sign-up and OTP verification, hybrid encryption and decryption, steganographic embedding and extraction, hash generation and integrity checking, and the learning and news modules. The reported test results indicate that all test cases passed successfully with no defects encountered. The implementation demonstrates that combining hybrid encryption with steganography keeps data indecipherable even if intercepted, while the hidden-message technique adds an additional layer of obscurity. Hash codes enable reliable verification of data authenticity at any time, and multi-factor authentication prevents unauthorised access. Performance and resource use depend on file size and image capacity, consistent with the qualitative behaviour described in the source.

Representative screenshots from the prototype implementation:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

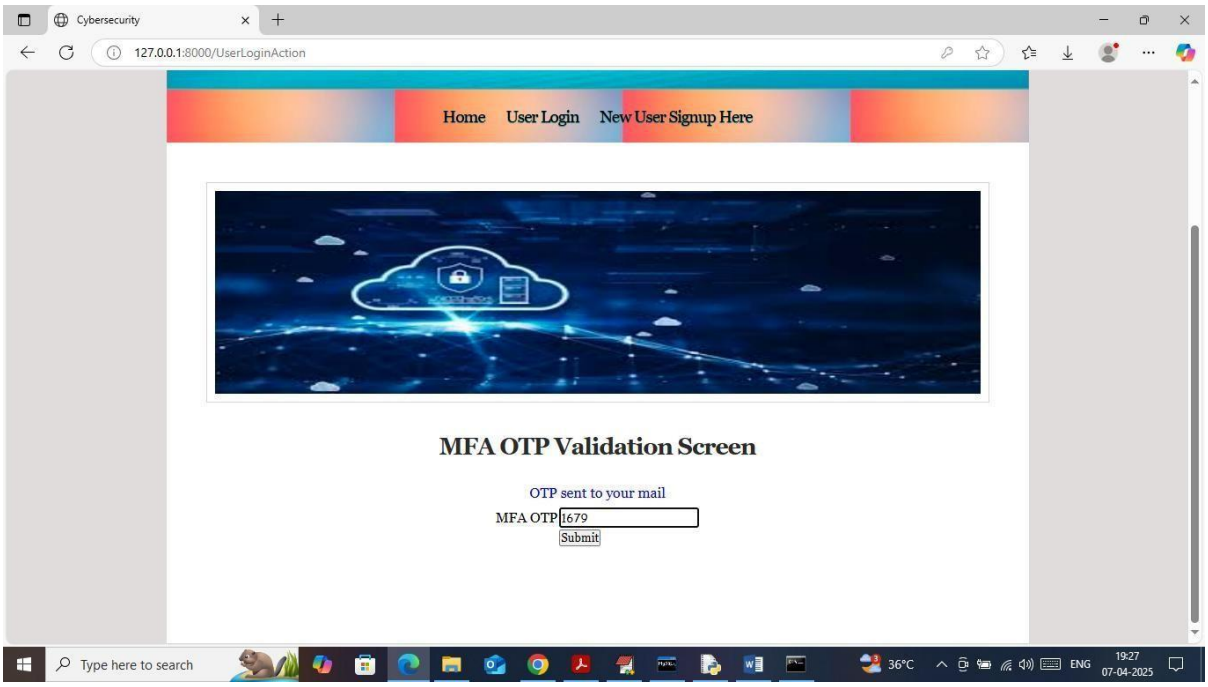


Fig. 1. Sign-up with email OTP verification.

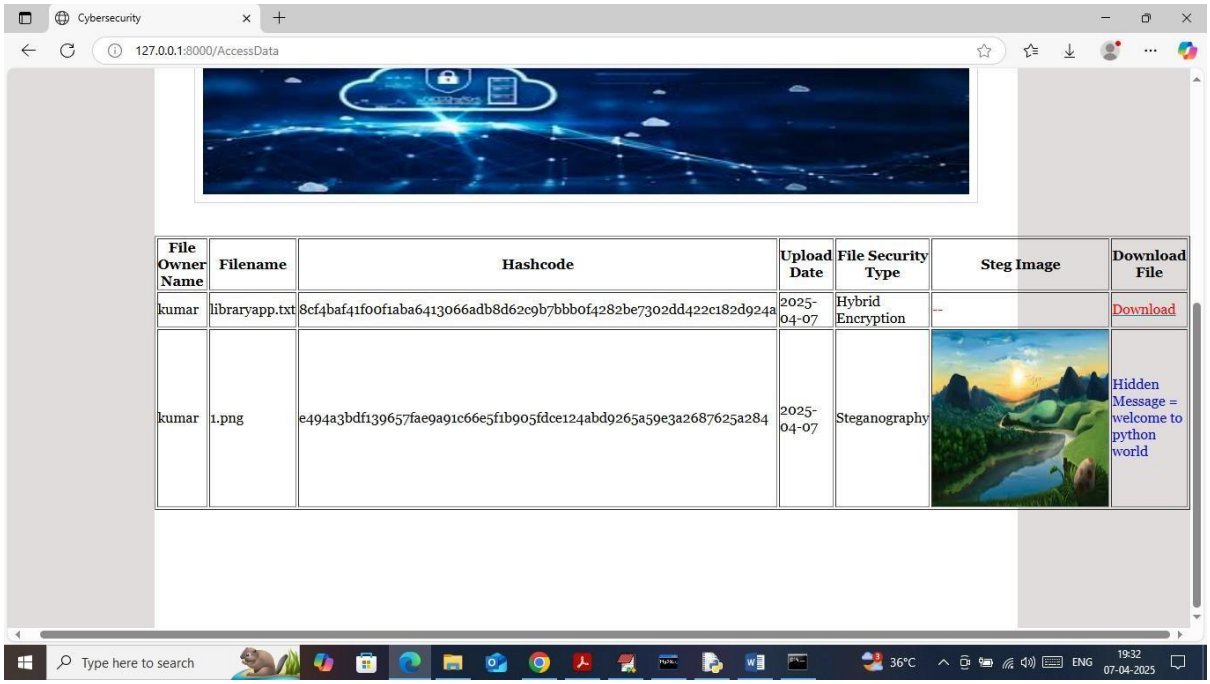


Fig. 2. Hybrid encryption (AES + ECC) of an uploaded file.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

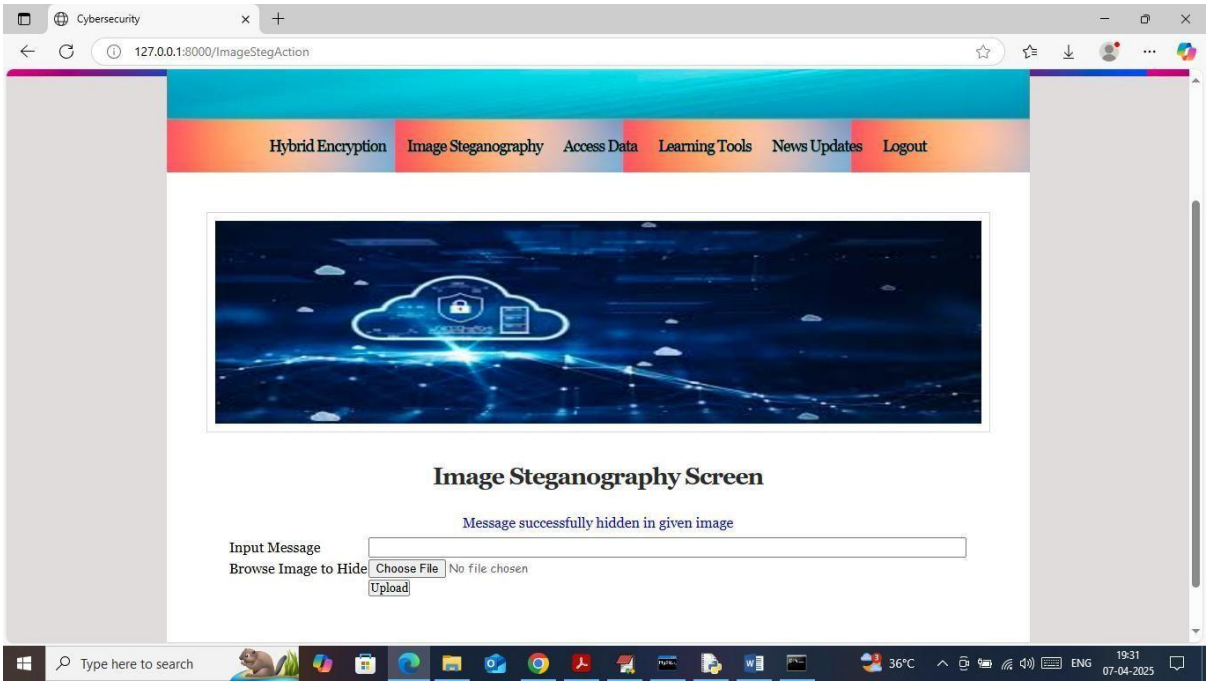


Fig. 3. Image steganography embedding a secret message.

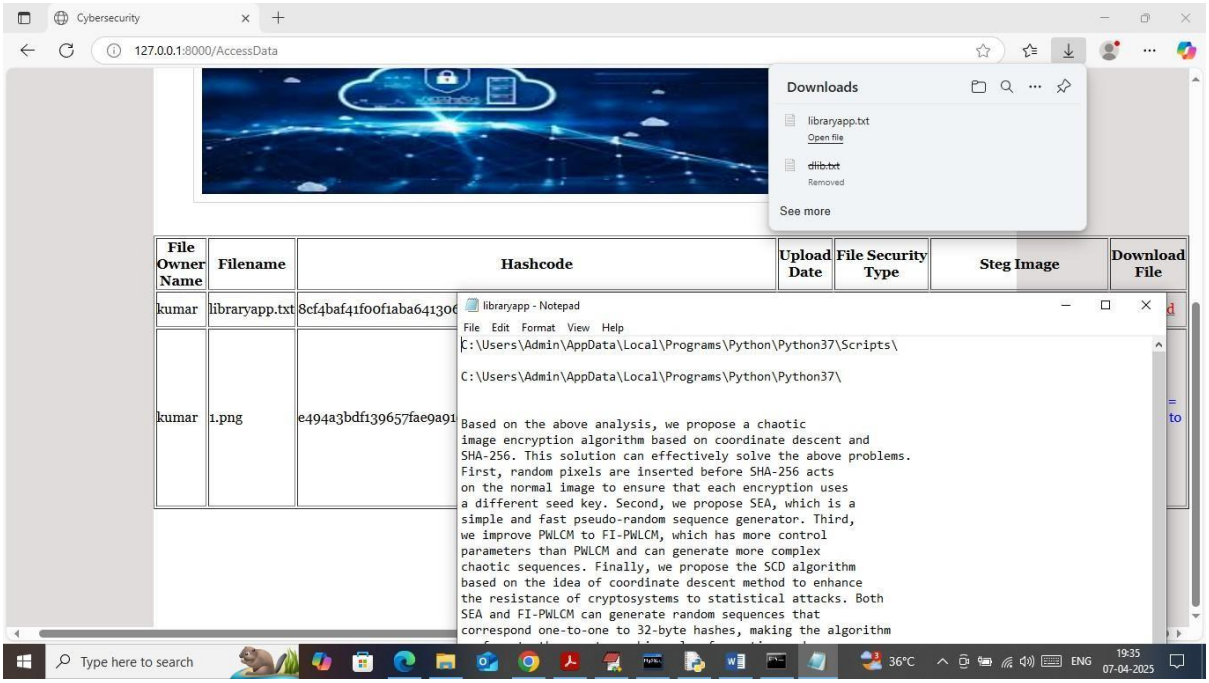


Fig. 4. File retrieval with hash-based integrity verification.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

VII. CONCLUSION AND FUTURE SCOPE

This project successfully implements 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 unauthorised parties, it remains indecipherable due to the dual-layered encryption, while image steganography hides sensitive information within image files, making it unrecognisable to potential attackers. Hash codes generated for uploaded files enable reliable verification of authenticity at any time, and multi-factor authentication via email OTP adds a further layer of user security. Supporting features such as cybersecurity learning tools and news updates enhance user awareness, and overall the platform demonstrates a secure, user-friendly, and practical approach to modern data protection.

Several improvements can be considered in future work. Integrating audio and video steganography would broaden applicability to multimedia data, though it would require more advanced computational resources and optimised algorithms. Migrating from local-server deployment to a cloud-based or blockchain-based backend could improve scalability, resilience, and decentralisation. Implementing real-time anomaly detection and AI-driven threat analytics would provide dynamic protection against evolving threats, and extending the system to mobile platforms with cross-platform encryption compatibility would enhance accessibility. Continued user feedback and security audits will be essential for identifying vulnerabilities and evolving the platform.

REFERENCES

[1] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.

[2] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[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 Proc. Network and Distributed System Security Symposium (NDSS), 2014.

[9] D. Bhattacharyya, T. H. Kim, and K. Pal, “A Comparative Study of Symmetric and Asymmetric Cryptography,” in Proc. Int. Conf. Information and Communication Technology, 2011.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[10] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.