RESEARCH ARTICLE OPEN ACCESS

Secure File Storage System Using Hybrid Cryptography

Divya Sharma*, Dev Jashani**

*(Department of Computer Science and Engineering, Global Institute of Technology, Jaipur

**(Department of Computer Science and Engineering, Global Institute of Technology, Jaipur

ABSTRACT: We are living in a digital world and so we store our files and important data in digital form only. For this we require a secure and reliable system on which we can securely store our files and retrieve them whenever required and someone else remain unable to access our file unless we give permission. Nowadays cloud is used heavily for storage purposes because it eliminates the need to buy and manage on-premises data storage infrastructure. It also allows remote access to data from anywhere and near-infinite scalability. But along with its numerous advantages it is also vulnerable to unethical hacking and data breaching. This is where a robust and secure system is required which not only prevents unauthorized access but even if data is accessed it is in unreadable form means the hacker is unable to understand it. This is where cryptography comes into picture. Although traditional encryption methods, such as symmetric and asymmetric encryption, have been essential to protect confidential information, they face several challenges that reduce their effectiveness in modern applications. So, a mechanism called hybrid cryptography is used where symmetric cryptographic algorithms i.e., AES, and an asymmetric cryptographic algorithm i.e., RSA are used to achieve confidentiality. These algorithms encrypt the files into the cloud and decryption is done by only the authorized user. Hybrid encryption systems combine the speed and efficiency of symmetric encryption for large data encryption with the security of asymmetric encryption for key exchanges. This dual strategy leverages the benefits of symmetric encryption's speed while maintaining the confidentiality and integrity of encryption keys through asymmetric encryption. This model not only enhances protection against unauthorized access, but also enables seamless scalability, making it well-suited for a broad array of real world applications.

Keywords **—** Asymmetric encryption, Data security, File storage, Hybrid cryptography, Encryption, Symmetric encryption.

I. INTRODUCTION

Secure file storage refers to storing files in a way that prevents unauthorized access or modifications and ensuring only authorized users access important information using strong security measures. A secure file storage system allows users to upload, download, share, and manage files while enforcing strict access controls and encryption to protect the data both in transit and at rest. Secure storage methods protect files using:

✔ Encryption (locks your files with unique codes)

✔ Secure password protection

✔ Controlled access permissions

The rapid growth of digital data and the increasing reliance on cloud-based storage systems have made secure file storage and sharing a critical concern for individuals and organizations both. With sensitive information being transmitted and stored across various platforms, the risk of data breaches, unauthorized access, and cyberattacks has escalated significantly. Traditional cryptographic methods, while effective to some extent, often face limitations in terms of scalability, computational overhead, and adaptability to modern security challenges. As a result, there is a pressing need for innovative solutions that can provide robust security

without compromising performance. This paper addresses this need by proposing a hybrid cryptography-based approach for secure file storage and sharing, combining the strengths of symmetric and asymmetric encryption techniques.

Traditional storage devices such as flash drives, hard disks and other kinds of physical storage devices are slowly becoming obsolete. The reason for this is that, on the business front, global expansion of companies require data to be shared amongst employees for collaborative working. On the user's personal usage front, many users nowadays have multiple devices, such as one or more mobile/cell phones, tabs, laptops and PCs . Hence cloud storage provides a way to access one's personal data across all of one's personal devices. Hence more and more people are shifting towards the more convenient option of cloud for storing their data. The ability to access files from remote locations using just a stable internet connection gives cloud an edge over other storage options.

How cloud storage works is that it stores the users' confidential files on the storage servers, and users have the freedom of accessing their files from any location. All of a user's devices such as tablets, laptops, mobile phones, desktop PCs and other technology gadgets can be used to store and access files stored on the cloud. Users today have numerous devices. Accordingly, cloud storage provides a secure way to store data and access the data from their own personal devices. Therefore, cloud storage has become one of the most beneficial and efficient methods to store data online. In cloud computing, the user, instead of saving the data at local storage or hard disk, stores data somewhere at a different location, which can be accessed using internet service.

The increasing adoption of cloud computing across various organizations and the IT sector has transformed how data is stored and accessed, offering a cost-effective and efficient solution for managing information. With the rapid shift towards cloud-based services, users can enjoy enhanced data accessibility through the Internet, enabling real -time collaboration and resource sharing. However, this is widespread reliance on cloud technology raises significant is concerns regarding data security and privacy, particularly when sensitive information is entrusted to cloud storage providers, some of which may be perceived as untrustworthy. The primary challenge lies in securely sharing and storing data while ensuring that it is remains protected from potential breaches or unauthorized access in entrusted cloud environments. As organizations migrate to the cloud, the need for robust encryption and decryption techniques becomes paramount.

Cryptography: It is the method of transforming messages into an unreadable format (known as ciphertext) that can only be decrypted into a readable format (known as plain text) by the authorized or intended recipient by using a specific secret key. It converts plaintext into ciphertext using algorithms and keys to ensure confidentiality, integrity, authentication, and non-repudiation. Put differently, it is the practice of developing and using coded algorithms to protect and obscure transmitted information so that it may only be read by those with the permission to decrypt it. Cryptography has become an essential cybersecurity tool for protecting sensitive information from hackers and other cybercriminals. Cybersecurity is the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. The process of transforming plaintext data into ciphertext with the help of an algorithm and an encryption key is called encryption

And the process of transforming ciphertext back into plaintext using the decryption key is called decryption.

Symmetric encryption is a method where the same key is employed for both the encryption and decryption processes. In this approach, the key used to secure the data must be shared between the entities involved in communication. Asymmetric encryption, on the other hand, utilizes a pair of keys - a public key for encryption and a private key for decryption. The public key can be openly distributed, allowing anyone to encrypt messages, while the private key must be kept confidential for decrypting the received messages. It is computationally more intensive compared to symmetric encryption but offers a higher level of security. Hybrid cryptography leverages the efficiency of symmetric encryption for bulk data encryption and the enhanced security of asymmetric encryption for key exchange and authentication. This combination ensures that the system is both secure and efficient, making it suitable for real-world applications. The proposed system in this paper incorporates a combination of symmetric and asymmetric encryption algorithms, including Advanced Encryption Standard (AES) and RSA algorithm. These algorithms ensure that files are securely encrypted before being uploaded to the cloud.

Symmetric encryption algorithms, such as AES (Advanced Encryption Standard), are known for their speed and low computational overhead, while asymmetric encryption algorithms, such as RSA (Rivest-Shamir-Adleman), provide a secure mechanism for key management and distribution. By integrating these two approaches, the proposed system aims to overcome the limitations of standalone cryptographic methods, offering a balanced solution that enhances data security while maintaining optimal performance. This hybrid model is particularly relevant in scenarios involving large-scale file storage and sharing, where both security and efficiency are most important. The solution enables users to encrypt files before they are uploaded to the cloud, thereby safeguarding sensitive information from potential threats.

II.LITERATURE REVIEW

The rapid growth of cloud computing and digital data sharing has significantly increased the need for secure file storage systems. Various researchers have proposed cryptographic techniques and security models to address data confidentiality, integrity, and access control challenges.

Early work by Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography, which laid the foundation for secure key exchange mechanisms. Building upon this, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, which remains one of the most widely used asymmetric encryption techniques for secure communication and key distribution.

Symmetric encryption techniques, particularly the Advanced Encryption Standard, have been extensively studied for efficient data encryption. AES is preferred due to its high speed and strong security, especially when handling large volumes of data. However, symmetric encryption alone suffers from the challenge of secure key distribution.

To overcome these limitations, researchers have explored hybrid cryptographic systems that combine symmetric and asymmetric techniques. Dan Boneh and Victor Shoup highlighted the effectiveness of hybrid encryption in modern cryptographic applications, emphasizing its ability to provide both efficiency and security.

In the context of cloud storage, Seny Kamara and Kristin Lauter proposed cryptographic cloud storage models that ensure data confidentiality even when storage providers are untrusted. Their work demonstrates the importance of

encrypting data before outsourcing it to cloud environments.

Additionally, Cloud Security Alliance has provided guidelines emphasizing encryption, identity management, and secure access control as critical components of cloud security. Similarly, the OWASP Foundation highlights risks such as insecure data storage and insufficient authentication, reinforcing the need for multi-layered security mechanisms.

III. PROBLEM STATEMENT AND OBJECTIVES

A. *Problem Statement*:

In the current digital landscape, cloud-based storage has become the standard for data management there is a high demand for secure sharing and storage mechanisms. Traditional cryptographic methods, while effective in certain contexts, may not provide comprehensive protection. Although these methods are beneficial in terms of security strength and system efficiency, they often fall short in addressing the challenges of modern data storage. Symmetric cryptography, for example, operates at high speeds and is efficient in processing but faces significant challenges in secure key generation and distribution. In contrast, asymmetric cryptography offers a secure key management solution but is inefficient when handling large datasets due to its higher computational cost. Also, organizations using cloud-based infrastructure don't have complete visibility and control over their infrastructure, meaning that they have to rely on security controls provided by their cloud service provider to configure and secure their cloud deployments. Here, data is encrypted by employing a secret key, then both the encoded message and secret key are sent to the recipient for decryption. The leading problem within the symmetric-key cryptographic algorithm is critical distribution since it's just one secret key. The disadvantage is the requirement to stay the key secret - this might be especially challenging where encryption and decryption happen in numerous locations, requiring the key to be moved safely between locations. Furthermore, the rising sophistication of cyber-attacks means that if a single layer of encryption is compromised, the entire dataset is exposed. There is a critical need for a Secure File Storage System that leverages Hybrid Cryptography to combine the computational efficiency of symmetric algorithms with the robust key management of asymmetric algorithms. The challenge lies in designing a system that ensures Confidentiality, Integrity, and Availability (CIA) without compromising system performance or user experience, particularly in environments where data is stored across untrusted third-party servers.

B. *Objectives:*

The primary objective of this paper is to design and evaluate a hybrid cryptography-based system for secure file storage and sharing. The proposed system is designed to address key challenges such as data privacy, integrity, and unauthorized access, while ensuring scalability and ease of implementation.

The paper proposes a comprehensive approach to safeguarding sensitive client information by employing a combination of well-established encryption algorithms. The project focuses on addressing critical need for secure data storage in the rapidly evolving landscape of cloud computing. As organizations increase migrate sensitive information to cloud environments, concerns over data security and privacy have intensified. This project aims to develop a secure file storage system that utilizes cryptographic techniques to protect the data from unauthorized access, ensuring confidentiality, integrity, and the availability.

- To Design a Multi-Layered Security Architecture: Develop a framework that integrates both symmetric and asymmetric cryptographic techniques to eliminate the weaknesses of single-algorithm systems.
- To Optimize Computational Efficiency: Implement Symmetric Encryption (e.g., AES) for the bulk encryption of data files to ensure high-speed processing and minimal latency during upload/download.
- To Enhance Key Management Security: Utilize Asymmetric Encryption (e.g., RSA or ECC) specifically for the secure exchange and storage of the symmetric keys, solving the "key distribution problem."
- To provide user authentication and authorization, ensuring that only permitted users can access specific files.
- To protect the system against common security threats such as Unauthorized access Data breaches Key leakage

IV. PROPOSED SOLUTION

The proposed system is a secure file storage and sharing platform that uses hybrid cryptography (AES + RSA) to ensure confidentiality, integrity, and controlled access to files.

Key Idea

- Use AES (Advanced Encryption Standard) for fast file encryption.
- Use RSA (asymmetric encryption) to securely share the AES key.
- Implement user authorization + OTP/email verification before granting access.

Core Features

1. **User Authentication**
   - Users register/login using email and password.
   - Session-based authentication ensures secure access.
2. **File Encryption & Storage**
   - File is encrypted using a randomly generated AES key.
   - AES key is encrypted using the uploader's RSA public key.
   - Encrypted file and encrypted key are stored separately.
3. **Secure File Sharing**
   - User B requests access to User A's file.
   - User A receives a request (with Allow/Deny option).
   - If approved, an OTP/key is sent securely to User B via email.
4. **Controlled Decryption**
   - User B enters OTP or receives key.
   - AES key is decrypted using RSA private key.
   - File is decrypted and downloaded securely.

***System Architecture* :**

The system follows client-server architecture with secure cryptographic layers.

1. Client Layer

- Web Interface (HTML/CSS/JS)
- Dashboard for:
  - Uploading files
  - Viewing files
  - Sending access requests
  - Entering OTP/key

2. Application Server (Flask Backend)

- Handles:
  - Authentication
  - File processing
  - Encryption/Decryption logic
  - Access control

3. Cryptographic Layer

- **AES**
  - Encrypts file data
- **RSA**
  - Encrypts AES key
  - Decrypts AES key

4. Database (SQLite/MySQL)

Tables:

- users
- files
- access_requests

Stores:

- Metadata (file name, owner)
- Encrypted AES key path
- OTP and request status

5. Storage Layer

- uploads/ → original files
- encrypted_files/ → AES encrypted files
- keys/ → RSA keys & encrypted AES keys

6. Email Service

- Sends:
  - OTP for verification
  - Access approval notifications
  - Decryption key (optional)

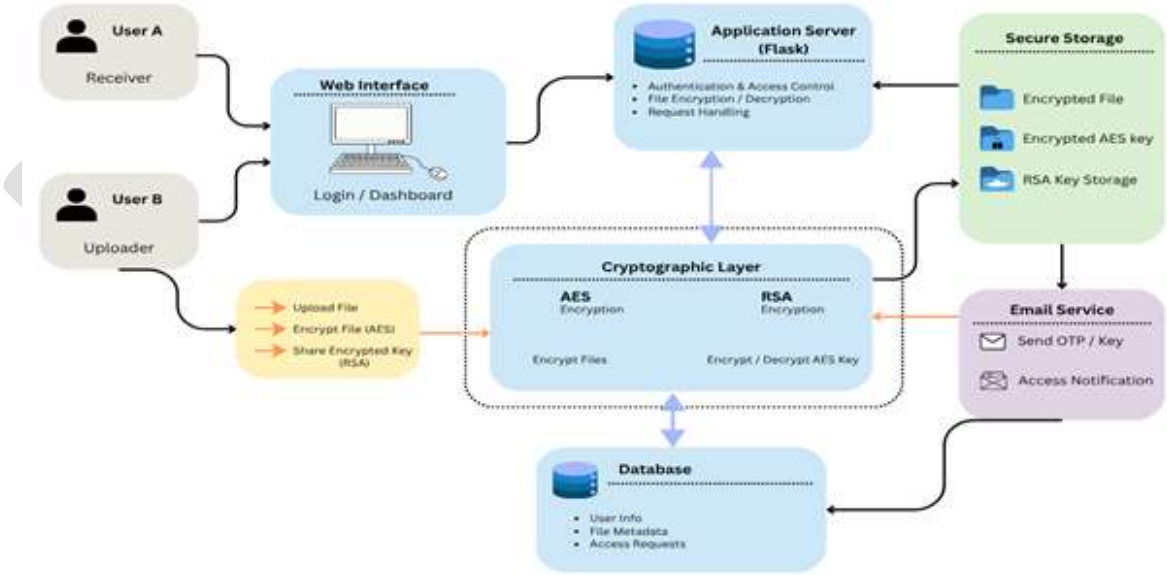

Fig.1: Architecture Diagram

***Methodology* :**

1. User Registration & Key Generation

- **User registers with email.**
- **System generates:**
  - **RSA Public Key**
  - **RSA Private Key**
- Keys are stored securely:
  - Public key → server/database

- Private key → secure storage (or user-controlled)

2. File Upload & Encryption

Steps:

1. User uploads file.
2. System generates random AES key.
3. File is encrypted using AES.
4. AES key is encrypted using RSA public key.
5. Store:
    - Encrypted file → encrypted_files/
    - Encrypted AES key → keys/

Save metadata in database.

3. File Access Request & Authorization

Steps:

1. User B searches User A.
2. User B requests access to file.
3. Entry created in access_requests table.
4. User A receives request:
    - Accept / Reject
5. If accepted:
    - OTP generated
    - OTP sent to User B via email
    - Status updated to "approved"

4. File Decryption & Download

Steps:

1. User B enters OTP.
2. System verifies OTP.
3. Retrieves encrypted AES key.
4. Decrypts AES key using RSA private key.
5. Decrypts file using AES key.

File is sent securely to User B.

Advantages of Proposed System

- Combines **speed (AES)** and **security (RSA)**
- Prevents unauthorized access
- Secure key distribution mechanism
- Scalable and easy to deploy (Flask-based)
- Real-world applicable (cloud storage systems)

V. RESULT AND DISCUSSION

A. Result:

The proposed secure file storage system was successfully implemented using a hybrid cryptographic approach that combines AES (Advanced Encryption Standard) for file encryption and RSA (Rivest–Shamir–Adleman) for secure key exchange.

The system was evaluated based on functionality, security, and performance metrics. The key results obtained are as follows:

1. Data Confidentiality

- All uploaded files were encrypted using AES before storage.
- The AES key was further encrypted using RSA, ensuring that only authorized users with the private key could decrypt it.
- Unauthorized users were unable to access file content even if they gained access to storage.

2. Secure File Sharing

- A user-based access control mechanism was implemented.
- File access requests required approval from the file owner.

- Upon approval, a secure key (via OTP/email) was sent to the requester.
- This ensured controlled and traceable file sharing.

3. Authentication and Authorization

- Users were authenticated through login credentials.
- Additional OTP-based verification added a second layer of security.
- Access control ensured only approved users could decrypt files.

4. System Performance

- AES encryption showed fast processing time for large files.
- RSA encryption was used only for small-sized AES keys, minimizing computational overhead.
- The system demonstrated efficient performance with minimal delay during upload and download operations.

B. Discussion:

The results indicate that the hybrid cryptographic approach significantly enhances the security and efficiency of file storage systems.

1. Effectiveness of Hybrid Cryptography

The combination of AES and RSA proved to be highly effective:

- AES ensured fast and efficient encryption of large data.
- RSA provided secure key distribution.
- This hybrid model overcame the limitations of using symmetric or asymmetric encryption alone.

2. Security Strength

- The system ensures end-to-end data protection.
- Even if encrypted files are intercepted, they cannot be decrypted without the RSA private key.
- OTP-based access adds an additional security layer against unauthorized access.

3. User-Centric Access Control

- The approval-based file sharing mechanism gives full control to file owners.
- This improves trust and prevents unauthorized data exposure.
- Email-based key sharing ensures secure delivery of decryption credentials.

4. Performance Trade-offs

- While RSA is computationally expensive, its usage was minimized by encrypting only AES keys.
- This resulted in a balanced system with both high security and good performance.
- Slight delays were observed during key generation and encryption, but they were acceptable within practical limits.

5. Practical Applicability

- The system can be applied in:
  - Cloud storage systems
  - Enterprise data sharing platforms
  - Academic and research data repositories
- It is scalable and can be extended with additional features such as:
  - Blockchain-based access logs
  - Multi-factor authentication

- Role-based access control

6. Limitations

- Dependence on email services for OTP delivery may introduce delays.
- Key management can become complex as the number of users increases.
- The system currently does not implement advanced intrusion detection mechanisms.

7. Future Improvements

- Integration of biometric authentication.
- Use of decentralized storage systems.
- Implementation of automated key rotation policies.
- Enhancing UI/UX for better usability.

VI. CONCLUSION

This research presented the design and implementation of a Secure File Storage System using Hybrid Cryptography, combining the strengths of symmetric and asymmetric encryption techniques to ensure robust data protection. The system effectively utilizes AES encryption for securing file contents and RSA encryption for safe key exchange, thereby overcoming the limitations of using either technique independently.The proposed system successfully achieves key security objectives such as data confidentiality, secure key management, controlled file sharing, and user authentication. The integration of OTP-based verification and user approval mechanisms further enhances access control, ensuring that only authorized users can access sensitive data.Experimental results demonstrate that the system maintains a balance between high security and efficient performance. AES enables fast encryption of large files, while RSA ensures secure transmission of encryption keys with minimal overhead. The modular architecture of the system also makes it scalable and adaptable for real-world applications such as cloud storage, enterprise systems, and secure data sharing platforms.

Despite its effectiveness, certain limitations such as dependency on email-based OTP delivery and increasing complexity in key management were identified. These can be addressed in future work by incorporating advanced techniques like multi-factor authentication, automated key management, and decentralized storage solutions. In conclusion, the proposed hybrid cryptographic model provides a reliable, secure, and practical solution for modern file storage challenges, making it highly suitable for applications requiring strong data security and controlled access.

REFERENCES

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

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

[3] NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, National Institute of Standards and Technology, 2001.

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[5] M. Bellare and P. Rogaway, “Introduction to Modern Cryptography,” 2005.

[6] K. Zhao and X. Ge, “A Survey on the Internet of Things Security,” Proceedings of the 9th International Conference on Computational Intelligence and Security, 2013.

[7] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” IEEE Second International Conference on Cloud Computing Technology and Science, 2010.

[8] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing,” 2017.

[9] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2020.

[10] M. Green and M. Smith, “The Cryptopals Crypto Challenges,” 2016. [Online]. Available: https://cryptopals.com

[11] OWASP Foundation, “Top 10 Web Application Security Risks,” 2021. [Online]. Available: https://owasp.org

[12] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Financial Cryptography and Data Security, 2010.

[13] N. Tiwari, D. Goyal, and N. Hemrajani, “A hybrid method for image watermarking,” International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[14] V. Singh, M. Choubisa, G. K. Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering Management, vol. 83, pp. 30561-30565, May-June 2020.

[15] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 277-280, 2023.

[16] A. Maheshwari, R. Ajmera and D. K. Dharamdasani, "Unmasking Embedded Text: A Deep Dive into Scene Image Analysis," 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), pp. 1403-1408, 2023.

[17] N. Tiwari, N. Hemrajamani, D. Goyal, "Improved digital image watermarking algorithm based on hybrid DWT-FFT and SVD techniques", Indian Journal of Science and Technology, Vol. 10, Issue. 3, pp. 1-7, 2017.

[18] A. Maheshwari, R. Ajmera and D. K. Dharamdasani, "Unmasking Embedded Text: A Deep Dive into Scene Image Analysis," 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), pp. 1403-1408, 2023.

[19] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[20] M. K. Ramaiya, D. Goyal, N. Hemrajani, "Improved Image Steganographic System by using Multiple Encryption and DWT", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 6, Issue. 8, 2017.

[21] Y. P. Singh, Dr. S. Soni, "Secure Image Encryption Using RSA Algorithm and Arnold Transformation", International

Journal of Global Research in Science and Technology (IJGRST) Vol. 10, pp. 8-12, 2025.

[22] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, Vol. 141, pp. 483-492, 2020.

[23] T. Saini, T. K. Gupta, A. Shukla, K. Paliwal, "Image Security Using Cryptography and Steganography: A Comprehensive Review and Hybrid Approach", International Journal of Global Research in Science and Technology (IJGRST) Vol. 10, pp. 231-235, 2025.

[24] G. K. Soni, H. Arora, B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[25] P. Jha, K. K. Sharma, B. Jain, V. Sharma, "Digital Image Encryption Using AES Algorithm", EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR), Vol. 4, Issue. 2, 2019.