Triple Cipher Security System Using Image Steganography in Cloud

Dr. M K Sandhya[1], Ameenath Fahmida D M[2], Swathi Priya S G[3], Swetha P[4]
[1]*Professor, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai-24*
[2,3,4]*Student, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai-24*

***Abstract*— In response to the escalating concerns surrounding data security breaches and privacy infringements within cloud environments, this paper presents a pioneering security paradigm that presents triple cipher encryption and image steganography techniques. It embodies a comprehensive approach, underpinned by a suite of pivotal security measures. These include the integration of Google authentication, user registration protocols, file encryption mechanisms. Central to the system's efficacy is the intricate triple cipher encryption methodology, comprising initial substitution encryption, AES and RSA encryption layers. This encryption cascade not only fortifies the confidentiality of sensitive data but also erects barriers against unauthorized access attempts. Moreover, the seamless incorporation of image steganography augments confidentiality measures by enabling the embedding of encrypted files within seemingly innocuous images. By offering a comprehensive solution that encompasses encryption, steganography, and authentication mechanisms, our system represents a significant advancement in the field of cloud security. Its applications extend to various sectors, including but not limited to military, finance, government and healthcare where safeguarding sensitive data is paramount. Overall, our research contributes towards establishing a more secure and reliable environment for storing and managing data in the cloud.**

Index Terms*— *Cloud security, triple cipher encryption, image steganography, Google authentication, file encryption, secure storage, AES, RSA.

I. INTRODUCTION

Cloud computing has revolutionized data storage and processing, offering scalability, flexibility, and cost-efficiency to both businesses and individuals. While it allows organizations to focus on innovation by outsourcing infrastructure management, concerns about data security and privacy have grown. The rise in data breaches and unauthorized access highlights vulnerabilities in cloud systems. This work aims to address these concerns by proposing a robust security system. Our approach combines triple cipher encryption with image steganography to offer multi-layered protection against breaches. We strive to enhance cloud security, ensuring data integrity and confidentiality while building trust in the cloud ecosystem.

II. PROBLEM STATEMENT

The reliance on remote servers for data storage and processing in cloud services raises significant concerns about data security and privacy. Despite security measures by cloud providers, data breaches and unauthorized access remain risks. Managing data across multiple cloud platforms complicates matters, increasing concerns about data sovereignty and regulatory compliance. Ensuring data confidentiality and integrity amid cyber threats and regulations is a major concern. This approach using triple cipher encryption and image steganography strives to improve data security in the cloud.

III. LITERATURE SURVEY

1. ‘A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network’ Harshit Sharma et al., (2023 IEEE)

The paper thoroughly examines hybrid cryptographic algorithms in cloud networks, evaluating their effectiveness, performance metrics, and limitations. It highlights authentication protocols, implementation strategies, and encryption/decryption efficiency. While it outlines the current state of hybrid cryptographic algorithms, it also identifies research gaps, particularly in authentication mechanisms for cloud environments. The paper stresses the importance of practical implementation and seamless integration for cryptographic solutions in cloud networks.

2. ‘Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment’ Sherief H. Murad et al., (2021 Procedia Computer Science)

The study examines cryptographic schemes in cloud computing, comparing two-tier and three-tier hybrid models using AES and RSA algorithms. It evaluates their efficiency in encryption time, decryption time, throughput, and security. The research also explores challenges in deploying these schemes, focusing on computational overhead, scalability, and interoperability. Through experiments, the study offers insights into the pros and cons of different cryptographic models and aims to enhance understanding and future research in cloud security.

3. ‘Hybrid Cryptography Algorithm for Secure and Low Cost Communication’ Suman Kalyan Ghosh et al., (2020 IEEE)

This hybrid cryptography algorithm combines Diffie-Hellman and RSA to ensure secure message encryption, especially in open networks like the internet. Compared to conventional RSA, the study shows this system is cost-effective and efficient for data transmission. The research delves into the hybrid approach, explaining its mechanisms and benefits over traditional methods. Using both Diffie-Hellman and RSA, it boosts security and reduces vulnerabilities of single methods. Through performance tests and comparisons, the study validates its effectiveness in real-world open network scenarios where security is crucial. This integration showcases potential for advancing cryptography, paving the way for stronger security solutions in modern computing.

4. ‘A New Cryptography Algorithm Based on ASCII code’ Ahmed Elmogy et al., (2019 IEEE)

The paper introduces a novel symmetric cryptography algorithm based on ASCII code manipulation. In this method, each character is linked to its previous one during encryption and decryption. The characters are encrypted within a set ASCII range, enhancing system security. By improving data security with new encryption techniques, the study addresses modern cybersecurity issues and promotes advancements in cryptography.

5. ‘Steganography: Double Encrypted Image Deployed In Cloud’ Ridhima Ahluwalia et al., (2020 IEEE)

The paper introduces a steganography method that hides encrypted data in images using discrete cosine transformation (DCT), RSA encryption, and Arnold transform. This approach focuses on making the hidden data undetectable to humans while preserving image quality. It employs strong security measures like RSA encryption and the Arnold transform to resist decryption by hackers. Users can securely store these encrypted images in the cloud for remote access. However, altering the image's statistics could be detected by specialized software, potentially exposing the hidden data. The method's complexity and the need to renew access tokens for cloud-stored images are also challenges. Still, the technique excels in combining security, invisibility, and convenience.

6. ‘Hybrid Cryptography for Secure File Storage’ Chivukula Susmitha et al., (2023 IEEE)

The paper emphasizes data security's crucial role in today's digital world, highlighting hybrid cryptography as a key method for ensuring data privacy, availability, and integrity. Hybrid cryptography blends symmetric and public-key encryption for added security. It addresses the security risks of relying on cloud storage for extensive data and explores encryption algorithms like RSA, DES, and Blowfish, noting their strengths and weaknesses. RSA uses large integer factoring for security, while Blowfish faces challenges with key distribution and speed. Elliptic Curve Cryptography (ECC) stands out for its efficiency and security advantages.

IV. EXISTING SYSTEM

Many file storage systems lack strong encryption, making sensitive data vulnerable to unauthorized access. They often use basic username/password authentication, which can be easily breached. This weak security increases the risk of data breaches and regulatory issues. Additionally, most systems don't use steganography, missing an extra security layer. Improved security measures, including robust encryption and steganography, are urgently needed to address these vulnerabilities and prevent data breaches.

V. PROPOSED SYSTEM

The proposed system addresses the limitations of current file storage by offering an advanced security solution that integrates encryption, steganography, and robust access controls. Unlike many existing systems that rely on weak encryption and basic authentication, this system employs multi-layer encryption methods, including substitution, AES, and RSA, ensuring both data confidentiality and integrity. With the inclusion of steganography, encrypted files can be covertly stored within images, further enhancing security. Instead of storing the original files directly, only encrypted images are uploaded to the cloud, minimizing the risk of unauthorized access. User authentication is streamlined by using Google account credentials, making registration simpler and access more secure. Overall, this approach provides a comprehensive solution to the security challenges faced by current file storage systems, improving data confidentiality, integrity, and availability while reducing the risks of unauthorized access and data breaches.

VI. METHODOLOGIES USED

- Initial Substitution Encryption

The initial substitution encryption algorithm utilizes a key generation process within the range [32, 126), excluding 94.It involves iterating through each character of the plaintext, shifting its ASCII value by the generated key, and adjusting it within the printable ASCII range [32, 126]. The simplicity in calculation reduces the computational overhead. Moreover, by constraining the encrypted characters within the printable ASCII range, the algorithm maintains compatibility with text-based systems while preventing encoding errors. Its dynamic key generation process enhances security against brute force attacks, contributing to its resilience against known-plaintext attacks.

Encryption

$$cipher\ text = \big((ASCII\ value\ of\ character + key - 32)\ \%94\big) + 32 \quad (1)$$

Decryption

$$plain\ text = \big((ASCII\ value\ of\ character - key - 32)\ \%94\big) + 32 \quad (2)$$

- AES (ADVANCED ENCRYPTION STANDARD)

AES is a popular symmetric encryption algorithm known for its strong security and efficiency. It provides robust data encryption and decryption, guarding against unauthorized access AES is widely used in securing communications, protecting stored data, and maintaining data. Its dependability and flexibility make it essential for modern cryptographic protocols and data protection.

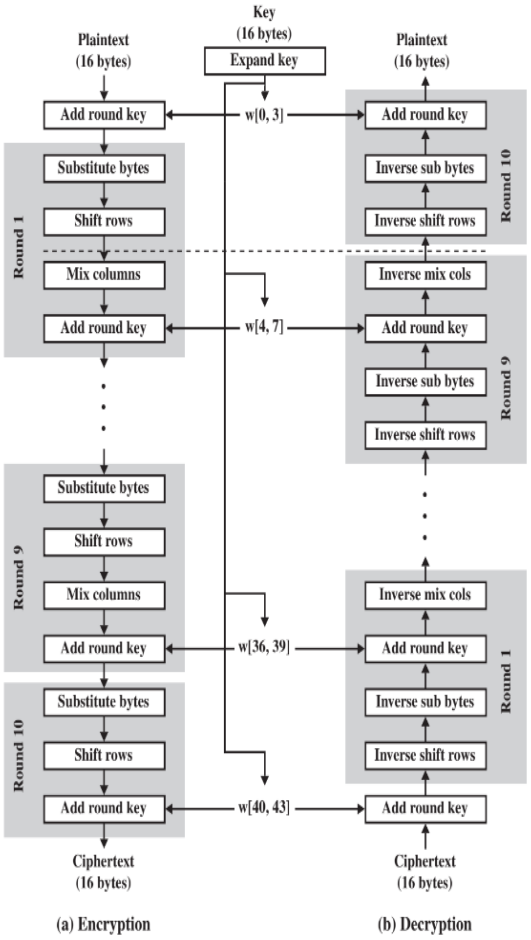


Fig.1 AES

- RSA

RSA is a popular asymmetric encryption algorithm known for its security and flexibility. It uses a public-private key pair based on the challenge of factoring large prime numbers. Its benefits encompass strong encryption, digital signatures, and key exchange. RSA is essential for secure communication, digital signatures, authentication, and key management.

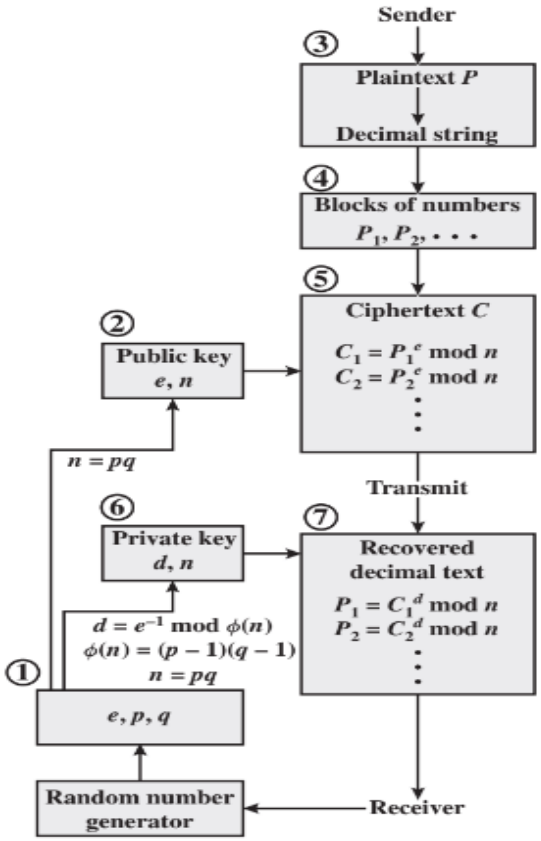


Fig 2. RSA

- IMAGE STEGANOGRAPHY

Image steganography hides secret messages or data in digital images without changing their appearance. By adjusting pixel values or metadata, text or data can be hidden invisibly. This method helps securely transmit sensitive information, staying hidden from unintended viewers. It's used in data encryption to maintain confidentiality and integrity.

VII. MODULE DESCRIPTION

- User Registration And Authentication

Users sign up using Google credentials for secure access to the cloud drive. Each user generates a unique encryption key during registration for encrypting files.

- File Upload And Encryption

Files undergo a three-step encryption process: initial substitution encryption, RSA encryption of the AES key with the user's public key, and AES encryption using the encrypted AES key. The encrypted file is then hidden in an image using steganography for added protection.

- File Retrieval And Decryption

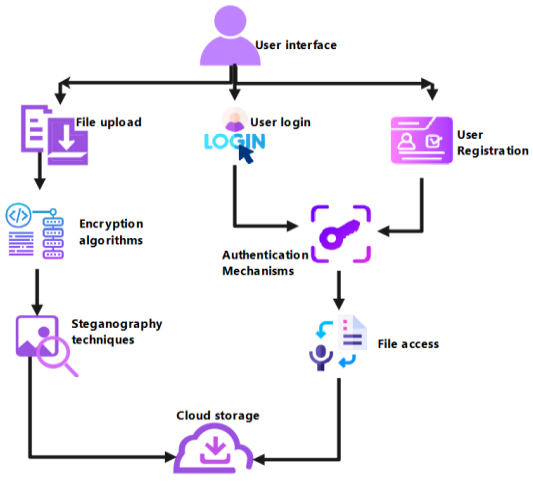
To decrypt, the steganographic image is first retrieved, followed by RSA decryption of the AES key with the user's private key. Then, AES decryption using the decrypted AES key and reversing the initial substitution algorithm recovers the file. This ensures secure data retrieval by reversing encryption steps with the correct keys.

- Secure Storage And Access

The encrypted steganographic files are stored. This conceals sensitive data from unauthorized users. Users need the decryption key to securely access and decrypt their files.

VIII. SYSTEM ARCHITECTURE

It integrates encryption and steganography for secure file storage. Users authenticate via Google and input a secret key. Files are encrypted before uploading to the cloud for confidentiality. Steganography embeds data within images, which are the only files stored in the cloud. This enhances security and restricts unauthorized access.



IX. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, the proposed system effectively addresses security concerns in existing file storage systems. Through encryption, steganography, and access control, it ensures data confidentiality, integrity, and availability in the cloud. Only the

encrypted stego image is stored, not the original file. Enhancing encryption and steganography can bolster the system's cyber threat resilience. Future work could focus on scalability and compatibility with other cloud platforms.

REFERENCE

[1] H. Sharma, R. Kumar and M. Gupta, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-5

[2] Murad, S. H., & Rahouma, K. H. (2021). Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. Procedia Computer Science, 194, 165–172.

[3] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra and S. Biswas, "Hybrid Cryptography Algorithm For Secure And Low Cost Communication," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-5

[4] A. Elmogy, Y. Bouteraa, R. Alshabanat and W. Alghaslan, "A New Cryptography Algorithm Based on ASCII Code," 2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Sousse, Tunisia, 2019, pp. 626-631.

[5] R. Ahluwalia, A. Gupta and P. Chaudhary, "Steganography: Double Encrypted Image Deployed In Cloud," 2020 International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 2020, pp. 519-525.

[6] C. Susmitha, S. Srineeharika, K. S. Laasya, S. K. Kannaiah and S. Bulla, "Hybrid Cryptography for Secure File Storage," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1151-1156.

[7] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in IEEE Access, vol. 9, pp. 31805-31815, 2021.

[8] Anushka and A. Saxena, "Digital image watermarking using least significant bit and discrete cosine transformation," 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India, 2017, pp. 1582-1586.

[9] Uttam Kumar,Mr. Jay Prakash, "Secure File Storage On Cloud Using Hybrid Cryptography Algorithm", 2020 International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.8, Issue 7, pp.334-340.