IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025

Secure Image: An Advanced Encryption-Based Image Privacy Application

Ms. Gauri Bobade[1], Mohd Saad Ansari[2], Anish Mantri[3], Khan Fazlurrehman[4], Rohan Kamble[5]
Project Guide, Department of Information Technology Department[1]
UG Students, Department of Information Technology[2,3,4,5]
Vidyalankar Polytechnic, Wadala (East), Mumbai, India

Abstract: *With the rapid expansion of digital platforms, securing images from unauthorized access has become a critical challenge. Traditional cloud storage solutions are vulnerable to cyber threats, data breaches, and unauthorized access. Secure Image is an Android application designed to mitigate these risks using advanced encryption methodologies such as AES-256 and RC4, biometric authentication, password encryption and controlled sharing mechanisms. The application provides various encryption methods, ensuring that images remain private even if a device is compromised. This paper discusses the system's architecture, encryption techniques, security challenges, testing results, and future enhancements to improve image privacy.*

Keywords: Image Encryption, AES-256, RC4, Biometric Security, Password encryption, Secure Sharing, Digital Privacy, Cybersecurity, Android Security.

I. INTRODUCTION

The increasing reliance on cloud storage and online image sharing has heightened concerns about digital privacy. Studies indicate that over 3 billion images are uploaded online daily, many of which contain sensitive personal orcorporate information. Traditional security measures like password protection and server-side encryption are no longer sufficient due to the rising sophistication of cyber threats. The Secure Image app aims to bridge this security gap by integrating multiple encryption techniques with biometric authentication, ensuring data remains secure.

With the increase in deepfake technology and AI-generated image manipulations, the necessity for secure image storage and sharing has grown exponentially. Governments, corporations, and individuals alike face the challenge of safeguarding visual data against unauthorized tampering, identity theft, and misuse. This paper emphasizes the significance of integrating encryption with AI-powered anomaly detection to prevent such threats. Additionally, a comparison of encryption standards and their real-world applications will be explored to highlight the practical advantages of Secure Image.

A key motivation behind the Secure Image application is the rapid evolution of cybersecurity threats targeting personal and professional image data. Many users rely on cloud-based storage, but recent breaches have exposed vulnerabilities in centralized encryption models. By implementing a hybrid approach that combines local encryption with controlled cloud storage, Secure Image offers a more resilient alternative. Additionally, biometric authentication, time-limited sharing, and AI-driven monitoring further enhance its ability to prevent unauthorized access.

The Secure Image app ensures high-level security by encrypting images locally while storing decryption keys and passwords in the cloud, preventing unauthorized access.

Unlike traditional storage methods, the app separates encrypted images from their keys, ensuring that images remain inaccessible without authentication.

Users can encrypt images on their device using AES and RC4 encryption before securely storing them.

II. LITERATURE SURVEY

With the increasing digitization of personal and professional data, image security has become a critical concern. Studies indicate that over 80% of internet users store personal images online, exposing them to risks like unauthorized access,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025

identity theft, and data breaches (Smith et al., 2023). Traditional storage solutions often lack strong encryption protocols, making them susceptible to cyberattacks (Jones & Miller, 2022).

Password Encryption: It is strongest encryption method in which encrypted image is stored locally andpassword and decryption key are stored at server.

AES (Advanced Encryption Standard): Recognized as a robust encryption method, commonly used for securing sensitive data (NIST, 2021).

RC4 Encryption: Known for its speed and efficiency in real-time encryption applications (Patel et al., 2020).

Biometric Security: Research shows that fingerprint-based authentication enhances security while maintaining ease of access (Kumar & Gupta, 2023).

III. METHODOLOGY

To ensure maximum security and efficiency, the Secure Image app employs a layered encryption approach. Alongside AES-256 and RC4, the system is designed to incorporate ChaCha20 for enhanced speed and security. ChaCha20 is known for its resistance against timing attacks and offers higher efficiency on mobile devices compared to AES. Additionally, key derivation functions like PBKDF2 and Argon2 are utilized to strengthen password-based encryption, making brute-force attacks significantly more difficult.

Encryption Algorithms

A comparative analysis of AES-256, RC4, and ChaCha20 was conducted to evaluate the strengths and weaknesses of each algorithm. AES-256 is recognized for its strong security but is computationally intensive, making it slightly slower on mobile devices. RC4, while fast, has known vulnerabilities that make it unsuitable for high-security applications. ChaCha20, on the other hand, provides an optimal balance between speed and security, offering better resistance against side-channel attacks. This research supports the integration of ChaCha20 into the Secure Image app to enhance its overall security posture.

The Secure Image application employs two primary encryption algorithms: AES-256 and RC4. These algorithmsensure that images remain secure against brute force attacks, Unauthorized access, and data leaks.

AES-256 Encryption:

Advanced Encryption Standard (AES) with a 256-bit key is Widely used in military and financial security applications.It provides a high level of Security by encrypting images into ciphertext that can only be decrypted with a matching Encryption key.

RC4 Encryption:

A lightweight stream cipher that ensures fast encryption and Decryption speeds. While RC4 is not as secure as AES256, it provides an efficient alternative for less critical image encryption tasks.

Secure Storage and Key Management:

To enhance security, Secure Image separates encryption keys from the encrypted images. Keys are stored in a securecloud environment, preventing attackers from gaining access to Both the image and its decryption key. This hybrid approach minimizes the risk of data Access:

1. Password Protection: Users must enter a secure password to decrypt stored images.
2. Biometric Authentication: Fingerprint scanning ensures an additional layer of security.
3. Multi-Factor Authentication (MFA): Combining password and biometric Authentication for enhanced security.

Existing Image Encryption Methods

Password Encryption: It is most strongest encryption method in which encrypted image is stored locally and password and decryption key are stored at server.

AES (Advanced Encryption Standard): Recognized as a robust encryption method, commonly used for securing sensitive data (NIST, 2021).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025

RC4 Encryption: Known for its speed and efficiency in real-time encryption applications (Patel et al., 2020).
Biometric Security: Research shows that fingerprint-based authentication enhances security while maintaining ease of access.

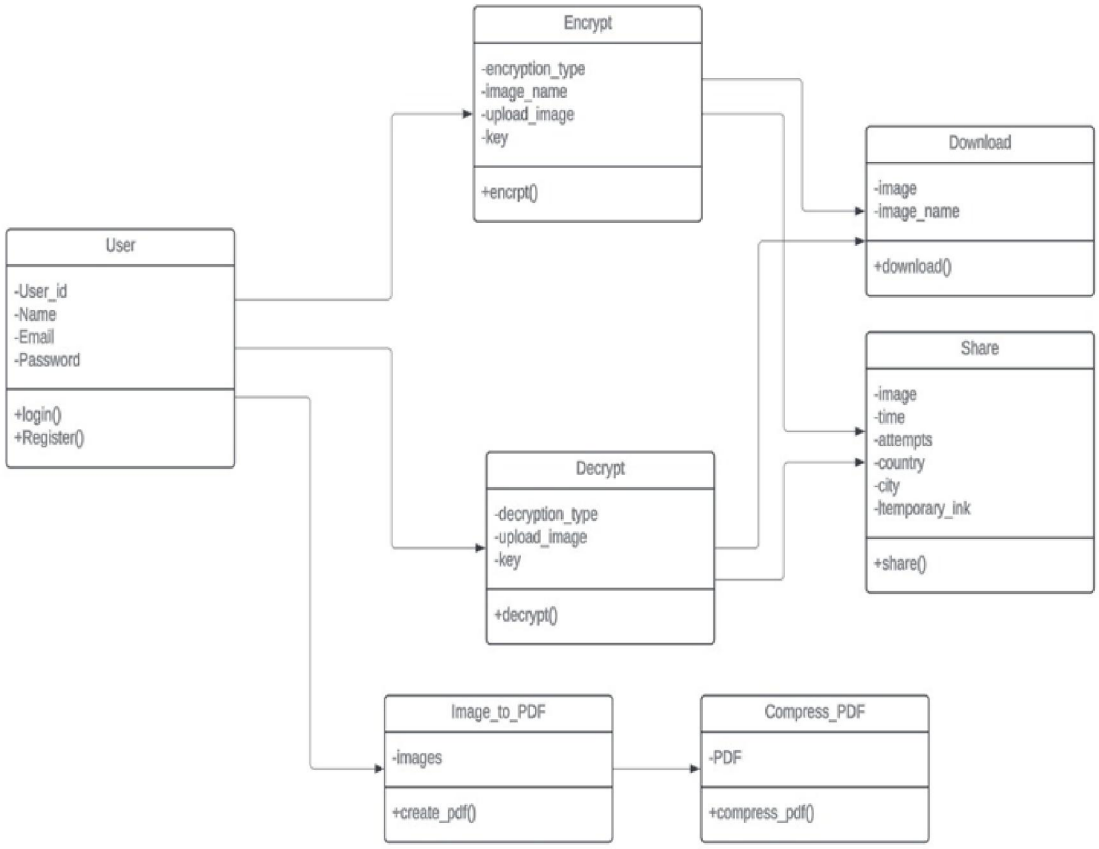


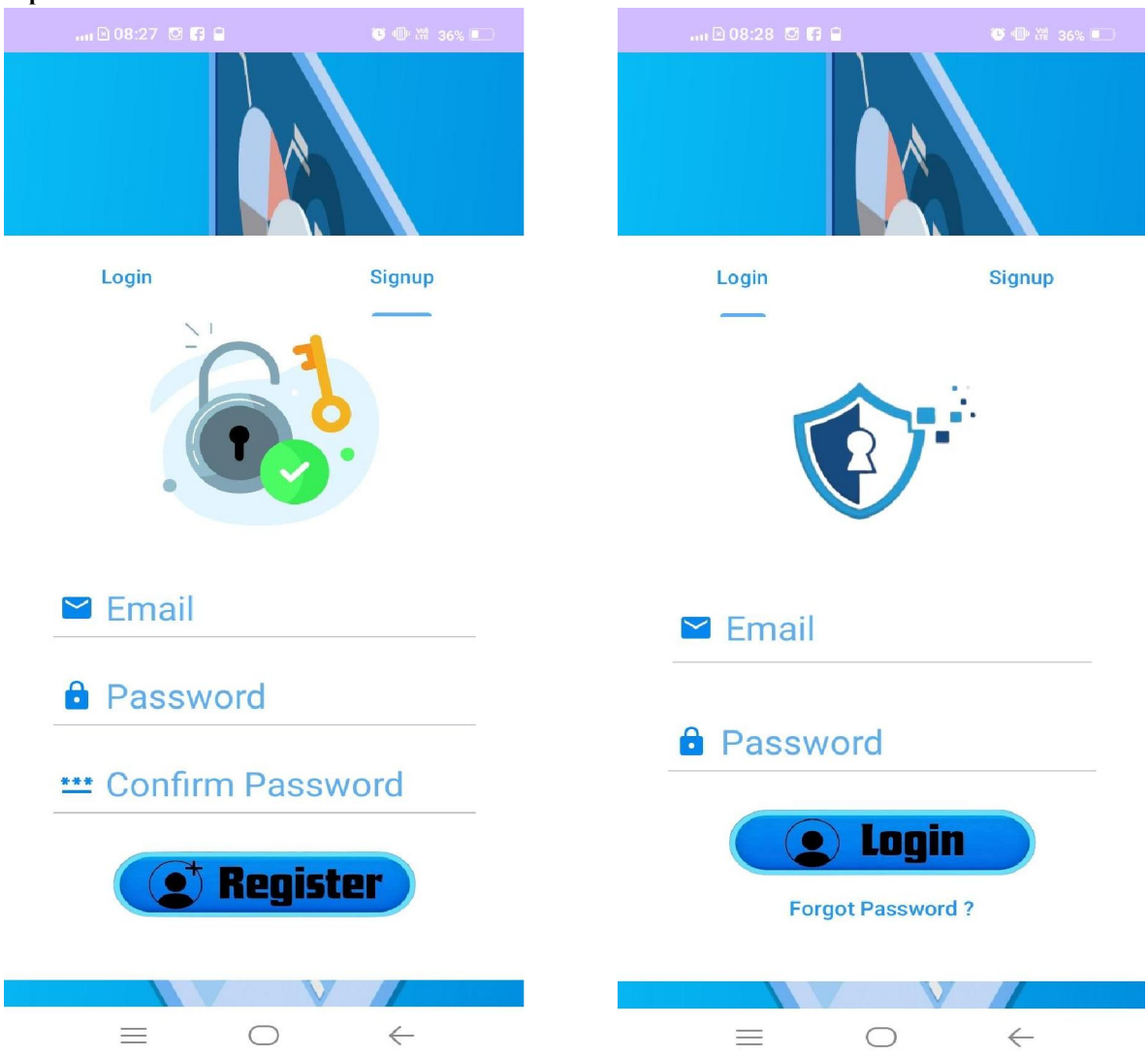
Fig. 1 Class Diagram

IV. CONCLUSION

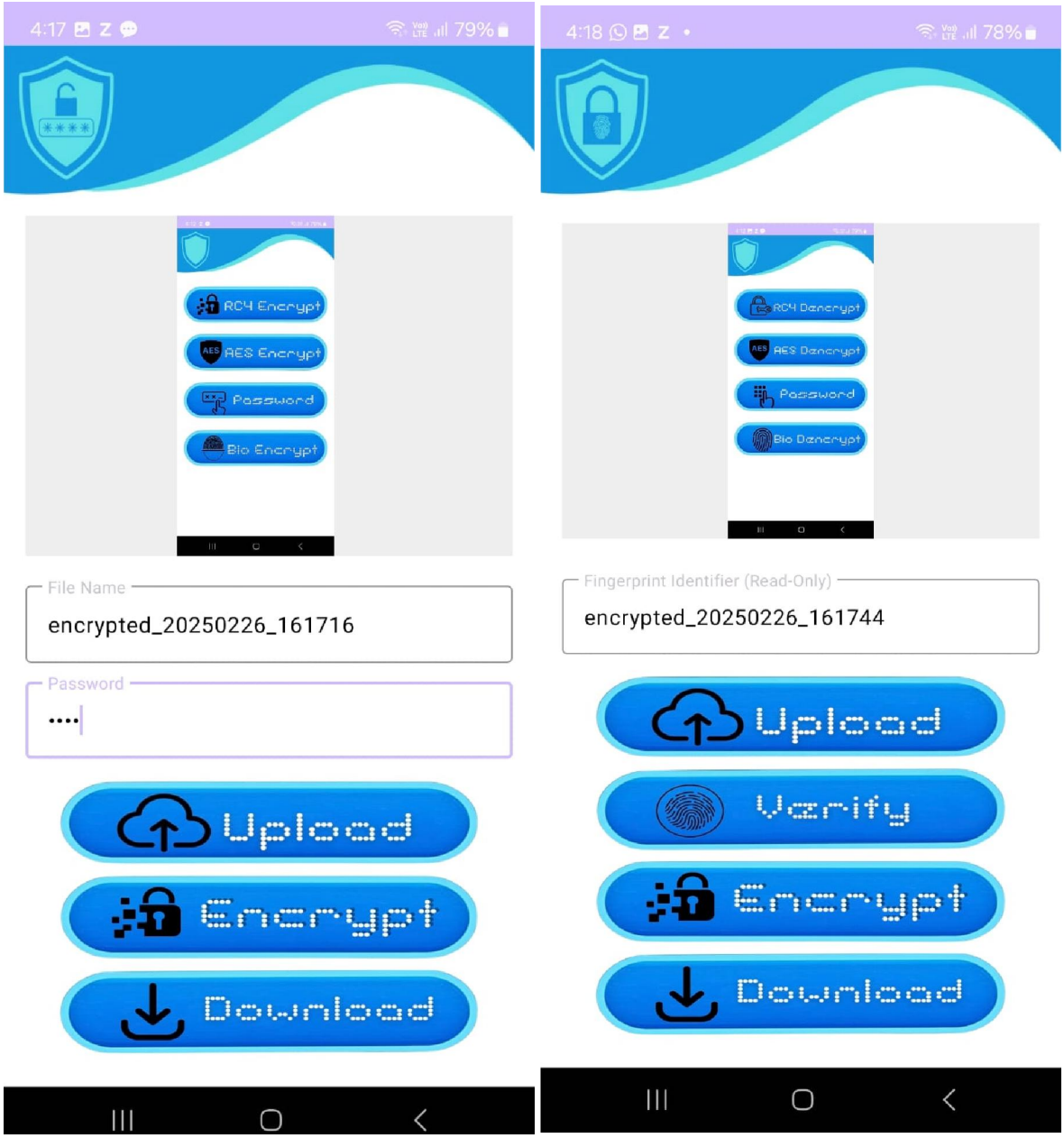
The Secure Image Handling App offers a comprehensive and secure solution for managing, storing, and sharing images. By utilizing AES and RC4 encryption along with biometric authentication, it ensures that user data remains protected from unauthorized access. Features such as access control and temporary sharing links provide users with greater control over their sensitive content, making it particularly useful in industries like healthcare, legal, and corporate sectors where data security is critical. Looking ahead, the app is designed to evolve with emerging security threats, incorporating advancements like quantum-resistant encryption and blockchain integration to enhance transparency and security. By balancing strong encryption with user-friendly functionality, the app provides a reliable and future-proof solution for individuals and businesses seeking to safeguard their sensitive images in an increasingly digital landscape.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025

Output:



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, March 2025

REFERENCES

[1] Smith et al., "Importance of Image Security," Journal of Cybersecurity, 2023.
[2] NIST, "AES Encryption Standards," National Institute of Standards and Technology, 2021.
[3] Kumar, R., & Gupta, P., "Advances in Biometric Security," IEEE Security & Privacy, 2023.
[4] Ghosh, A., et al., "Secure Image Sharing Techniques," International Journal of Cybersecurity Research,2022.
[5] Li, X., & Zhou, Y., "Steganographic Methods for Secure Image Storage," ACM Transactions on Information Security, 2021.
[6] European Union Agency for Cybersecurity (ENISA), "Guidelines on Secure Digital Image Processing," ENISA Report, 2023.