iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79319

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

IntelCrypt: Data Vault with Customizable Encryption Techniques

Aniket L. Davane[1], Aarya K. Patil[2], Ayush S. Patil[3], Mihir A. Shigavn[4], Prof. Raees Ahmed[5]
Department of Computer Engineering, Theem College of Engineering, University of Mumbai, India

Abstract: ***Secure communication is a fundamental requirement in modern digital systems due to the increasing number of cyber threats and privacy concerns. This paper presents IntelCrypt, a secure messaging platform designed to provide enhanced data protection through multiple security mechanisms. The system integrates End-to-End Encryption (E2EE), biometric authentication, and image steganography to ensure confidentiality, integrity, and secure communication. A hybrid cryptographic model using AES-256-GCM and RSA-2048 is implemented to provide strong encryption and efficient key exchange. In addition, Least Significant Bit (LSB) steganography is used to hide encrypted messages within digital images, enabling covert communication without noticeable visual distortion. The system architecture is implemented using Flutter for the frontend and Spring Boot for the backend, following a clean and scalable architecture. Experimental implementation demonstrates improved security and performance for high-security communication environments.***

Index Terms: End-to-End Encryption, Secure Messaging, Steganography, Biometric Authentication, Cryptography.

I. INTRODUCTION

The rapid growth of digital communication technologies has significantly increased the need for secure messaging systems. Traditional messaging platforms often face security challenges such as data interception, unauthorized access, and privacy breaches. These vulnerabilities highlight the need for advanced security mechanisms that ensure the confidentiality and integrity of transmitted data.

To address these challenges, this research proposes IntelCrypt, a secure messaging system that integrates encryption, biometric authentication, and steganography. The objective of the system is to provide a robust communication platform capable of protecting sensitive information from potential cyber threats.

The system follows a multi-layered security approach known as Defense in Depth, where multiple security mechanisms operate together to protect the communication channel.

II. SYSTEM ARCHITECTURE

IntelCrypt follows a Clean Architecture model that separates system components into different layers, improving scalability and maintainability.

A. Frontend Implementation

The mobile application is developed using Flutter, which allows cross-platform deployment on Android and iOS devices. State management is implemented using Riverpod, which provides reactive and testable application logic.

Sensitive data such as authentication tokens and cryptographic keys are stored using secure storage integrated with device-level security features such as Android Keystore and iOS Keychain. Additional security features implemented in the frontend include biometric authentication, automatic session locking after inactivity, and password strength analysis.

B. Backend Implementation

The backend system is implemented using Spring Boot with Java. Authentication and authorization are handled using Spring Security and JSON Web Tokens (JWT). This enables stateless authentication and secure communication between the client and server.

The system uses an H2 database during development and PostgreSQL for production deployment. Secure logging and monitoring mechanisms are implemented to maintain audit records of sensitive operations.

©IJRASET: All Rights are Reserved

III. CRYPTOGRAPHIC FRAMEWORK

IntelCrypt employs a hybrid encryption model combining symmetric and asymmetric cryptographic algorithms.The system uses AES-256-GCM to encrypt message content because of its strong security and high performance. For secure key exchange between communicating users, RSA-2048 encryption is used.

In this hybrid approach, a unique AES session key is generated for each communication session. The message is encrypted using AES encryption, and the AES session key is encrypted using RSA before transmission. This approach combines the efficiency of symmetric encryption with the security advantages of asymmetric encryption.

IV. STEGANOGRAPHY MODULE

To further enhance privacy, IntelCrypt integrates an image steganography module that hides encrypted messages within digital images.

The system uses the Least Significant Bit (LSB) encoding technique to embed encrypted data into image pixels. Because only the least significant bits of pixel values are modified, the visual quality of the image remains almost unchanged.

This approach allows encrypted communication to be hidden within ordinary image files, providing an additional layer of security through covert communication

V. SECURITY MODEL

IntelCrypt follows a Defense-in-Depth security strategy, where multiple security layers protect sensitive information.

At the transport layer, secure communication channels use TLS protocols to prevent interception and tampering. At the authentication layer, the system implements multi-factor authentication using password verification and biometric authentication.

At the application layer, the system prevents plaintext storage of sensitive data and includes additional protections such as screenshot detection and self-destructing messages.

VI. IMPLEMENTATION RESULTS

The IntelCrypt project has currently achieved approximately 82% completion of planned features. The backend codebase consists of nearly 15,000 lines of code, while the Flutter frontend contains approximately 5,000 lines of code.

Initial testing demonstrates that the system successfully encrypts, hides, transmits, and decrypts secure messages with minimal performance overhead.

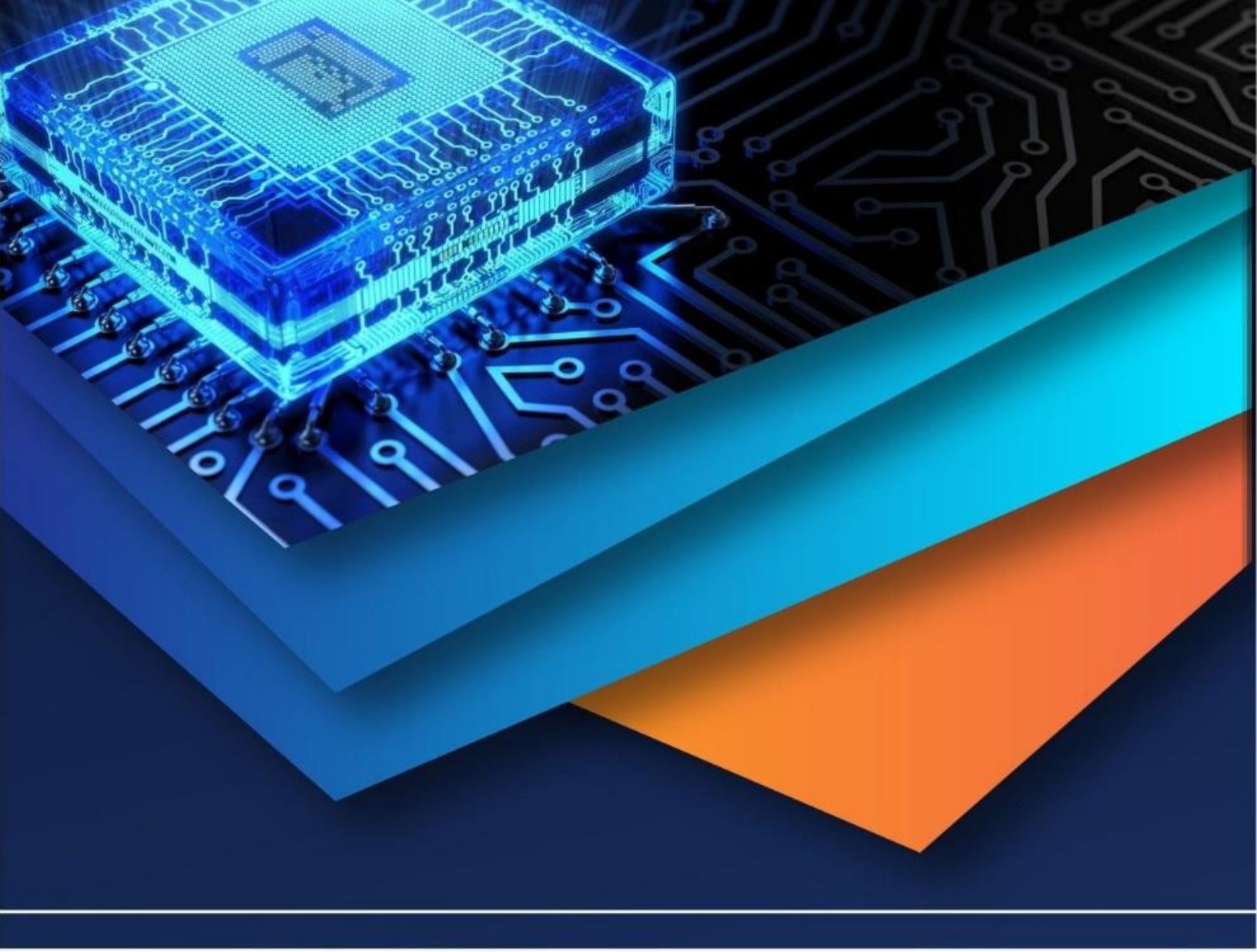
VII. CONCLUSION

This paper presented IntelCrypt, a secure messaging system designed to enhance communication privacy and security using encryption, biometric authentication, and steganography. The hybrid cryptographic model ensures strong data protection while maintaining efficient system performance. Future work will focus on improving system scalability, implementing advanced intrusion detection mechanisms, and optimizing the platform for large-scale secure communication environments.

REFERENCES

[1] M. I. Khaleel, M. Y. Shakor, M. Safran, S. Alfarhood, and M. Zhu, “Dynamic aes encryption and blockchain key management: A novel solution for cloud data security,” IEEE Access, Jan 2024.
[2] V. Kadre, “Securing hadoop/hdfs with aes encryption,” International Journal of Computer Applications (IJCA), Nov 2015.
[3] P. Selvi and S. Sakthivel, “Hybrid ecc-aes encryption framework for cloud data protection,” Scientific Reports (Springer Nature), Feb 2025.
[4] G. S. Poh, V. M. Baskaran, J.-J. Chin, M. S. Mohamad, K. W. Lee, D. Maniam, and M. R. Z’aba, “Searchable encryption with order-preserving techniques,” Algorithms (MDPI), May 2017.
[5] V. Komandla, “Cloud data security for financial applications,” International Journal of Innovative Science and Research Technology (IJISRT), Jan 2025.
[6] S. Kumar and D. Kumar, “Symmetric aes approaches for cloud data security,” Security and Communication Networks (Wiley), Jan 2020.
[7] G. S. Chauhan, “Hybrid encryption for healthcare data security,” Mathematical Problems in Engineering (Hindawi), Dec 2022.
[8] K. A. Al-Dhlan, “Secure searchable cloud storage,” Mathematical Problems in Engineering (Wiley), Dec 2022.
[9] C. Umeaku, “Deduplication-aware secure cloud storage,” International Journal of Innovative Science and Research Technology (IJISRT), Jan 2025.
[10] M. Shiraz, “Comparative study of cryptographic techniques for cloud data,” International Journal of Innovative Science and Research Technology (IJISRT), Jan 2025.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)