ZKG INTERNATIONAL ISSN: 2366-1313

CIPHER SAFE – AN ANDROID BASED ENCRYPTED CHATTING SYSTEM

[1]Mr. M. Suresh Babu,[2]K.Roshan Kumar,[3]M. Sriram Reddy,[4]M.Bhashitha

[1]Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

principaliis@rediff.com

[2, 3, 4, BTech] Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

roshandhoni202@gmail.com,sriramreddy712@gmail.com,Bhashithareddyb@gmail.com

ABSTRACT:

Cipher Safe is a secure mobile messaging application that encrypts user messages using AES256 before storing them in Google Firebase's cloud database. It offers a "clear" functionality for easily deleting stored messages. An innovative OTP system generates one-time passwords sent to the user's mobile or email for secure login. Additionally, Cipher Safe implements a 2-step authentication process, requiring both the password and OTP for account access, providing enhanced security. This approach combines robust encryption, intuitive data control, two-factor authentication, and multi-step login verification to provide a comprehensive, privacy-focused messaging solution. By prioritizing encryption strength, user authority over data, and multi-layered login security, Cipher Safe aims to redefine standards for private mobile communication.

Keywords: Cipher Safe, OTP.

ISSN: 2366-1313

I INTRODUCTION

In the modern digital age, where personal communication has become an integral part of our daily lives, privacy and security have emerged as paramount concerns. Traditional messaging applications often lack robust encryption mechanisms, storing user messages in plaintext format on centralized servers. This practice exposes sensitive data to potential breaches, unauthorized access, and surveillance, compromising the very essence of private communication.

Fig- 1: Cloud Encryption

Recognizing the pressing need for secure messaging solutions, we present "Cipher Safe" – a groundbreaking mobile application that redefines the standards of privacy and data protection in personal communications. Cipher Safe leverages the power of client-side encryption, employing the industry-standard AES-256 algorithm to safeguard user messages before they are transmitted and stored in the cloud.

At the core of Cipher Safe lies a unique approach that empowers users with unparalleled control over their data. Unlike traditional messaging applications, Cipher Safe incorporates a "clear" functionality, enabling users to effortlessly delete all stored messages with a single click. This feature ensures that sensitive communication data can be swiftly and securely removed from cloud storage, further enhancing user privacy. To fortify the security measures, Cipher Safe implements a robust two-factor authentication system, requiring both a password and a one-time password (OTP) for account access. This additional layer of verification prevents unauthorized access and account takeovers, safeguarding user accounts and data from potential threats. Moreover, Cipher Safe takes security a step further by incorporating a multi-step login verification process. This innovative feature introduces an extra level of scrutiny, ensuring that only authorized users can gain access to their accounts and mitigating the risk of brute-force attacks or other malicious attempts.

II. LITERATURE SURVEY

1. Existing messaging applications like What Sapp, Facebook Messenger, and Telegram offer varying levels of security measures, including end-to-end encryption and self-destructing messages. However, these solutions often lack transparency regarding their encryption implementations and data handling practices, and they provide limited user control over stored data.

2. Client-side encryption, where data is encrypted on the user's device before transmission, offers a more secure approach. However, few messaging applications currently implement this due to its complexities and performance implications.

3. Two-factor authentication (2FA) and multi-step login verification are widely recognized security measures that enhance account security by requiring additional verification steps beyond a single password. These measures help prevent unauthorized access and account takeovers, further protecting user privacy and data integrity.

4. The Advanced Encryption Standard (AES) is an industry-standard encryption algorithm that has been extensively studied and widely adopted for its robust security and efficient performance. Many secure messaging applications and security products rely on AES for data encryption due to its proven strength and real-world implementations.

5. The Relevant research papers and studies, such as "Secure Messaging: An Analysis of Encryption in Mobile Messaging Applications" and "Encrypted Messaging: A Systematic Review of Secure Messaging Apps," provide insights into the security challenges and best practices in the realm of secure messaging. 6. Relevant Decentralized storage solutions, such as distributed ledgers or peer-to-peer networks, have gained attention for their potential to increase data security and privacy by reducing reliance on centralized servers.

III SYSTEM ANALYSIS

EXISTING SYSTEM

Traditional messaging applications, such as Whatsapp and Facebook Messenger, store user messages in plaintext format on their servers, leaving sensitive data vulnerable to potential breaches, unauthorized access, and surveillance. These applications lack robust encryption mechanisms and provide limited user control over stored data, posing significant risks to user privacy and data security.

ISSN: 2366-1313

PROPOSED SYSTEM

Cipher Safe is a secure mobile messaging application that addresses the limitations of existing systems by implementing the following key features:

1. Client-Side Encryption: User messages are encrypted on the client-side (user's device) using the industry-standard AES-256 algorithm before being transmitted and stored in Google Firebase's cloud database. This ensures that even if the server is compromised, the message content remains confidential and inaccessible to unauthorized parties.

2. User-Controlled Data Management: Cipher Safe empowers users with the ability to delete all their stored messages from the cloud database with a single "clear" button click. This feature provides users with complete control over their data and enhances their privacy by allowing them to selectively remove sensitive information.

3. Two-Factor Authentication (2FA): Cipher Safe implements a two-factor authentication system, requiring both a password and a one-time password (OTP) sent to the user's mobile or email for account access. This additional layer of security helps prevent unauthorized access and account takeovers, further protecting user accounts and data.

4. Multi-Step Login Verification: In addition to two-factor authentication, Cipher Safe incorporates a multi-step login process, further enhancing the security of user accounts and preventing unauthorized access through brute-force or other attack vectors.

IV IMPLEMENTATION

The Cipher Safe follows a client-server architecture, with the mobile application serving as the client and Google Firebase acting as the server-side component for data storage and authentication.

Architecture:

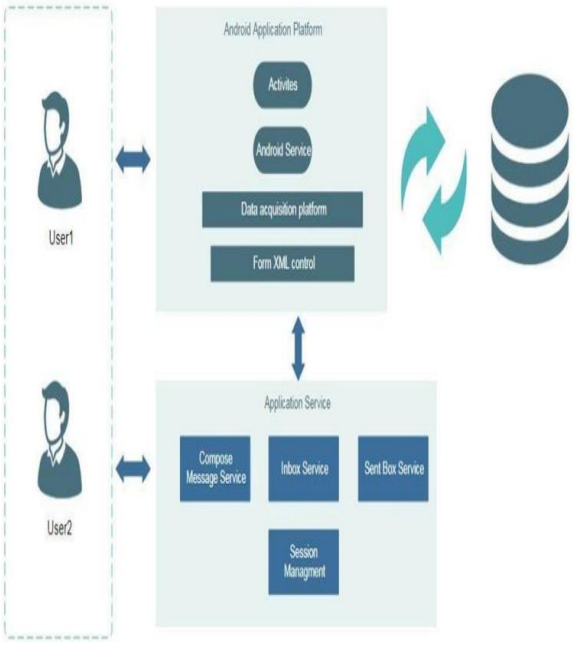


Fig-2. Architectures of the system model

Client-Side (Mobile App):

- The mobile app is responsible for encrypting user messages using the AES-256 algorithm before transmitting them to the server.
- It implements the user interface for messaging, account management, and security settings.
- The app handles user authentication, including two-factor authentication with OTP 8 generation and verification.
- The multi-step login verification process is implemented on the client-side to ensure secure access to user accounts.
- The app communicates with the server-side component (Firebase) for secure data storage and retrieval.

Server-Side (Google Firebase):

- Google Firebase serves as the cloud-based database for storing encrypted user messages. • Firebase Authentication is used for user account management and verification of two-factor authentication credentials.
- Firebase Cloud Functions may be utilized for server-side operations, such as OTP generation and verification.
- Firebase Cloud Messaging (FCM) can be integrated for secure push notifications and message delivery.

Data Flow and Encryption:

- When a user sends a message, the mobile app encrypts the message using the AES256 algorithm and a secure key.
- The encrypted message is then transmitted to the Firebase database for storage.
- Upon receiving a message, the mobile app retrieves the encrypted data from the database, decrypts it using the same key, and displays the original message content to the user. User

Authentication and Access Control:

- User authentication is handled by Firebase Authentication, which supports two factor authentication with OTP verification.
- The multi-step login process is implemented on the client-side, requiring users to provide their password and OTP in multiple steps for enhanced security.
- Access controls are enforced to ensure that only authenticated users can access and manage their respective message data

ISSN: 2366-1313

Mobile App Development:

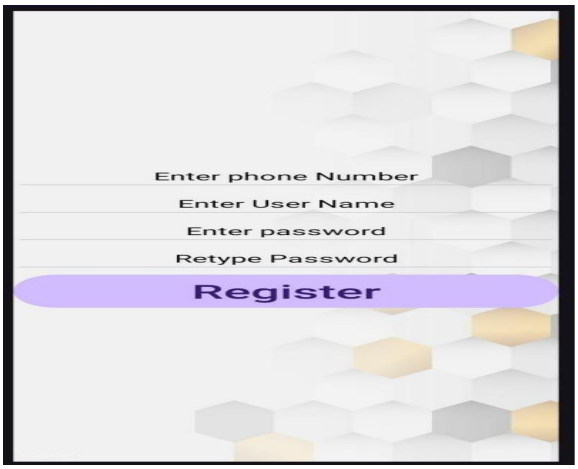
- The Cipher Safe mobile app is developed using Java and the Android SDK, ensuring native performance and compatibility with Android devices.

- The app integrates with Firebase services, including Firebase Real-time Database for data storage and Firebase Authentication for user authentication and OTP verification.

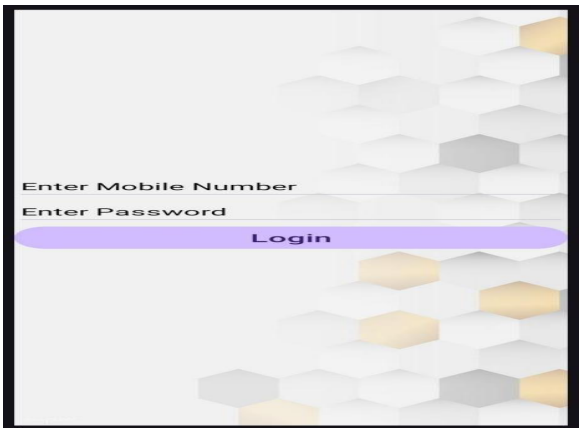
V RESULT AND DISCUSSION

Home Screen:

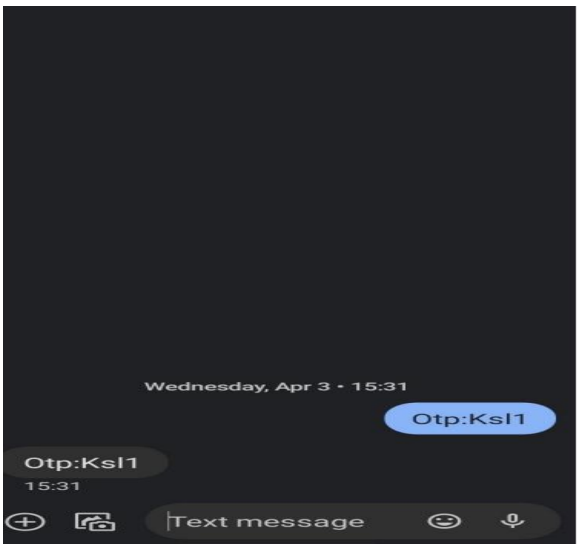
Register Page:



Login Page:



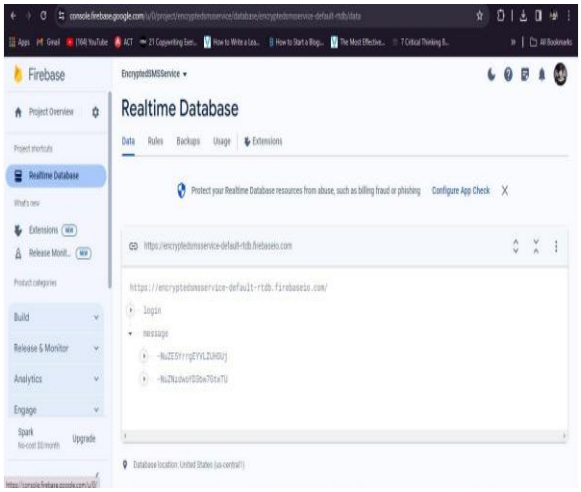
OTP Verification:



ISSN: 2366-1313

Features:

FirebaseCloudServer:



VI CONCLUSION

Cipher Safe is a secure mobile messaging application that addresses the critical need for robust encryption and user privacy in personal communications. By implementing client-side encryption using the industry-standard AES-256 algorithm, Cipher Safe ensures that user messages remain confidential and inaccessible to unauthorized parties, even in the event of a server breach. The application empowers users with complete control over their data by providing a "clear" functionality that allows them to delete all stored messages with a single click. Additionally, Cipher Safe incorporates a two-factor authentication system with OTP verification and a multi-step login process, enhancing account security and preventing unauthorized access. By combining state-of-the-art encryption techniques, user-controlled data management, and advanced authentication measures, Cipher Safe sets a new standard for secure messaging and user privacy in the mobile application landscape. Its innovative approach addresses the limitations of existing messaging solutions and provides a comprehensive, secure, and user-friendly platform for private communication.

FUTURE ENHANCEMENT

1. Implement additional encryption algorithms or modes, such as ChaCha20-Poly1305 or GCM, to provide more encryption options and enhanced security.
2. Explore secure key exchange protocols, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH), for improved key management and secure key distribution.
3. Implement end-to-end encryption for enhanced security during message

transmission, ensuring that messages are encrypted on the sender's device and can only be decrypted on the recipient's device.

4. Incorporate biometric authentication methods, such as fingerprint or facial recognition, for added security and convenient user authentication.

5. Implement self-destructing or ephemeral messaging features, allowing users to set expiration times for messages to automatically delete after a specified period, further enhancing privacy.

6. Develop a web-based version of Cipher Safe to provide multi-platform access and extend the secure messaging capabilities beyond mobile devices.

VII REFERENCES

1. Asokan, N., Pavlovic, D., & Unger, N. (2021). Secure Messaging: An Analysis of Encryption in Mobile Messaging Applications. arXiv preprint arXiv:2101.08090.

2. Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2022). Encrypted Messaging: A Systematic Review of Secure Messaging Apps. arXiv preprint arXiv:2202.10599.

3. Daemen, J., &Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag.

4. React Native Documentation: https://reactnative.dev/docs/getting-started

5. Stutton, A. (2018). Secure by Design: A Guide to Building Secure Applications. Apress.

6. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

7. Prasadu Peddi (2015) "A review of the academic achievement of students utilisinglarge-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

8. Prasadu Peddi (2016), Comparative study on cloud optimized resource and prediction using machine learning algorithm, ISSN: 2455-6300, volume 1, issue 3, pp: 88-94.

AUTHORS

Mr.M. Suresh Babu,Professor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.

Email: principaliis@rediff.com

Mr. K.Roshan Kumar, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: roshandhoni202@gmail.com

ISSN: 2366-1313

Mr. M. Sriram Reddy, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.
Email: sriramreddy712@gmail.com
Miss. M.Bhashitha, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.
Email: Bhashithareddyb@gmail.com