International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

CYPHER TALKS-Chatting Application

Mr.M Pragadheesh Thirumal, Asst.Professor

Keerthi Shankkar J , Ranjith Kumar A , Vishalini B , Dharsan S M , Shivarama Krishnan T S

UG Student

Department of Computer Science and Engineering

Coimbatore institute of Technology, Coimbatore-641014

Abstract— CypherTalks is a novel chatting application designed to prioritize user privacy and security in the digital communication landscape. In an era marked by increasing concerns over data breaches and privacy infringements, CypherTalks emerges as a robust solution offering end-to-end encryption and advanced privacy features. This paper presents the architecture, functionality, and security mechanisms of CypherTalks, emphasizing its commitment to safeguarding user data and conversations. Leveraging state-of-the-art cryptographic techniques, CypherTalks ensures that messages remain encrypted from sender to recipient, thwarting any unauthorized access or interception attempts. Furthermore, the application integrates additional privacy-enhancing features such as ephemeral messaging, anonymous login options, and metadata protection, empowering users with full control over their digital footprint. Through rigorous implementation of industry best practices and adherence to established standards, CypherTalks sets a new standard for secure and private communication platforms. This paper highlights the significance of CypherTalks in addressing contemporary privacy challenges and provides insights into its potential impact on fostering trust and confidentiality in online interactions.

I.INTRODUCTION

Chatting applications have become integral tools for modern communication, offering users the convenience of instant messaging across various devices and platforms. In recent years, the proliferation of messaging apps has led to a diverse landscape, with offerings ranging from mainstream platforms to niche applications catering to specific user needs. Popular messaging apps such as WhatsApp, Telegram, and Signal have dominated the market, boasting millions of active users worldwide. These platforms provide users with features like multimedia sharing, group chats, and voice/video calling, shaping the way individuals interact and connect in the digital age. However, amidst the convenience and connectivity they offer, concerns regarding privacy and security have emerged as significant considerations for users. As data breaches and privacy infringements continue to make headlines, there is a growing demand for chatting applications that prioritize user privacy and offer robust security features. This paper explores the current landscape of chatting applications, highlighting the strengths and limitations of existing platforms in addressing user privacy concerns.

II.RELATED WORKS

The system provided in the [1] employs on how the privacy is used in the chatting application. So the system is built by a framework named flutter which was developed by Google in 2017 . The main feature of the flutter is to give the developers the power of developing a cross platform application which saves the development time instead of creating separate applications for both Android and IOS . The flutter framework uses DART as its language

The Google firebase which is a database service provided by Google is used as the backend to store the data such as usernames, passwords of the users . The Google firebase is a cloud store which is provided by Google as a BaaS(Backend as a service) The Google firebase is very useful to the develops since there is analytics in we can see which data is being accessed frequently and form which part of the wold the data is being accessed.

The Google firebase uses Scrypt for storing the passwords of the users . To be specifc the Google firebase uses a modified version of the Scrpy hashing algorithm to store the passwords of the users in the database along with the details mentioned by the users for the authentication purpose

Scrypt provides password protection through the process of password hashing, which involves converting a user's plaintext password into a fixed-length string of characters called a hash. This hashed password is then stored in the database instead of the plaintext password. When a user attempts to authenticate, their provided password is hashed using the same algorithm, and the resulting hash is compared to the stored hash in the database.

III.LITERATURE SURVEY

In paper[1] ,"Secure Communication in Chatter Application"(2021) - This study focuses on enhancing communication security in the Chatter application by incorporating the Forge framework and Keypair framework for RSA key generation. However, the application's reliance on Angular for development introduces potential vulnerabilities, highlighting the importance of rigorous security testing to safeguard against potential exploits and breaches.

In paper[2],"Security Aspect in Instant Mobile Messaging Applications"(2018)- reviews the rapid growth of smartphone usage and the proliferation of instant messaging apps, noting their popularity and the competitive market. It highlights significant security issues, with many apps failing to meet adequate security standards, leading to privacy concerns. The literature survey emphasizes the need for robust encryption and security measures to protect user data. It evaluates several popular messaging apps to underscore the importance of improving security to enhance app quality and user trust.

In paper [3], "Design of an Android Application for Secure Chatting"(2017) -This paper presents a comprehensive approach to secure chat application development on the Android platform, integrating ECDH, AES, and RC4 algorithms for encryption. While RC4 offers expedited processing, its compromise on certain security aspects is acknowledged, with an emphasis placed on the secure key exchange facilitated by ECDH for overall chat security.

In paper[4],"Development of Chat application"(2022)- This paper delves into the development process of a chat application utilizing the Python programming language. While it capitalizes on Python's versatility and extensive modules for application development, it overlooks the crucial inclusion of a feature for disappearing messages, which is fundamental for enhancing user privacy and security. Despite its programming language choice and emphasis on modular development, the absence of such a feature may hinder its competitiveness in the crowded chat application market.

IV.PROPOSED SYSTEM

a) System Architecture

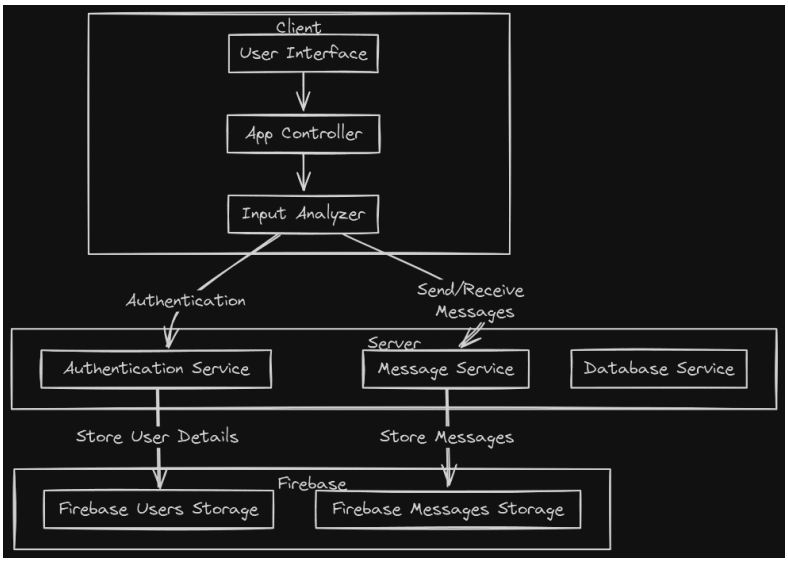
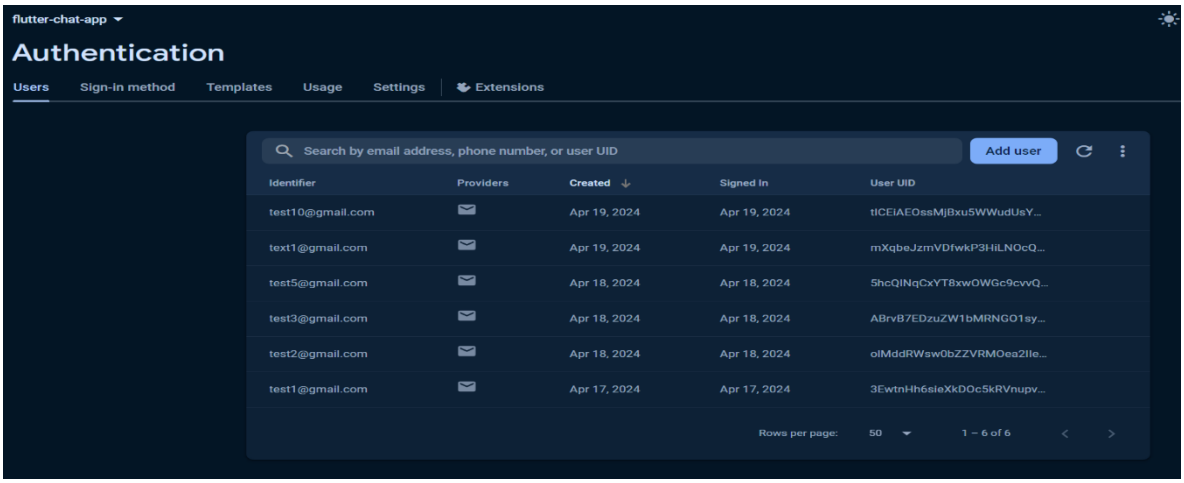


Fig 4.1 Overview of the system

The figure 4.1 represents that the user interacts with the system through the client, which could be a web or mobile application. The app controller manages the overall flow of the application, while the input analyzer determines the appropriate action to take based on the user's input. The authentication module ensures that only authorized users can access the system, and the send/receive module handles the sending and receiving of messages between users. The server is the central hub of the system, where all messages are processed and stored.The authentication, message, and database services handle user authentication, message processing, and data storage, respectively. User details and messages are stored in Firebase Users Storage and Firebase Messages Storage, respectively.

b) Database(Google Firebase)



Fig

4.2 Sample database

Firebase Authentication is a feature within Google Firebase that provides developers with secure mechanisms for managing user authentication in their applications. It supports various authentication methods, including email/password authentication, phone number authentication, social authentication via providers like Google, Facebook, and Twitter, and more.

V.IMPLEMENTATION

The selection of the framework for developing the application can play a crucial role in developing the application there are many ways to develop an mobile application like doing it in Kotlin , Java but the app which are developed by these languages can be only used in android and cannot be used on IOS . So there are two other options , they are either Flutter framework which runs upon Dart language and React Native which runs on Javascript.

These two have their own advantages and disadvantages. Flutter is known for its high-performance rendering engine, which enables smooth animations and transitions. While React Native provides good performance, it might not match Flutter's performance in terms of complex animations and transitions.

Along with Google firebase we will be able to build a comprehensive full stack application which will be secure and be fault tolerant . The Google's Firebase serves as the primary database which stores the users data like username and password.

VI.RESULTS

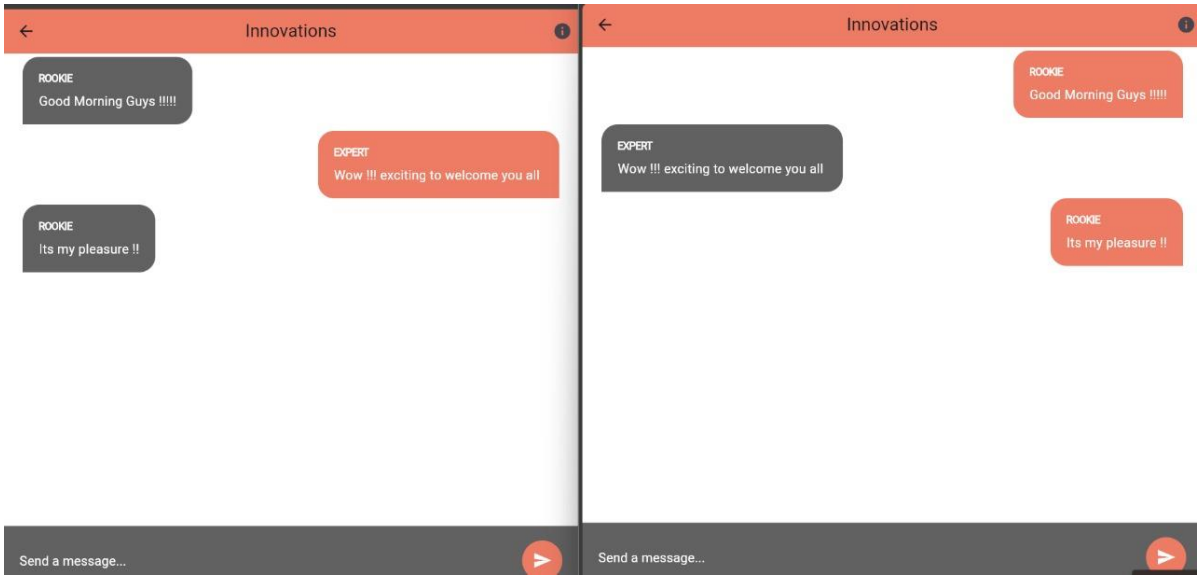


Fig 6.1 Chatting between different users

VII.CONCLUSION

Cypher Talks is a new, promising player in digital communication, about to raise the bar for chat application functionality. It will provide an unprecedented level of security combined with a seamless communication experience. Cypher Talks will maintain user feedback and innovation in the course of its development to provide even more enhanced measures with regards to privacy and new technologies. With that, Cypher Talks will go a long way to shape the future of digital conversations.

VIII.REFERENCES

[1] Moric, Z[latan]; Pinjuh, J[ure] & Kurelic, S[anjin], **"Securing communication in Chatter application"** 2021 32nd DAAAM International symposium on Intelligent manufacturing and automation.
[2] Puneet Kumar Aggarwal, P.S.Grover, Laxmi Ahuja , **"Security Aspect in Instant Mobile Messaging Applications"** 2018 Recent Advances on Engineering ,Technology and Computational Sciences.
[3] Ammar Hammad Ali , Ali M Sagheer , **"Design of an Android application for Secure Chatting"** 2017 International Journal of Computer network and Information Security.
[4] Dr.Abhay Kasetwar, Ritik Gajbhiye, Gopal Papewar, Rohan Nikhare, Priya Warade, **"Development of Chat Application"** 2022 International Journal for Reseach in Applied Science and Enineering Technology.

LINKS

[1]**https://medium.com/@m.romaniiuk/system-design-chat-application-1d6fbf21b372**
[2]**https://firebase.google.com/docs/projects/learn-more**