NORTH SOUTH UNIVERSITY

Department of Electrical and Computer Engineering

Spring 2023 | Course: CSE299 | Section: 21

PROJECT PROPOSAL

Project Name: GOSSIPER - An End-To-End Encrypted Chatting Application

Group No: **04**

Team Members

Dipto Datta Pappu	**2012045042**
Sk. Md. Towfikul Islam Siam	**2012389042**
Fahmida Akter Rapa	**2013903042**
Md. Mofazzal Hossen	**2011298642**

Submitted to

Name: Dr. Mohammad Abdul Qayum (MAQm)

E-mail: mohammad.qayum@northsouth.edu

Submission Date: 21.03.2023

Abstract

With the growing concern about online privacy and security, the need for secure messaging apps has become more important than ever. These apps provide a secure and private way for users to communicate with each other without the fear of their messages being intercepted by unauthorized parties. An end-to-end encrypted chatting app ensures that only the sender and the intended recipient can read the messages exchanged, and not even the app providers or third parties can access the contents of the communication. Our messaging app offers end-to-end encryption and an advanced security feature that uses face recognition and fingerprint scan to ensure safety.

Developers of such apps use various security measures, such as perfect forward secrecy, where a unique encryption key is used for each message sent, making it difficult for an attacker to gain access to multiple messages.

We secured our app **Gossiper** in such a way that if a user's account is hacked, the hacker will not be able to decrypt the user's messages in any way without user authentication. The chatting app employs a strong encryption protocol that secures all user messages. The encryption keys are generated locally on the user's device and are never stored on the app's servers, ensuring that only the intended recipients can access the messages.

Overall, the end-to-end encrypted chatting app provides a secure, user-friendly, and privacy-focused communication channel that can be used for personal or professional communication. Using an E2EE chatting app, users can be confident that their conversations remain private and secure, even in the face of sophisticated cyber attacks.

Features

- Easy Signup process in the application.
- Users can Log in directly using Gmail or their registered Phone no & Password.
- Real-time chat.
- After login, the user can see all their chat list.
- Users can see how many chats are unseen.
- When a user tries to open a chat, the chat will open with a pop-up window to verify the user's face.
- If authentication fails, texts are open like encrypted text. For example-(4f5d%4$dgdgdgue%jfhfj).
- To authenticate the user in a dark area user need their registered fingerprint to decrypt the texts because, in a dark area, the front camera will not work correctly to verify the user.
- When users switch from one chat to another chat or their Phone goes to sleep mood, they need to verify again.
- If a user wants, they can keep turning off this verification process.
- Even developers of this app will not be able to read the user's texts.
- Secure Logout.

Technology

We decided to go with the latest technologies for developing this application to give users a better experience.

Frontend:

To develop the frontend in Android Studio, we will need to use XML to define the UI and Java to add functionality to the UI. The UI components available in Android Studio include TextViews, EditTexts, Buttons, ImageViews, RecyclerViews, and more.

To create a new UI element in Android Studio, we need to add it to the XML layout file. Once added, we can customize the element's properties, such as text, color, size, and position. We can also add event listeners to the UI elements in Java to respond to user interactions, such as clicks.

Backend:

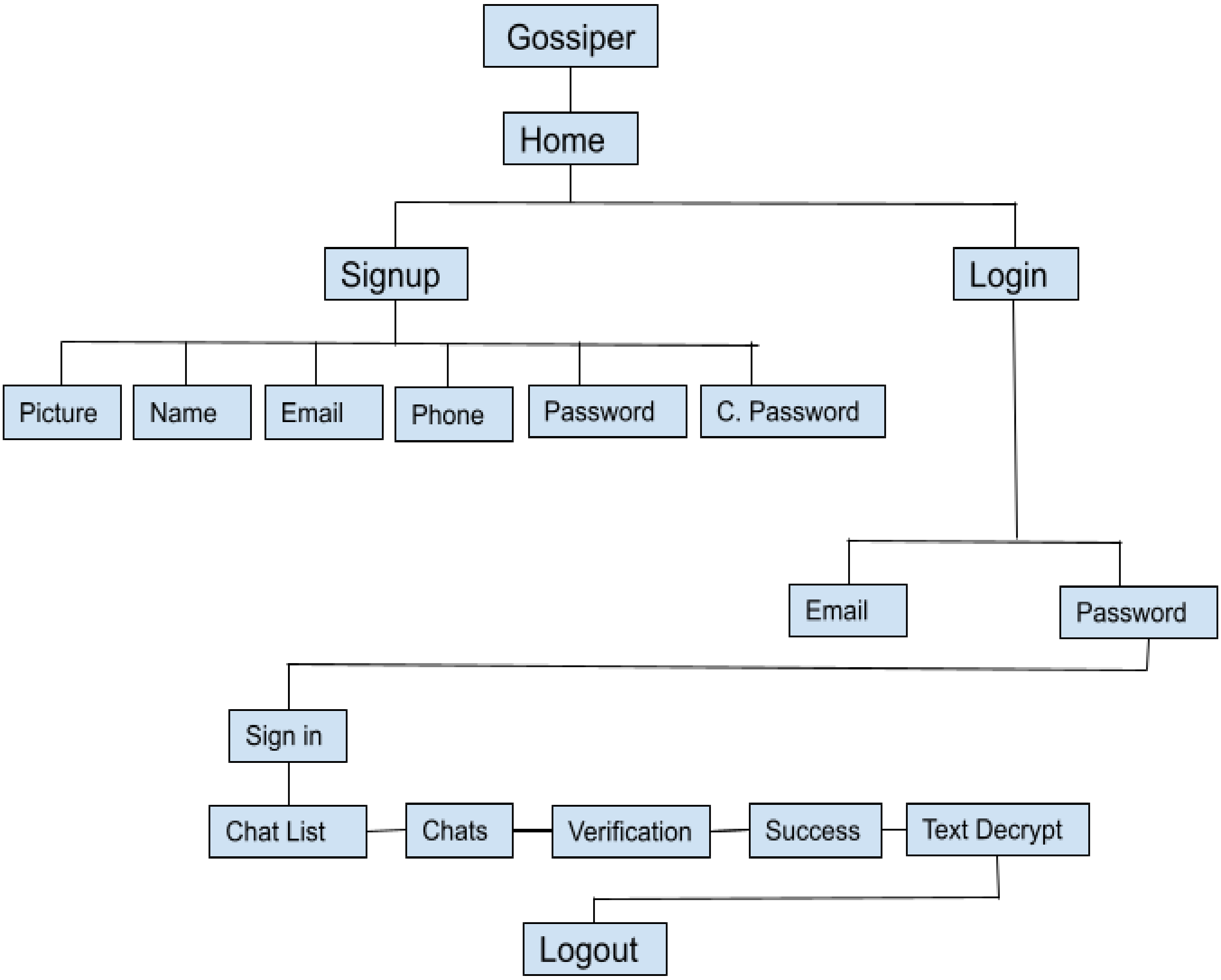
The backend of an Android application typically involves the server-side components that enable the app to access and store data, handle user authentication, and perform other functions that require server-side processing. Android Studio provides several tools and libraries that can help you develop the backend of your Android application.

We will use Raw Java for the backend, and for the authentication process, we will use an API called JCA (Java Cryptography Architecture).

Database:

We will use Google Firebase, which is a mobile and web application development platform. Firebase provides several backend services, such as Realtime Database, Cloud Storage, Cloud Functions, and Authentication, which can help you develop the backend of your Android application quickly and easily.

Sitemap


Gossiper
Home
Signup
Login
Picture
Name
Email
Phone
Password
C. Password
Email
Password
Sign in
Chat List
Chats
Verification
Success
Text Decrypt
Logout

Workflow/Gantt Chart

Weeks	Workflow
Week-1	Background research, related work, and UI Design
Week-2	Sign up and log in page design using Java XML
Week-3&4	Chat List Build using java XML with Unseen and Seen Box
Week-5&6	Implement JCA for verification to encrypt and decrypt texts
Week-7	Connect Database using cloud server; we are using Google Firebase.
Week-8	App testing and Bug fixing

Conclusion

In conclusion, the rise of cybersecurity threats and the need for secure communication has led to the development of end-to-end encrypted chatting apps. These apps offer a secure and private way for users to communicate with each other without the fear of their messages being intercepted by unauthorized parties.

GitHub Repository Link

https://github.com/diptodp/CSE299-Junior-Design-Project.git