**Icon

Description automatically generated**

**CIS 634 Object-Oriented Software Engr**

**Group 11**

**Secure Chat App Software Requirements Specification**

**2836088 – Abdul Rehman**

**2836430 – Tejam Reddy**

**2828837 - Varun**

**2837055 - Sravan**

**1.0 Introduction**

Hush Android chat app, which is a chat application used for personal and office purposes. A friend or office colleague can share any kind of private data through this application. It will help to chat with friends and office colleagues. Mainly, it will help people who want to hide their conversation. Privacy is the top priority of this application. Languages that have been used are Java and XML, developed in Android. Android studio is the tool that is used for this chat application development.

**1.1 Goals and objectives**

The main goal of Hush is a secure messaging app featuring end-to-end encryption as well as the ability to encrypt your messages so no one can read them. You can safely text a friend or family member your personal details like banking info, phone numbers, health information, and much more

* Sign in or Sign up using your phone number
* One to One chat
* Encrypt and decrypt messages
* Preventing screenshots during chatting
* Firebase Real-Time Chat Integration
* Group chat
* Status Updating Feature
* Beautiful Material Design
* Sweet and Clean animations
* Image Sharing

**1.2 Statement of scope**

Hush is an Android chat app, focused on individuals who have trouble following safely texting with loved ones and want to hide their conversation. It is developed in a Java and XML environment, The Main Features of the application.

* Dashboard
* Chat
* Profile
* Contacts
* Settings

**1.3 Software context**

The software is placed in a business or product line context. Strategic issues relevant to context are discussed. The intent is for the reader to understand the 'big picture.

This application is based on privacy and secure chatting among friends, family, and office colleagues. Different kinds of functionalities have been implemented to make sure the high ratio success of this chat app. Functions like encryption and decryption, Group chatting with security and easy use of the application are the important factors of this developed application.

**1.4 Major constraints**

* All database maintenance will be handled by the users and it is available when the user needs it.
* Data is secure enough that no user can see the personal information of the other user.
* Data must be restored in any case loss of data.

**1.4.1 System constraints**

* The Internet should be available to use this system.
* All the records of the User are stored in the Database.

**2.0 Usage scenario**

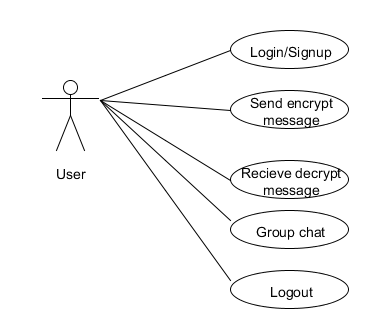
This section provides a usage scenario for the software. It organized information collected during requirements elicitation into use cases. Use cases are a description of how users will perform tasks. The following are our systems use cases:

**2.1 User profiles**

* User

Users who are using this chat application will perform a different kind of functions. Sending and receiving messages with full privacy are the main functions.

**2.2 Use-cases**



**3.0 Data Model and Description**

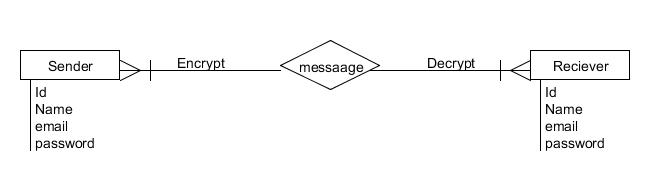
This section describes the information domain for the software

**3.1 Data Description**

An android application is developed with the privacy of data, and messages and provides full security using real-time database. Every person can use this application as per need. This application provides some special functions like data encryption and decryption using different algorithms. A group chat option is available to chat in a group securely.

**3.2 Complete data model**

An ERD for the software is developed



**4.0 Functional Model and Description**

A description of each major software function and software interface is presented.

**4.1.** **Description of Major Functions**

Each requirement is uniquely identified.

**4.1.1** User signup for the application by entering details.

* User can sign up using the application.
* Validation made during sign up:
* Username can be on the choice of user and availability in the system (numbers and special characters are not allowed)
* Phone number for account creation(numbers)
* Phone number will be validated.
* User get 6 digit OTP number.
* All fields must be filled.

**4.1.2** User should sign in by entering credentials.

* Users can login into the app using login activity.
* Validation made during login:
* Phone numbers should be present in the database.
* User get 6 digit OTP number

**4.1.3** User must be able to send and receive messages.

* User needs to log in to access message activity.
* A message can be sent:
* Receiver’s number should be in the contact list.
* User can click on the receiver’s username to start a chat.
* User can send a message:
* By clicking the camera icon gallery will open.
* User can select any picture or video (up to 16MB).
* User can click send button to send pictures or videos.
* User can send type messages in the text field.
* User can click send button to send text messages.
* Text field cannot be empty to send a message.

**4.1.4** Encryption of message should be available.

* User can encrypt the message by clicking on the encryption button.
* User can send an encrypted message:
* Message must be entered in the text field.
* User can encrypt the message by clicking encrypt button.

**4.1.5** Decryption of the message at the receiver end.

* User (receiver) can decrypt the message by entering the password given by the sender:
* Message must be received with encryption from the sender side.
* Message can be unlocked by entering a given matching password by the sender.
* Password should be available in the database.
* Password field cannot be blank.

**4.1.6** Group chat should be available.

* Users can create groups for group chat:
* User can click on the create group button to add other users in the group.
* User should be in the contact list of admin.
* On creating group admin can add user from contact list.
* User can send or receive messages in the group.
* Encryption and decryption can be implemented using password.

**4.1.7** The System must be reliable so that database should not go down and can handle it effectively.

* System reliability depends on backups in case of a down server:
* Firebase by Google will be used for this application to make it reliable.

**4.1.8** This system should be available 24 hours and provide services to the users when the user wants to access the system.

* Availability:
* Google play store platform will be used to make sure 24/7 availability.

**4.1.9** Our product will be easy to use by anyone because its interface is not complex.

* App should be easy to use:
* Iconic guide for user to use it simply.
* General colour scheme to make application more usable.

**4.1.10** System should give a quick response to user action.

* Firebase real time database will be used to make sure quick responses.

**5.0 Restrictions, Limitations, and Constraints**

Special issues which impact the specification, design, or implementation of the software are noted here.

**5.0.1 Restrictions**

* Unauthorized users do not use this system.
* To use this system users will be registered first.

**5.0.2 Limitations**

* Android based application
* Only firebase implemented specifications are usable
* Do not support cross platform working

**5.0.5 Constraints**

* All database maintenance will be handled by the users and it is available when the user needs.
* Data is secure enough that no user can see the personal information of the other user.
* Data must be restored in any case loss of data.
* The Internet should be available to use this system.
* All the records of the User stored in Database.