Deliverable #1

SE 3A04: Software Design II – Large System Design

Tutorial Number: T02
Group Number: G2
Group Members: Chengze Zhao, Ganghoon (James) Park, Jack Walmsley, Luna Aljammal, Pranav Kalsi, Samih Dalvi

1 Introduction

The **SRS** document will provide an intricate view of the requirements, purpose, scope, and the use case diagrams of SecureChat, a secure communication application developed on the Android platform. This will allow the employees of the company to communicate securely, eliminating the concerns of corporate espionage within the organization.

1.1 Purpose

The purpose of the **SRS** is to provide a detailed description of the software requirements of a secure online chat application based on the Android platform. The document serves as a communication tool between the developing team and the clients, allowing both an in-depth understanding of the software's functionality and objectives. Additionally, the document acts as a guide, aiding the development team meet the specified requirements.

The document serves as the primary source of information for the software development team (includes team lead, QA's, UI/UX designers, maintenance team etc.). It provides key information of the functionalities and requirements, essential to the development team for the understanding of the application at large. Additionally, the **SRS** will be an important document for the key stakeholders. This includes the board of directors, the employees and the members of the company at large. They can consult the **SRS** to review and understand project scope, requirements, features, and limitations of the project.

1.2 Scope (James)

The secure online chat application, **SecureChat**, will allow users to establish secure and encrypted communication channels and allow users to send and receive messages securely. It will also allow users to set their out-of-office hours for automatic replies as an innovative feature.

In order to access the application, users must create an account by entering their personal information, such as their name, company email address, employeeID, and password. Upon successful log in, the application will have three options: "Create Chat", "View Chat", and "Set Out-of-Office Hours". The "Create Chat" option will ask the user to enter relevant information about their recipient, such as their name and company email address. The mediated authentication protocol will ensure that the request agent or the message sender is authorized to obtain the requested keys. In the "View Chat" mode, the user can view their messages with other colleagues. Lastly, the "Set Out-of-Office Hours" mode will allow users to set times when they are not expected to be available for work or communication. During these times, the application will send automatic replies after receiving a message.

The software aims to develop a secure chat application for Android devices while safeguarding sensitive information and secrets against corporate espionage. The application will establish secured and encrypted communication channels using a key distribution centre (**KDC**) server, a mediated authentication protocol (**MAP**) to ensure authorized access to encryption keys, and a symmetric-key cryptography for encryption. The **KDC** generates a symmetric key for the user and the recipient that are within the secure communication channel. An encryption service will be used to decrypt the user's key to ensure security over the channel. More importantly, the **KDC** will regularly update the keys, further enforcing security. In addition, **SecureChat** will securely store chat history logs on a separate server and act as a storage system. It will include timestamps,

employeeID, and other identifiers to hold accountability and compliance. The log will not be modifiable or erasable. This will allow the human resources (**HR**) team to review chat logs. Anyone other than the **HR** team will not have access to the chatlog and will not be able to access or view other employee accounts.

Through these functions, **SecureChat** will be designed to protect company secrets and sensitive information, ensure only authorized personnel access, employ secured communication channels, and provide traceable chat history log for accountability. It also aims to create a user-friendly experience, making it useful and easy to use tool for employees within the company to use. Lastly, the application will be designed to respect user privacy, protect company secrets, and consider cultural and legal requirements while being reliable, accurate, available, robust, maintainable.

1.3 Definitions, Acronyms, and Abbreviations

- SecureChat → Name of our secured online chat application
- KDC → Key Distribution Centre
- MAP → Mediated Authentication Protocol
- HR → Human Resources
- Android SDK → Android Software Development Kit
- SRS → Software requirements specifications
- OOO → Out-of-Office

1.4 References

[1] M. Eddy, "The best secure Messaging apps for 2024," *PCMAG*, Jan. 09, 2023. https://www.pcmag.com/picks/best-secure-messaging-apps

[2] S. Jain and S. Jain, "How WhatsApp Ensures Chat Security with End-to-End Encryption - Requestly," Requestly - Chrome Extension to Intercept and Modify HTTP requests, Dec. 26, 2023. https://requestly.io/blog/how-whatsapp-ensures-chat-security-with-end-to-end-encryption/

[3] G. Veiga, "10 rules for creating a mobile look and feel," OutSystems, Oct. 28, 2016. https://www.outsystems.com/blog/posts/mobile-look-and-feel/

[4] A. Kumar, "A Beginner's Guide to understanding User Interface (UI) design," Medium, Oct. 05, 2023. [Online]. Available: https://bootcamp.uxdesign.cc/a-beginners-guide-to-understanding-user-interface-ui-design-f4e3a95a0ad6

[5] G. Veiga, "10 rules for creating a mobile look and feel," OutSystems, Oct. 28, 2016. https://www.outsystems.com/blog/posts/mobile-look-and-feel/

[6] Sabah, Noor & Kadhim, Jamal & Dhannoon, Ban. (2017). Developing an End-to-End Secure Chat Application. 17. https://www.researchgate.net/publication/322509087_Developing_an_End-to-End_Secure_Chat_Application

[7] L. Perri, "What Is a Digital Immune System and Why Does It Matter?," Gartner, 2022. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter

[8] 16 metrics to ensure mobile app success, https://www.appdynamics.com/media/uploaded-files/1432066155/white-paper-16-metrics-every-mobile-team-should-monitor.pdf (accessed Feb. 12, 2024).

[9] C. Wright, "Information gathering," in Elsevier eBooks, 2008, pp. 73–114. doi: 10.1016/b978-1-59749-266-9.00005-9.

1.5 Overview

Section 2 provides a high-level product description, the product perspective, its functions, user characteristics, assumptions and dependencies, and apportioning of requirements. Sections 3 contains the Use Case Diagram of an employee creating a chat. Section 4 describes the business events and their respective viewpoints. Section 5 explores the Non-Functional Requirements, specifically the Look and Feel Requirements, Usability and Humanity Requirements, Performance Requirements, Operational and Environmental Requirements, Maintainability and Support Requirements, Security Requirements, Cultural and Political Requirements and Legal Requirements. Section 6 describes our innovative feature. Finally, Section A includes the Division of Labour to provide adequate credit to contributing team members.

2 Overall Description

2.1 Product Perspective

Although this product has a new angle which is generating a new key for each communication it is similar to a lot of large-scale communication apps. The products' requirements are related to a lot of existing products but still maintains a clear differentiator (key-generation). Other products that may come to mind are messaging apps, email, and existing corporate communication platforms.

Starting with messaging apps, a lot of apps namely WhatsApp, Signal, and Telegram [1] feature encrypted messaging. For example, WhatsApp has unique keys for each device's conversations, meaning only the target recipient has the key to open the message [2]. The difference between **SecureChat** versus something like WhatsApp is that our app is tailored for corporate use. This means that that the app will not have the social media aspects seen in WhatsApp and other messaging apps, meaning the look and feel will be more professional.

Additionally, a lot of emailing platforms and existing corporate communication platforms exist but they do not use a **KDC** to generate unique keys for each conversation. Security is a key concern for the client as they are constantly conversing and sharing sensitive information. The existence of key creation adds an additional level of security.

This app will be a completely standalone app and will not be integrated into any other system. This app will strictly be used for chatting, sharing files, and pictures. Additionally, being a standalone app and not integrated into other systems will result in a more secure application. This is a result of less data transfer between apps consequently ensuring that there are less places the app could be vulnerable to malicious attacks.

This application is not applicable to being defined as a product that is a component of a larger system. A block diagram showing the major components of the larger system is also not applicable.

2.2 Product Functions

There will be 3 modules in the product: The authentication service, the chat service, and the logging service. The major function of the chat encryption service is to encrypt and decrypt private keys, and to verify keys between users in the conversation. The main functions include registering the user with the **KDC** and providing them with a public key, and a private key that will be used to message them. The private key is decrypted upon request of a chat, and if decryption fails then the chat is not created and the key remains encrypted, this will be implemented using an automated protocol. **SecureChat** will encrypt and decrypt the private session keys which can later be used to access conversation history. Essentially, the software distributes encrypted keys and decrypts them for the registered users to begin a secure session. Moreover, it verifies that the request is made by an authorized user before decrypting the key.

Modules	**Functions**
Authentication Service	- Create an account - Verify that employee is registered within the company

	- Provide them with a public and private key upon registration - Confirm that the employee is authorized to access the organization using the public key - Update and cancel employee registration
Chat Service	- Creating a chat - Selecting members to chat with - Encrypting a session's key - Decrypting private keys to provide chat access
Logging Service	- Maintains a record of all existing chats - Records the dates and times of messages - Stores the private keys of the members within a chat

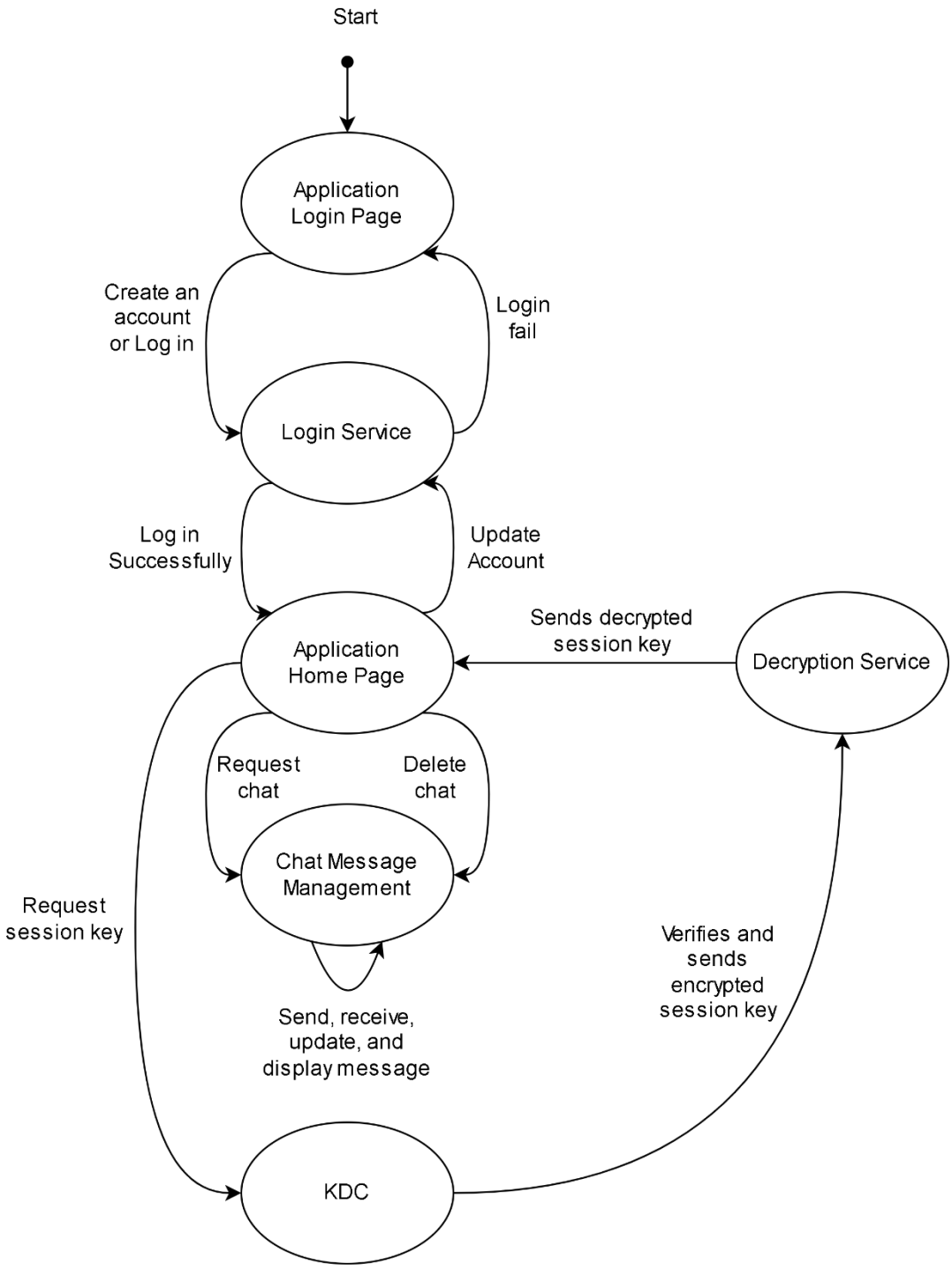

Figure 1. State Diagram

2.3 User Characteristics

The intended users of the product are not technical experts, but they have a basic level of technical education in technology fields. Their experience with professional technical tools, especially for information security software, or bank systems, is limited. The group contains people from various backgrounds who uses technology in daily lives.

The specific requirements make it necessary to design a product that is intuitive and easy to use, while maintaining minimal and viable design features. The goal is to reduce the complexity for users to use the software in user interface, especially the system designed to solve complex sensitive finance problems.

2.4 Constraints

- **Time Constraints**: Time constraints can limit the amount of time for software development, testing, and iterations.
- **Budgets Constraints**: Budget constraints can limit the scope of the project, it will affect the quality of the resources can be utilized, the number of features can be implemented, number of tests can be done, etc.
- **Resource Constraints**: The limitations we face while developing a software in terms of available resources such as software, hardware tools, servers, or third-part services can have big impact on the scalability, performance, functionality of the software.

2.5 Assumptions and Dependencies

- Operating System: changing the version of Android will affect what **SDK** functionality will be available to us, we assume it is the most recent version (Android 14 currently).
- Internet Connectivity: having no internet connection would make communication impossible, we assume there will be internet connectivity whenever the user is using the app.
- Malware: having malware installed on a client device would possibly compromise the security of the app beyond what we can account for, we must assume all client devices are working properly with no malware.

2.6 Apportioning of Requirements

1. Allow capabilities to send images through the chat
    i. Current version will only allow to send text messages
2. Allow voice/video call in group chat
    i. Allows employees to communicate more easily by speaking with each other as opposed to texting
3. Allow group calling
    i. Can be utilized for company meetings, enabling work from remote settings

3 Use Case Diagram

The most important business event is starting a new chat with a user. This business event requires the use of almost every part of the system. The user first logs into the app, they then choose a person to send a message to. The server authenticates them and generates a key for the new conversation they are starting. This key is then sent back to the user where it is used to encrypt future messages, while the user is given a textbox to enter their first message.

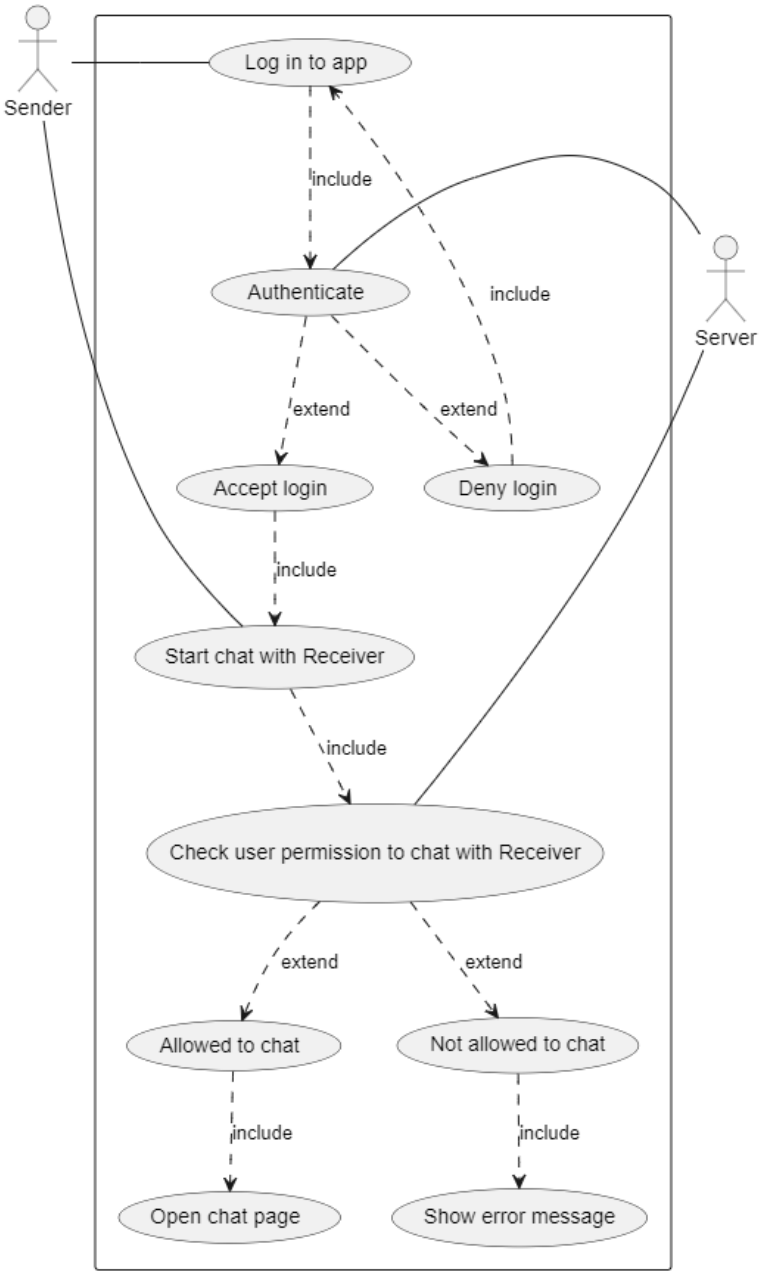

Figure 2. Use case diagram

4 Functional Requirements

The business events that are considered include:

- BE1: Register/create an account
- BE2: User Login
- BE3: Start a chat with a colleague
- BE4: Set out-of-office hours and generate automated response (innovative feature)
- BE5: Delete a message
- BE6: Delete account/leave company
- BE7: Use chat logbook

The viewpoints that are considered:

- VP1: App user
- VP2: Security
- VP3: Company IT department
- VP4: **HR**

Business Events:

BE1: Register/create an account.
Pre-Condition: User does not have an existing account.

VP1.1 App User

S1: The system prompts the user to enter personal information including name, company email address, employeeID, and password.
E1: User enters relevant information.
S2: System authenticates information.
S2.1: If authentication is approved, user is allowed access to the application.
E2.1.1: User uses the app and its features.
S2.1.2: System registers the user with the Key Distribution Centre (**KDC**) and provides the user with key(s)
S2.2: If authentication fails, indicate user to enter credentials correctly and provides user an option to contact IT department.
E2.2.1: User enters correct information or wants to connect with IT department.
S2.2.1: System creates account or notifies IT department (who help employee create account)

VP1.2 Security

S2: Authenticate user information by checking if credentials match company database (outside the scope). Prevent outsiders from gaining access to the application.

VP1.3 Company IT department

S2.2: If authentication fails, the system throws an error message, indicating user to enter credentials correctly and provides user an option to contact IT department.
E2.2: IT department setup account on behalf of employee
S2.2i: System creates account for employee

VP1.4 HR

N/A

Global Scenario:
Pre-Condition: User does not have an existing account.
Main Success Scenario:

S1: The system prompts the user to enter personal information including name, company email address, employeeID, and password.
E1: User enters relevant information.
S2: System authenticates information.
S2.1: Authenticate user information by checking if credentials match company database (outside the scope). Prevent outsiders from gaining access to the application
E2: User uses the app and its features.
S3: System registers the user with the Key Distribution Centre (**KDC**) and provides the user with key(s)

Secondary Scenario:
S2.2: authentication fails, indicating user to enter credentials correctly and provides user an option to contact IT department.
E2.2: User enters correct information or wants to connect with IT department.
S2.2i: System creates account or notifies IT department (who help employee create account)

BE2: User Login.
Pre-Condition: User does have an existing account.

VP2.1 App User
S1: The system prompts the user to enter login information (employeeID and password).
E1: User enters login information.
S2: System authenticates information.
S2.1: If correct information is received by the system, the system requests access to a session key from **KDC** on behalf of the user, the **KDC** verifies credentials and allows access to session key if verification is successful.
E2.1: User can access the app and use its features.
S2.2: If system receives wrong information, let user know incorrect information is entered and return to main menu.
`

VP2.2 Security
N/A

VP2.3 Company IT department
N/A

VP2.4 HR
N/A

Global Scenario:
Pre-Condition: User does have an existing account.
Main Success Scenario:
S1: The system prompts the user to enter login information (employeeID and password).
E1: User enters login information.
S2: System authenticates information.
S2.1: If correct information is received by the system, the system requests access to a session key from **KDC** on behalf of the user, the **KDC** verifies credentials and allows access to session key if verification is successful.
E2.1: User can access the app and use its features.

Secondary Scenario:
S2.2: If system receives wrong information, let user know incorrect information is entered and return to main menu.
E.2.2: User tries to login again. Loop to ***S2***

BE3: Start a chat with a colleague

Pre-Condition: There is no existing chat that would be available to message the intended people. The user must have an account and is already logged into the app.

VP3.1 App User
Main success scenario:

S1: The application prompts the user to enter the people they would like to message in the required fields.
E1: The user submits a request to create a chat with the given accounts.
S2: A chat is created for the user to contact their colleagues.

Secondary scenario:

S2.2: System identifies an existing chat with requested parties.
E2.2.1: User is directed to continue in the existing chat.

VP3.2 Security

N/A.

VP1.3 Company IT department

S2.2: If request to chat is rejected, the system throws an error message, indicating user to choose a verified individual to chat with.
E2.2: IT department suggests a list of accessible accounts to an employee.
S2.2i: System creates a chat.

VP1.4 HR

N/A

Global Scenario:
Pre-Condition: User does not have an existing chat with the requested groups.
Main Success Scenario:

S1: The system prompts the user to enter the information of the people they wish to message (employee name).
E1: User enters account information.
S2: System authenticates information.

S2.1: If correct information is received by the system, the system creates a chat between the user and the requested accounts.
E2.1: User can access the chat and send messages.

Secondary Scenario:

S2.2: If system receives request to chat with a non-existent account, let user know incorrect information is entered and re-enter an account on main-menu.
E.2.2: User tries to message again. Loop to ***S2***

BE4: Set out-of-office hours and generate automated response (innovative feature)
Pre-Condition: The user must have an account. User has a schedule of when they are going to be unavailable. User has an automated response in mind.

VP4.1 App User
Main Success Scenario

S1: System presents an option to set automated replies.
E1: User selects automated replies and requests to set automatic replies.
S2: System prompts user to set specific start and end times for their **OOO** period.
E2: User selects a valid start time and end time for when they would like to send automated replies.
E3: User enters the message they desire and sets up automated replies.
S3: System confirms the configured out-of-office hours and the generated automated reply, then sets automated response as active for the specified duration.
S3.1: If system receives message during specified out-of-office hours, the message sender receives automated reply set by the message receiver.
E3.1: User can view the chat with the automated reply.

VP4.2 Security
N/A

VP4.3 Company IT department
N/A

VP4.4 HR
E2: If employee sets out-of-hours for an extended period of time, such as over 5 days.
S2.1: System sends alert to **HR** about employee's extended absence.
E2.2: HR reviews alert and ensures it aligns with company policies and procedures.
E2.3.1: If extended out-of-office period complies with company policies or if it is a special case, **HR** approves or ignores alert.
E2.3.1: If extended out-of-office period violates company policies, **HR** contacts employee to modify automated response accordingly.

Global Scenario:
Pre-Condition: The user must have an account. User has a schedule of when they are going to be unavailable. User has an automated response in mind.

Main Success Scenario:
S1: System presents an option to set automated replies.
E1: User selects automated replies and requests to set automatic replies.
S2: System prompts user to set specific start and end times for their **OOO** period.
E2: User selects a valid start time and end time for when they would like to send automated replies.
E3: User enters the message they desire and sets up automated replies.
S3: System confirms the configured out-of-office hours and the generated automated reply, then sets automated response as active for the specified duration.
S3.1: If system receives message during specified **OOO** hours, the message sender receives automated reply set by the message receiver.
E3.1: User can view the chat with the automated reply.

Secondary Scenario:
E2: User enters an invalid range of **OOO** hours.
E3: User enters unsupported characters in the message.
S3: If user encounters technical issues during the out-of-office automated reply configuration and reports issue to the company IT department through app's support channel.
S3.1: IT department investigates reported issue and checks for system bugs or glitches.
E3.1.1: If it is a software issue, IT department reports the issue and releases a patch or update to address the problem.

E3.1.2: If it is user-specific issue, such as incomplete information, unsupported characters in the message, network connectivity issues, insufficient memory or storage, IT department provides technical support and guidance to resolve the problem.

BE5: Delete a message.
Pre-Condition: The user is logged in, the message to be deleted exists, finally the user has a valid to enter the chat and delete.

VP5.1 App User

S1: The chat UI prompts if the user would like to delete the message.
E1: The user deletes the message.
E2.1: If user deletes the message.
S2.1.1: Chat is deleted from the UI and annotated in the logbook that its deleted.
E2.2: The user doesn't delete.
S2.2.1: No changes.

VP5.2 Security

N/A

VP5.3 Company IT department

N/A

VP5.4 HR

N/A

Global Scenario:
Pre-Condition: The user has an account, the message to be deleted exists, finally the user has a valid to enter into the chat and delete.

Main Success Scenario:

S1: The chat UI prompts if the user would like to delete the message.
E1: The user deletes the message.
E2.1: If user deletes the message.
S2.1.1: Chat is deleted from the UI and annotated in the logbook that its deleted.

Secondary Scenario:

E2.2: The user doesn't delete.
S2.2.1: No changes.

BE6: Delete account/leave company
Pre-Condition: The user has an existing account.

VP6.1: App user

S1: The application prompts the user to enter their login information.
E1: User provides the required login information.
S2: System checks if user account is still active
E2: User does not successfully log in

VP6.2: Security

S2: The system verifies the user's login information for authentication.
E2: User authentication is successful, granting access for account management.
S3: The system ensures that only authenticated users can access account deletion.

VP6.3: Company IT department

E3: IT department receives notification can initiates necessary procedures for account deletion.

S4: In case of account deletion, the system notifies the company IT department about the pending account deletion request.
E4: Account is deleted by IT department.

VP6.4: HR

S5: The system notifies **HR** that the user is leaving the company if IT department receives the account deletion request.
E5: HR personnel receives notification and initiates the necessary procedures for account deletion.
S6: HR personnel updates employee records and ensures compliance with company policies and regulations.
E6: User's employment status is updated by **HR**.

Global Scenario:
Pre-Condition: The user attempt to delete the account or leave the company is logged into the app and has appropriate permissions to access account management.
Main Success Scenario:

S1: The application prompts the user to enter their login information.
E1: User provides the required login information.
S2: System checks if user account is still active
E2: User does not successfully log in
S2: The system verifies the user's login information for authentication.
E2: User authentication is successful, granting access for account management.
S3: The system ensures that only authenticated users can access account deletion.
E3: IT department receives notification can initiates necessary procedures for account deletion.
S4: In case of account deletion, the system notifies the company IT department about the pending account deletion request.
E4: Account is deleted by IT department.
S5: The system notifies **HR** that the user is leaving the company if IT department receives the account deletion request.
E5: HR personnel receives notification and initiates the necessary procedures for account deletion.
S6: HR personnel updates employee records and ensures compliance with company policies and regulations.
E6: User's employment status is updated by **HR**.

BE7: Use Chat logbook
Pre-Condition: There is existing chat that would be available to access of the target people.

VP7.1 App User

N/A

VP7.2 Security

N/A

VP7.3 Company IT department

N/A

VP7.4 HR

S1: HR personnel navigate to the chat logbook section with the application.
E1: HR personnel requests access to the logbook.
S2: The system presents options for selecting specific chat logs or filters for the logbook.
E2: **HR** personnel select desired options or filters.
S3: The system retrieves and displays the requested logbooks based on the HR personnel's selection.
E3: **HR** personnel view the requested chat logbook.

Global Scenario:
Pre-Condition: HR personnel are logged into the application and have legal permissions to access the chat logbook by requests.
Main Success Scenario:

S1: HR personnel navigate to the chat logbook section with the application.
E1: HR personnel access/request the logbook.
S2: The system presents options for selecting specific chat logs or filters for the logbook.
E2: **HR** personnel select desired options or filters.
S3: The system retrieves and displays the requested logbooks based on the **HR** personnel's selection.
E3: **HR** personnel view the requested chat logbook

5 Non-Functional Requirements

5.1 Look and Feel Requirements

5.1.1 Appearance Requirements

LF-A1 Interface must be easy to interact with.

Rationale Although the backend logic of the system might be a little bit complicated and easy to learn interface is key. The easier to use the app, the quick users can adapt and use the app.

LF-A2 Team of the app should be such that it neutral and should cater to all ages and demographics.

Rationale: Having insignia that only represents a certain group might alienate other users. [3]

LF-A3 The apps widgets and buttoned should fill the screen.

Rationale: making sure that buttons are easy to use and ensures a user-friendly design.

LF-A4 Fonts should be consistent throughout the app.

Rationale: This will ensure users never felt lost throughout the app. Often users appreciate consistency. Consistency throughout the app ensures that the user does not feel overwhelmed and focus on the key value proposition and the barrier of user isn't high [4].

5.1.2 Style Requirements

LF-S1 The style requirements for this app are that the app's format suits all users.

Rationale: This encompasses using colour combinations and font sizes that are easy on the eye and are easy to read. It will be important to design for functionality and usability rather than generating a complicated art piece.

LF-S2 Respect conventions of standard app. [5]

Rationale: This includes keeping the search button where it's expected to be. Human attention spans are decreasing by the year. Users need easy access to common features, and they must follow the convention of where frequently used buttons are commonly placed on the screen.

LF-S3 Colors should not be clashing otherwise it will be hard for the user to read.

Rationale: Users will be spending a lot of time on the app meaning that the colour combination must be such that it does not cause eye strain.

5.2 Usability and Humanity Requirements

5.2.1 Ease of Use Requirements

UH-EOU1. The system shall allow users to provide feedback on bugs, using experiences, and suggestions.

Rationale: User feedback is invaluable for identifying issues, improving usability and enhancing features within the app.

UH-EOU2. The user interface should be like other message apps like messenger/WhatsApp.

Rationale: Familiarity with existing messaging apps like Messenger and WhatsApp ensures that users can quickly adapt to the new app without a steep learning curve

UH-EOU3. The system shall allow synchronization of messages and conversations over multiple devices, including smartphones, laptops.

Rationale: Synchronization across multiple devices ensures that users can pick up conversations where they left off, regardless of the device they are using, which enhances user convenience, productivity, and continuity of communication.

UH-EOU4. Implement clear and informative error messages to guide users in case of connectivity issues, server errors, or other unexpected situations.

Rationale: Clear and informative error messages reduce user frustration and confusion by providing insights into the nature of the problem and potential solutions.

5.2.2 Personalization and Internationalization Requirements

UH1-PI1. The system shall support multiple languages, allowing users to select their preferred language for the user interface and communication within the app.

Rationale: Enabling users to interact with the messaging app in their native language enhances comprehension, usability, and overall user satisfaction.

UH1-PI2. The system shall offer customizable themes and personalization options, allowing users to tailor the appearance and visual elements of the app according to their preferences

Rationale: Customizable themes enable users to express their personality, mood, or brand identity through the visual aesthetics of the app.

5.2.3 Learning Requirements

UH1-LP1. The system shall employ machine learning algorithms to analyze conversation patterns, providing intelligent suggestions for quick replies based on user behavior.

Rationale: Machine learning algorithms enable the system to learn from user interactions and adapt its suggestions over time, improving accuracy and relevance based on individual preferences and communication habits.

5.2.4 Understandability and Politeness Requirements

N/A

5.2.5 Accessibility Requirements

UH1-AR1. The system shall support integration with screen readers and voice assistants, ensuring accessibility for users with visual impairments or disabilities.

Rationale: Accessibility features like screen reader support promote inclusivity to digital communication apps, empowering users with disabilities to participate fully in online conversations.

UH1-AR2. The system shall provide comprehensive keyboard navigation support and customizable shortcut options to facilitate accessibility for users who prefer keyboard-based navigation.

Rationale: Customizable shortcut options empower users to personalize their navigation experience according to their preferences and accessibility needs, promoting a more efficient and intuitive user experience.

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1. The app start-up time should be less than 2 seconds.

Rationale: Typical mobile apps that have integrated APIs have a response time that averages 1 second [8]. To provide the team with a buffer, we aim to have a response time of ~2 seconds. This is to ensure a speedy service to our clients. Since this will be integrated into a company, launch efficiency is critical to ensure that company communications are not delayed.

5.3.2 Safety-Critical Requirements

PR-SC1. The app must not leak conversations to people that are not in the chat.

Rationale: The privacy within the messaging system is critical to the correctness of the system.

PR-SC2. Logbook access is only available to authorized individuals.

Rationale: Tracking conversations and chat history must be exclusive to authorized individuals within the **HR** team. This provides the main value of the application to prevent corporate espionage.

5.3.3 Precision or Accuracy Requirements

PR-PA1. The app must show the time stamps of when chats were created and when messages were sent. The accuracy of these stamps can deviate by a few seconds.

Rationale: The precision is critical as the log is a core component of the app in providing an accurate history to review and track in the case of misconduct.

5.3.4 Reliability and Availability Requirements

PR-RA1. The system must maintain previous messages which are accessible by entering the associated key.

Rationale: This ensures traceability of previous communications. Additionally, having access to old chats in a secure manner provides insights into social dynamics within the company when needed.

PR-RA2. The system must preserve the history of the chat correctly within the chat and the logbook. There cannot be a difference between the recorded data in each location.

Rationale: Maintaining the integrity of chats is crucial when tracing conversation history. Ensuring the correctness of the logs is critical to avoid potential misinterpretations.

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1. The user must be able to initiate or contribute to a chat if they have access to the app and internet. They would be able to view previous messages, however, they will not be able to send or receive new messages until their internet connection is restored.

Rationale: Even if a user does not have access to the internet, they should be able to read pre-loaded chats as they would not have to re-enter the chat when the internet connection is restored.

5.3.6 Capacity Requirements

PR-C1. The system must be able to handle multiple chats at once and should be able to send and encrypt multiple keys at a time.

Rationale: This is critical to ensure the efficiency of the app, as its main functionality is to provide secure chatting. It would be unreasonable for there to be a queue for users that want to chat at a given time, especially since the app will be used within working hours.

5.3.7 Scalability or Extensibility Requirements

PR-SE1. The app must abide by SOLID Design principles, to ensure that it is designed thoughtfully and allowing it to be scaled over time.

Rationale: The app caters to the entire company, meaning it should handle more users as the company grows.

5.3.8 Longevity Requirements

PR-L1. The app must store the chat logs on the server for as long as the app is working. Data must remain on the logbook if the company is still using the app.

Rationale: Maintaining chat logs and history is required for the app, as the company might be interested in identifying previous conversations at any point of operation.

5.4 Operational and Environmental Requirements

5.4.1 Expected Physical Environment

OE-PE1. The chat application should be designed for use on android devices in both indoor and outdoor environments. Should work reliably in environments with fluctuating connectivity such low bandwidth and high latency.

OE-PE2. it should only allow employees on office premises or currently approved for hybrid work to use the app services.

Rationale: Since the app should only allow access to employees, it would be beneficial to only allow employees on office premises or approved to work in a hybrid environment to gain access to app. For employees working in a hybrid environment, the connectivity should not have a grave impact on app functionality.

5.4.2 Requirements for Interfacing with Adjacent Systems

OE-IA1. The system should have a secure and authenticated connection to the Key Distribution Centre (**KDC**) to request and receive encryption keys.

Rationale: Since the app relies on receiving keys from the **KDC**, it should have a secure connection to it at all times.

5.4.3 Productization Requirements

N/A

5.4.4 Release Requirements

OE-R1. The application must be compatible with company issues android devices (i.e., should work with the android version that is available on the devices)

Rationale: The employees should be able to use the app on company-issued devices as that is the only communication channel that is permitted for use of the app.

5.5 Maintainability and Support Requirements

5.5.1 Maintenance Requirements

MS-M1. The system should have monthly maintenance & updates to resolve any issues and bugs in the software. (Weekly for the first month of release)

Rationale: To enable smooth functionality of the app, it is vital that there are regular fixes, ensuring good app quality and user satisfaction.

5.5.2 Supportability Requirements

MS-S1. The system must have a help section that connects the employees directly with the IT department should any issues arise (ideally 24/7 support or during company work hours).

Rationale: Users should have access to support at all times during work hours for any technical app related issues that may arise.

5.5.3 Adaptability Requirements

MS-A1. The system should work on the company issues android devices and should be adaptable for future android versions shall the company decide to upgrade the devices in the future.

Rationale: The app should provide a long term solution to the company's problem of corporate espionage and thus should work on their devices.

5.6 Security Requirements

5.6.1 Access Requirements

SR-AC1. The user must be enrolled in the organization to have access to the chatting Services.

Rationale: for this is that to maintain confidentiality and security we must ensure that the person in the organization. Additionally, using the **KDC** we are able to figure out if the correct user is being sent too.

SR-AC2. The user must enter the correct key to enter or continue using the chat.

Rationale: We want to confirm that the person receiving the message is the intended receiver.

5.6.2 Integrity Requirements

SR-INT1. App must utilise AES encryption strategy to ensure that the keys are secure.

Rationale: This makes sure that all of the keys are encrypted and secured from external access.

SR-INT2. The message data integrity must be maintained.

Rationale: The chat data contains a lot of sensitive information, along with the logbook. Effective authentication protocols must be put in place to ensure the integrity of the data is maintained. For this we will implement the BIBA model for integrity [9] to ensure that people can only read down and write up.

5.6.3 Privacy Requirements

SR-P1. Only the sender and stakeholders who have access to the logbook may view the message that is sent to them. [6]

Rationale: This ensure that only people with a high security clearance can access the messages. This ensures that corporate espionage is prevented.

5.6.4 Audit Requirements

SR-AU1. A logbook is kept with all the chats. The purpose of the app is to mitigate corporate espionage.

Rationale: This logbook will allow the tracking of messages ensuring investigations can be carried our easily. Additionally, this can help resolve inter-employ conflicts.

SR-AU2. A secure third-party source to perform security audits.

Rationale: Security is tough to maintain and create requirements for. Integrating the use of a third-party auditor can ensure that the system is secure. Additionally, it will ensure that the system is following all standard security requirements.

5.6.5 Immunity Requirements

SR1. Prevents outside attacks, such as malicious hackers. [7]

Rationale: Authenticates each user before entering a chat. This ensures only the intended users have access to the chat and the companies trade secrets are safe.

5.7 Cultural and Political Requirements

5.7.1 Cultural Requirements

CP-C1. User profile images must adhere to guidelines prohibiting the use of culturally insensitive imagery, including symbols, flags, or gestures that may be considered offensive or discriminatory based on ethnicity, religion, or sexual orientation.

Rationale: By enforcing guidelines for user-generated content, the application maintains a welcoming and inclusive environment, fostering positive interactions among users from various cultural backgrounds.

CP-C2. The application should provide users with the option to customize their display names within parameters that exclude discriminatory or offensive terms. A list of unacceptable words should be referenced to prevent the use of offensive language.

Rationale: Enforcing responsible and respectful user behavior by restricting the use of offensive language or terms helps foster a positive and inclusive environment within the application.

CP-C2. The application must incorporate a feature that allows users to report abusive or inappropriate behavior, with the ability to cancel ongoing communication sessions or block offending users.

Rationale: Promoting a safe and harassment-free environment within the application encourages user trust and engagement, contributing to a positive user experience.

5.7.2 Political Requirements

CP1-P1. The system shall incorporate a feature allowing authorized government entities to broadcast emergency messages to all users within the system, ensuring timely dissemination of critical information during emergency situations such as natural disasters, public safety threats, or national security emergencies.
Rationale: Facilitating the dissemination of emergency messages from government enhances public safety and crisis response capabilities within the community.

5.8 Legal Requirements

5.8.1 Compliance Requirements

LR-COMP1. All personal information must be kept secured and protected.
Rationale: To ensure compliance with legal requirements, such as privacy right and data protection.

LR-COMP2. Users must be informed of the use of their personal information, user agreement, and the app's terms and conditions.
Rationale: To ensure that users are aware of how their personal information will be used by the app.

LR-COMP3. All personal information and sensitive data will be collected and used for a legitimate purpose and reason.
Rationale: This will ensure that the application uses collected data for its intended use and do not misuse or share sensitive information for other purposes.

LR-COMP4. The application must be under Intellectual Property Rights Protection and relevant policies must be enforced.
Rationale: This measure will protect intellectual property rights, such as copyrights, trademarks, and patents for the application. This will help prevent infringing on the intellectual property rights and violations.

5.8.2 Standards Requirements

LR-STD1. Fulfill all data privacy laws in region of operation.
Rationale: Legislation provides a standard for everything. This standard must be upheld when it comes to protecting the user's data. These guidelines are around sharing data and accessing user data.

LR-STD2. The content and features are accessible for all audiences.
Rationale: Employees with impairments require accessible features throughout the app. This would involve having larger font sizes, and making sure that the UI is clear and visible. Companies have a responsibility to make sure that tools that are mandated for use are accessible and usable for all audiences.

LR-STD3. The application's internal storage should be used to store any personal or sensitive data.
Rationale: This is a general standard practiced by many app and enforced by Google.

LR-STD4. The application must follow encryption standards and protocol.
Rationale: This will help protect confidentiality and integrity of users and communication channels, especially when sharing sensitive information, company secrets, or personal information.

6 Innovative Feature

The selected innovative feature to integrate into **SecureChat** is an option to set and send automated response to manage the user's availability and streamline communication during out-of-office hours. Upon logging into the application, there will be an option to set out-of-office hours, which will allow users to set the start and end date and time that they would be unavailable. For example, they can indicate their unavailability from February 18th at 9am to February 19th at 5pm. Then, in the text box, they can write down their automated response message. For example, "Thank you for your message. I am currently out of the office and will be back on February 20th at 9am. For any urgent inquiries, please contact Sarah Smith at sarahsmith@abc.ca. I will respond to your message

shortly. Thank you". This feature would allow users to set their availability status and indicate days or times when they are unavailable for communication. Moreover, this would ensure that other users are informed of the recipient's unavailability by sending an automated response. Upon receiving a message during the user's designated unavailable period, **SecureChat** will automatically send the response to notify the sender of their unavailability while providing information on when they will next be available for communication. This innovative feature can greatly reduce frustration and facilitate clear communication more efficiently. In doing so, it will enhance user experience, improve communication, and promote effective time management within the company.

Other innovative features the team came up with include:

- Flagging inappropriate messages and informing **HR**.
- Creating group chat.
- Having smart reply suggestions, such as "yes" or "no" for questions, "thank you", "I will get back to you shortly", etc.
- Sending emojis, pictures, or videos.
- Having an option to voice call or video call.
- Changing display settings, such as dark mode, different backgrounds, animations, text size.
- Adding a speech to text function.
- Translating different languages to address language barriers.
- Including interactive polls, questionnaires, and surveys.

A Division of Labour

Include a Division of Labour sheet which indicates the contributions of each team member. This sheet mustbe signed by all team members.

Samih Dalvi:

- Introduction
- Section 1.1: Purpose
- Section 2.6: Apportioning of requirements
- Came up with some of the BE's
- Completed BE's 1 &2 and their global scenarios
- Completed all sections of 5.4 & 5.5 of NFR's:
    - Expected Physical Environment
    - Requirements for Interfacing with Adjacent Systems
    - Productization Requirements
    - Release Requirements
    - Maintenance Requirements
    - Supportability Requirements
    - Adaptability Requirements
- Helped with preliminary editing and formatting alongside Pranav

Pranav Kalsi

- Formatted and added references.
- Product perspective
    - Put the product into perspective with other related products, i.e., context
    - If the product is independent and totally self-contained, it should be stated here

    - If the SRS defines a product that is a component of a larger system, then this subsection should relate the requirements of that larger system to the functionality of the software being developed. Identify interfaces between that larger system and the software to be developed.
    - A block diagram showing the major components of the larger system, interconnections, and external interfaces can be helpful.
- Business Event 5 (Deleting a message) and corresponding global scenario.
- Look and Feel Non-Functional Requirements
    - Appearance Requirements
    - Style Requirements
- Security Requirements
    - Access Requirements
    - Integrity Requirements
    - Privacy Requirements
    - Audit Requirements
    - Immunity Requirements
- Was apart of 1st editing session with Samih.
- Was apart of 2nd editing session with Chengze, Luna, James.
- Assisted in adding to team member parts.

Luna Aljammal

- Section 1.5: Overview of SRS
- Section 2.2: Product Functions
- Section 4: Business Event #3: Initiating a Chat
- Section 5: Non-Functional Requirements: Performance Requirements (5.3.1- 5.3.8)
    - Speed and Latency Requirements
    - Safety-Critical Requirements
    - Precision or Accuracy Requirements
    - Reliability and Availability Requirements
    - Robustness or Fault-Tolerance Requirements
    - Capacity Requirements
    - Scalability or Extensibility Requirements
    - Longevity Requirements
- Brainstormed business events and contributed to main ones to further explore
- Shared ideas for an innovative feature
- Formatted citations
- Helped with finalizing formatting of the document
- Participated in the team editing session

Chengze Zhao

- Section 2.3: User Characteristics
- Section 2.4: Constraints
- Section 4: Functional Requirements
    - Come up with Business Event #7 Chat logbook request
    - Fixing Business Event #6 Delete account/leave company
- Section 5: Non-Functional Requirements --- Usability and Humanity Requirements
    - Ease of Use Requirements
    - Personalization and Internationalization Requirements
    - Learning Requirements
    - Understandability and Politeness Requirements
    - Accessibility Requirements
- Section 5: Non-Functional Requirements --- Cultural and Political Requirements

- Cultural Requirements
- Political Requirements

Ganghoon (James) Park

- Section 1.2: Scope
- Section 2.2: State diagram
- Section 4: Business Event #4: Set out-of-office hours and generate automated response (innovative feature)
- Section 5: Non-Functional Requirements: Legal Requirements
- Section 6: Innovative Features
- Brainstormed business events and contributed to main ones to further explore
- Formatted document
- Joined team meetings to edit and review the document
- Participated in the team editing session
- Contributed to team discussions and suggested ideas

Jack Walmsley:

- Completed section 3: Use Case Diagram
  - Wrote PlantUML and description of diagram
- Completed business event BE 6: Delete Account
- Completed section 2.5: Assumption and Dependencies
- General document formatting