

SFWR ENG 3A04 Deliverable #1

Tutorial Number: T02

Group Number: G03

Group Members:

- Takhtar, Tarnveer (Captain)
- Hannoufa, Akram
- Patel, Aryan
- Damjanovski, Alexander
- Bradbury, Matthew

1 Introduction

This SRS (Software Requirements Specification) document aims to provide an overview of the specifications and requirements of *LockTalk*, a secure chat *Android* application. This document outlines the purpose, scope, and key terminology of the system. It also outlines the product perspective and functions, as well as user characteristics, constraints, assumptions, and dependencies. A use case diagram is included along with a list of both functional and non-functional requirements.

1.1 Purpose

The Software Requirements Specification (*SRS*) for *LockTalk* aims to outline the development of the secure chat *android* application. It is designed to provide a comprehensive guide for the project's specifications and requirements.

The intended audience for this *SRS* includes the development team, project managers, and stakeholders involved in the creation and implementation of the secure chat *android* application.

1.2 Scope

LockTalk is a secure chat application that will allow employees to send messages to other employees, using company-issued *Android* devices.

The main features of *LockTalk* include the capability for sending group messages and tracking and securely storing chat log history. *LockTalk* ensures security through the

implementation of a symmetric-key crypto system for message encryption and decryption. Secure communication is also protected with the use of a Key Distribution Centre (*KDC*) server and a mediated authentication protocol, by managing user access to the service.

The relevant objectives associated with the application would be implementing advanced encryption and security measures in order to allow *LockTalk* to ensure that all communications remain confidential. Additionally the secure storage of chat logs provides a dependable record of all communications that occur between employees aiding in compliance and oversight of usages. Furthermore the unique *geofencing* feature adds an additional security layer by restricting access to sensitive communication based on the user's location.

The overall goal of the application is to reduce the threat of corporate espionage. This is done by improving internal communication by making it easier to connect and collaborate securely. The information communicated between users would remain secure, reducing the risk of data breaches to the outside world. Another goal of *LockTalk* is to increase the adoption of company-provided devices by offering a communication tool on *Android* devices encouraging the use. Lastly, it would aid in meeting compliance requirements by securely logging all communications and implementing strict security protocols.

1.3 Definitions, Acronyms, and Abbreviations

Android: Mobile Operating System

API: Application Programming Interface

APK: Android Package Kit, compiled program to be installed

GeoFencing: Access and use is limited to a certain geographical region

KDC: Key Distribution Centre

LockTalk: A secure chat Android application – the main project being built from this SRS

SKCS: Symmetric-Key Crypto-System

SRS: Software Requirements Specification

1.4 References

- [1] Snapchat, "When does Snapchat delete snaps and Chats?," Snapchat, <https://help.snapchat.com/hc/en-us/articles/7012334940948-When-does-Snapchat-delete-Snaps-and-Chats> (accessed Feb. 14, 2024).
- [2] Signal, "Speak freely," Signal Messenger, <https://signal.org/> (accessed Feb. 12, 2024).
- [3] "Recommendations for Android Architecture : android developers," Android Developers, <https://developer.android.com/topic/architecture/recommendations> (accessed Feb. 15, 2024).
- [4] I. Team, "Network latency - common causes and best solutions," IR, <https://www.ir.com/guides/what-is-network-latency> (accessed Feb. 15, 2024).
- [5] GPS.gov, "GPS accuracy," GPS.gov: GPS Accuracy, <https://www.gps.gov/systems/gps/performance/accuracy/> (accessed Feb. 16, 2024).
- [6] R. Bongula, "The why and how of High Availability Infrastructure," ConnectWise, <https://www.connectwise.com/blog/engineering/the-why-and-how-of-high-availability-infrastructure> (accessed Feb. 14, 2024).
- [7] "Recommended minimum SDK version for Android Projects," Brand mark MeguMethod, <https://www.megumethod.com/blog/recommended-minimum-sdk-version-for-android-projects> (accessed Feb. 15, 2024).
- [8] M. Chojnowska, "Best practices for developing large-scale applications," Sunscrapers, <https://sunscrapers.com/blog/development-best-practices-large-scale-applications/> (accessed Feb. 15, 2024).
- [9] "How Often Should You Update Your App?" Accessed: Mar. 10, 2024. [Online]. Available: <https://www.appify.digital/post/how-often-should-you-update-your-app>
- [10] "Declare your app's data use : App quality : android developers," Android Developers, <https://developer.android.com/privacy-and-security/declare-data-use> (accessed Feb. 15, 2024).
- [11] Xu, Z., Filtering offensive language in online communities using grammatical relations. Paper presented at 7th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference, CEAS 2010, Redmond, WA, United States. (accessed Feb. 15, 2024).

[12] “Restricted content - play console help,” Google, <https://support.google.com/googleplay/android-developer/topic/9877466> (accessed Feb. 15, 2024).

[13] “Privacy, deception and device abuse - play console help,” Google, <https://support.google.com/googleplay/android-developer/topic/9877467> (accessed Feb. 15, 2024).

[14] “Spam and minimum functionality - play console help,” Google, <https://support.google.com/googleplay/android-developer/topic/9876964> (accessed Feb. 15, 2024).

[15] “Malware - play console help,” Google, <https://support.google.com/googleplay/android-developer/topic/9975838> (accessed Feb. 15, 2024).

[16] “Mobile unwanted software - play console help,” Google, <https://support.google.com/googleplay/android-developer/topic/9969691> (accessed Feb. 15, 2024).

1.5 Overview

Overall Product Description (Section 2) gives the overall product description including product perspective, product functions, user characteristics, constraints, assumptions and dependencies, and apportioning of requirements. The next section (Section 3) outlines the Use Case Diagram for the main use case scenarios of *LockTalk*. Viewpoints and key business events are then described in Section 4, along with the principal functional requirements of the system. Non-Functional Requirements are broken down into a series of categories in Section 5, with the categories being: 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. There is a final appendix-style section, Section A that contains the Division of Labour.

2 Overall Description

2.1 Product Perspective

Related products to *LockTalk* include other messaging applications available on *Android* such as WhatsApp, Facebook Messenger, Discord, Snapchat, Instagram, and Signal. *LockTalk* aims to consolidate the security features present in some of these applications into a singular messenger that can leverage each feature to create the most secure environment possible. Some features, such as the “vanishing” messages seen on Snapchat and Instagram [1], will be expanded upon by *LockTalk* so that messages can be set to vanish not only after they are read by the user (as is the case for the latter applications) but can also be set to vanish after a predetermined amount of time.

Signal is a messaging application that fills a similar niche to *LockTalk*, marketing itself as an extremely secure messenger featuring end-to-end encryption, scheduled send of messages, vanishing messages, automatic face blurring in photos, and a separate passcode for access to the application [2]. Notably, Signal generates encryption keys on the user devices and does not store them on external servers. The implementation of *LockTalk* only on devices administered by a company will allow the application to use similar features in an even more secure manner. For example, confirmation that a user is who they really claim to be can be done via in-person QR code scan to initiate messaging, or manually administered by the company’s IT department. Further, user registration will not require the user’s personal phone number as is the case with Signal, further anonymizing the accounts.

LockTalk is fully self-contained within the company environment. It will have to interface with certain external applications/databases that are administered by the company, but nothing beyond the company's own technological environment. For certain features, such as authorizing uses for certain employees, or associating a specific work phone with a specific employee, *LockTalk* will have to interface with company databases that store this information. Since *LockTalk* will not store the personal information of its users it will have to rely on the company's existing infrastructure for this.

1. Client Application (*Android* App):

This is the user interface where employees interact. It handles chat functionalities, encryption/decryption of messages using symmetric-key cryptography, and communicates with the Key Distribution Centre (*KDC*) for key management.

2. Key Distribution Centre (*KDC*) Server:

A central server responsible for generating, storing, and distributing encryption keys to clients. It frequently updates and sends new keys to registered clients, ensuring secure communication.

3. Authentication Server:

Part of the *KDC* or a separate entity, this server implements a mediated authentication protocol like Kerberos. It authenticates users before they access keys from the *KDC*.

4. Database/Storage:

A secure server or database system that stores chat history logs. Each log contains identifiers of communicating agents, timestamps, and the encrypted chat content.

5. Administrative Backend:

For managing users, overseeing application security, and possibly implementing features like remote wipe or activity monitoring.

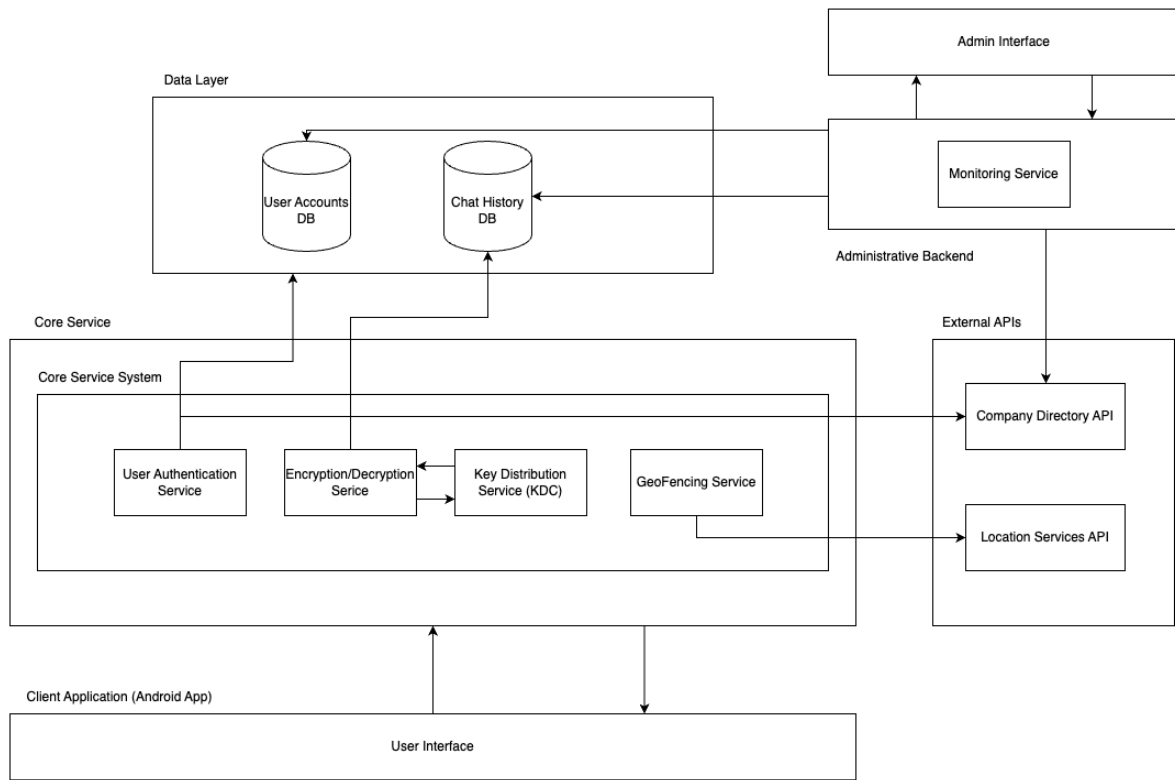


Figure 1: System Diagram

2.2 Product Functions

The *LockTalk* application will encompass several key modules: User Messaging Service, Account Management, Encryption Service, and *Geofencing* Control. The primary functionalities in the User Messaging Service module include individual messaging, group chats, secure chat logs, and encryption protocol management. The Account Management module is responsible for account creation, updates, and authentication processes. The Encryption Service module ensures message security through the application of a symmetric-key crypto-system. Lastly, the unique *Geofencing Control* module (**innovative feature**) implements location-based access restrictions and tracking information for enhanced physical security of communications.

Modules	Functions
User Messaging Service	<ul style="list-style-type: none"> • Individual Messaging <ul style="list-style-type: none"> ◦ Allow users to send private messages to each other • Group Chat <ul style="list-style-type: none"> ◦ Enables multiple users to communicate in a common chat room • Secure Chat Logs <ul style="list-style-type: none"> ◦ Maintains a record of all communications within the platform • Manage Encryption <ul style="list-style-type: none"> ◦ Handles the symmetric--key encryption protocol for securing messages
Account Management	<ul style="list-style-type: none"> • Create Account <ul style="list-style-type: none"> ◦ Enables new users to register for the service • Update Account <ul style="list-style-type: none"> ◦ Allows users to update their personal and security settings • Authentication <ul style="list-style-type: none"> ◦ Manages user login and ensures that access is restricted to authorized users only
Encryption Service	<ul style="list-style-type: none"> • Symmetric-Key Crypto-System (SKCS) <ul style="list-style-type: none"> ◦ Secures messages with a symmetric encryption algorithm to ensure confidentiality and integrity
Geofencing control	<ul style="list-style-type: none"> • Location-Based Access <ul style="list-style-type: none"> ◦ Restricts access to certain conversations unless the user is within a predefined geographical area • Enforce Geofencing Policies <ul style="list-style-type: none"> ◦ Applies the company's <i>geofencing</i> policies to control the flow of information based on location

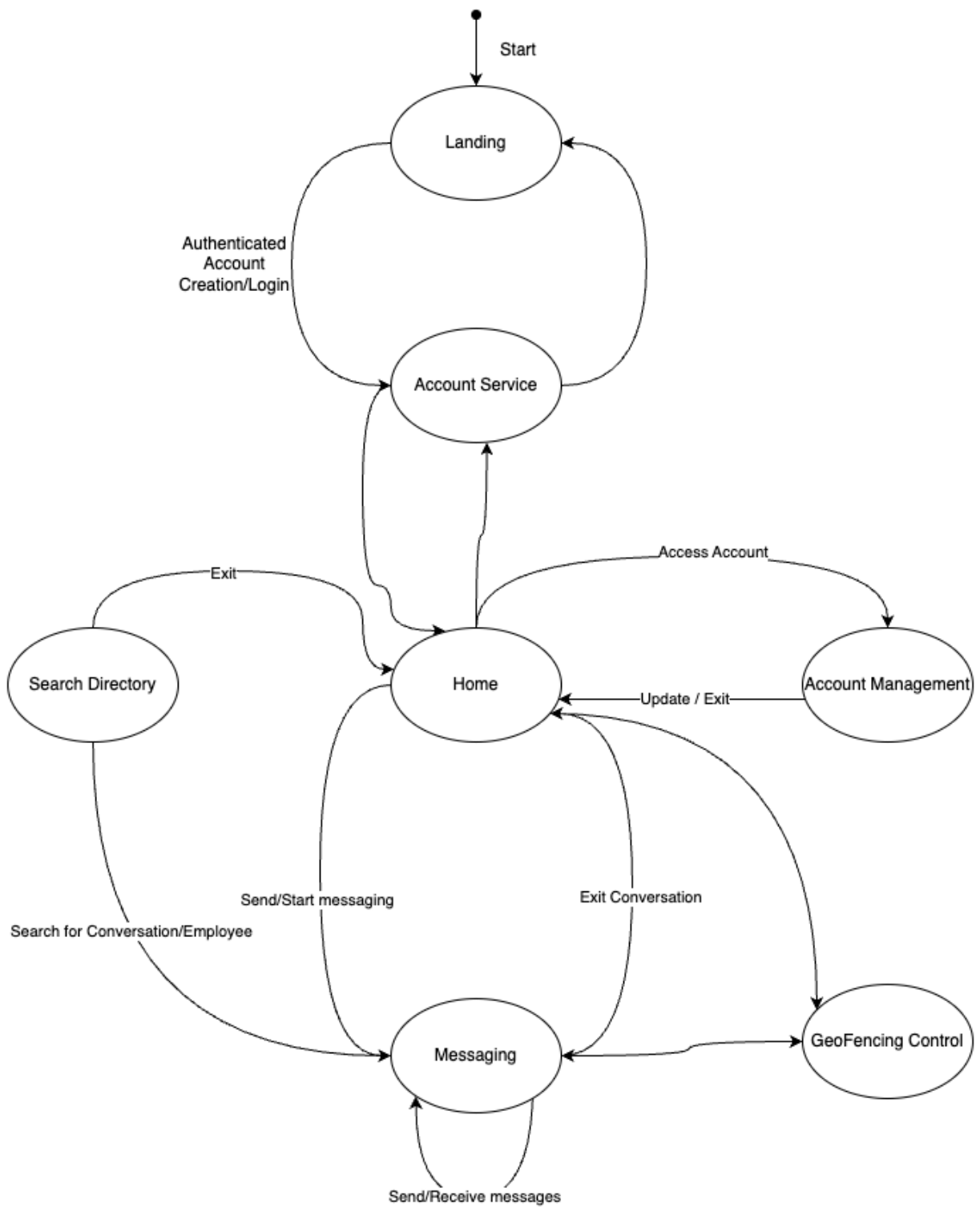


Figure 2: State Diagram

2.3 User Characteristics

1. Education Level: Basic Literacy Skills

- Users are expected to have fundamental literacy skills, including the ability to listen, speak, read, and write, facilitating smooth interaction with the app.

2. Experience: None Required

- The app's user-friendly design ensures that even employees who are new to the app can navigate and utilize its features without significant issues.

3. Age Requirement: 18 Years or Older

- Users must meet the company's minimum age requirement for employment to use this application.

4. Employment Status: Company Employees

- Users will be exclusively employees of the company, spanning various departments and teams.

5. Technical Proficiency: Basic Digital Literacy

- Users should have a basic understanding of operating digital devices, particularly mobile phones, which will aid in the adoption and use of the app.

6. Ease of Use: User-Friendly Interface

- *LockTalk* is tailored to ensure a seamless onboarding process so that new users can quickly set up and begin using the application with minimal training.

2.4 Constraints

This section outlines the constraints that will shape the development of the *LockTalk* application:

1. **Budget:** Financial resources allocated to the *LockTalk* project will dictate the scope of technology and features implemented. Strict adherence to the budget is essential.
2. **Timeline Constraints:** The project's development is bound by a fixed timeline, which influences the project's scale and impacts the availability of resources and development phases.
3. ***Android* Development Best Practices:** Adherence to established *Android* development protocols and best practices will guide the app's creation, affecting design and feature set [3].
4. **Accessibility Design Considerations:** The app must be accessible to all users, requiring a design that accommodates various needs and abilities, potentially limiting design complexity.
5. **Device Capabilities:** The functionality of *LockTalk* may be limited by the specific features and capabilities of the company-issued *Android* devices.
6. **Legal Constraints:** Legal guidelines provided by the company will impose restrictions on app content, data handling, and compliance requirements.
7. **IT Restrictions:** The IT department's policies on software integration, security, and network compatibility will directly impact the app's infrastructure and capabilities.
8. **Marketing Requirements:** The marketing team's vision for brand alignment and user engagement strategies will influence the app's user interface and experience design.

2.5 Assumptions and Dependencies

Assumptions:

1. **Uniform User Devices:** The assumption that all company-issued *Android* devices will have the same operating system version and hardware capabilities, which is essential for uniform operation.
2. **Reliable Internet Connectivity:** Continuous and reliable Internet or LTE connectivity is assumed for the Individual Messaging, Group Chat, and Secure Chat Logs functions to operate effectively.
3. **Consistent Encryption Protocols:** The Manage Encryption function depends on the assumption that the symmetric-key encryption standards will not undergo significant changes that could affect the app's security features.
4. **Geolocation Accuracy:** For the *Geofencing Control* module to work effectively, it is assumed that the device's location services are accurate and reliable. This also means location services are enabled for the devices.
5. **User Authentication:** The Authentication function assumes that the company's user directory services are always available and accurate for validating user credentials.

Dependencies:

6. **Company Policy:** The employees must follow the company's policies regarding app usage.
7. ***Android API* Stability:** The application's performance, particularly for features like Location-Based Access and Enforce *Geofencing* Policies, is dependent on the stability and continuity of the *Android APIs*.
8. **Regulatory Compliance:** The Encryption Service module's effectiveness is contingent upon compliance with global encryption regulations, which could change and impact requirements.
9. **Third-Party Service Reliability:** The app relies on third-party services for the Symmetric-Key Crypto-System (Java module). Any disruptions or changes in these services could affect the app's functionality.

10. System Integration Compatibility: The application's ability to integrate with the company's existing IT infrastructure is a dependency that could be impacted by changes in the company's IT environment.
11. Device Security Policies: For the *geofencing*, it is assumed that the security policies on the company-issued devices allow for the necessary permissions to enforce *geofencing*.

2.6 Apportioning of Requirements

1. Multilingual Support: Initially, *LockTalk* will be available exclusively in English. Future versions will incorporate additional languages of the employees within the company.
2. Accessibility Features: A future update of *LockTalk* will include features that assist users with different abilities. These may include voice-to-text, text-to-speech functions, and enhanced visual aids for users who require assistance with the app's navigation.
3. Group Communication Features: This will allow for larger group channels for communication between employees. It will also allow for separate channels to be created with multiple users.

3 Use Case Diagram

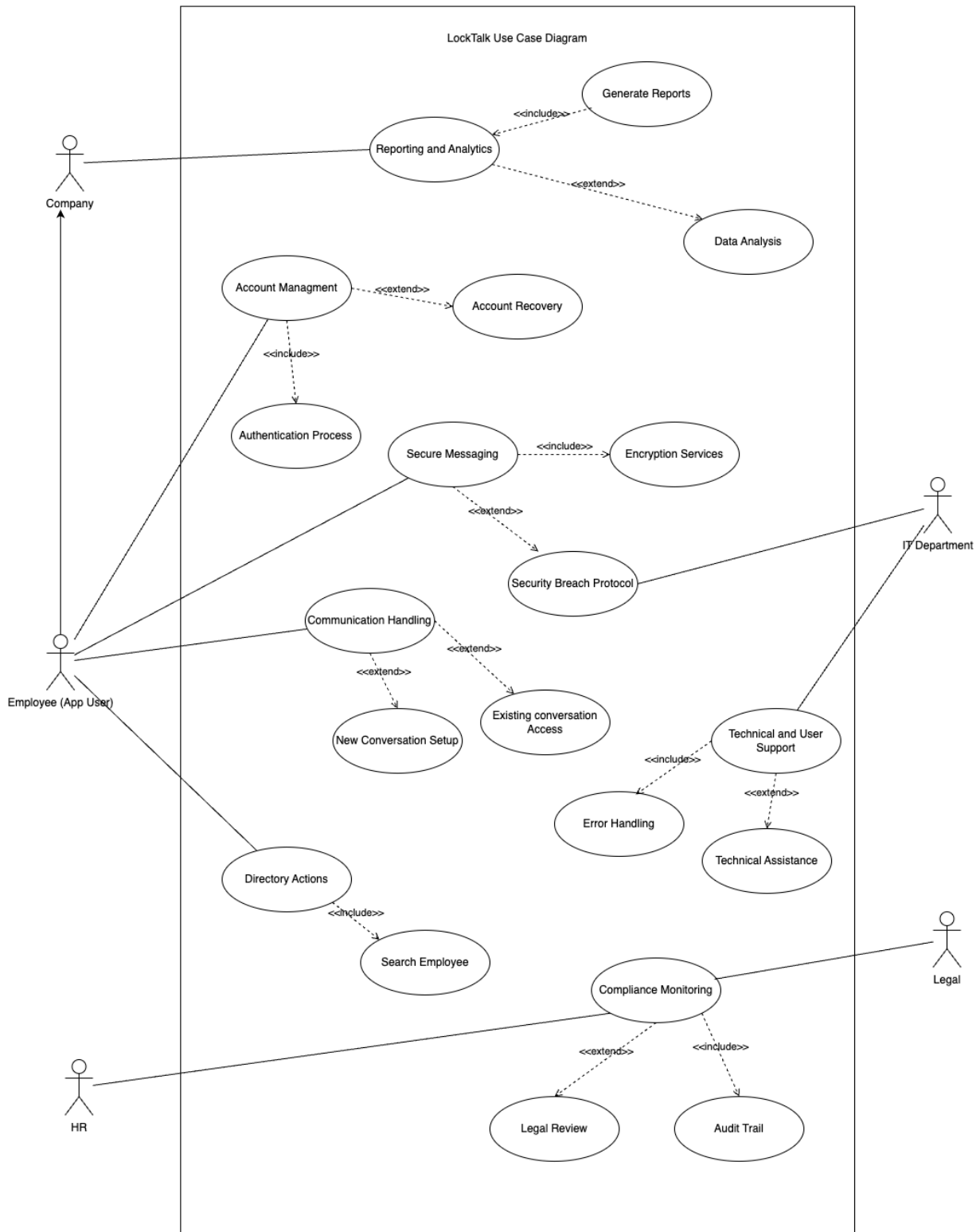


Figure 3: Use Case Diagram
(added connection between User and Employee)

4 Functional Requirements

The business events we will consider include:

- BE1 Create account
- BE2 Login
- BE3 Start a new conversation with an employee
- BE4 Access an existing conversation with an employee
- BE5 Attempt screenshot/screen recording of app
- BE6 Search directory
- BE7 Editing account details
- BE8 Sending message

The Viewpoints we will consider are:

- VP1 Employee
- VP2 Company
- VP3 IT Department
- VP4 Legal
- VP5 HR

Business Events

BE1. Create Account #1

Precondition: Employee has no existing *LockTalk* account associated with their employee ID

VP1. Employee #1

Main Success Scenario

1. System asks for employee ID
2. System sends secure link to employee email
3. System verifies link accessed by user
4. Employee sets account password
5. System authenticates user

Secondary Scenario

- 1i. Employee ID is invalid
 - 1i.1 Create account failed
- 3i. Expired/Used link
 - 3i.1 Create account failed
- 3ii. Link accessed from different device
 - 3ii.1 Create account failed

VP2. Company #2

N/A

VP3. IT Department #3

- 2i. System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.
- 3i. System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.

5i. System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.

VP4. Legal #4

N/A

VP5. HR #5

N/A

Global Scenario:

Precondition: Employee has no existing *LockTalk* account associated with their employee ID

Main Success Scenario

1. System asks for employee ID
2. System sends secure link to employee email
3. System verifies link accessed by user
4. Employee sets account password
5. System authenticates user

Secondary Scenario

- 1i. Employee ID is invalid
 - 1i.1 Create account failed
 - 1i.2 System shows an error page and prompts the user to contact the IT Department via the chat should they require any assistance.
- 3i. Expired/Used link
 - 3i.1 Create account failed
 - 3i.2 System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.
- 3ii. Link accessed from different device
 - 3ii.1 Create account failed

BE2. Login #2

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

VP1. Employee #1

Main Success Scenario

1. Employee enters authentication details.
2. System verifies employee entered data, and device used to login
3. System authenticates user

Secondary Scenario

- 2i. Employee credentials are invalid
 - 2i.1 System rejects login
- 2ii. Employee attempts login with unauthorized device
 - 2ii.1 System rejects login

VP2. Company #2

N/A

VP3. IT Department #3

2i. System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.

3i. System should show an error page and prompt the user to contact the IT Department via the chat should they require any assistance.

VP4. Legal #4

N/A

VP5. HR #5

N/A

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Employee enters authentication details.
2. System verifies employee entered data, and device used to login
3. System authenticates user

Secondary Scenario

- 2i. Employee credentials are invalid:
 - 2i.1 System rejects login.
 - 2i.2 System shows an error page and prompts the user to contact the IT Department via chat if assistance is required.
- 2ii. Employee attempts login with unauthorized device:
 - 2ii.1 System rejects login.
 - 2ii.2 System shows an error page and prompts the user to contact the IT Department via chat if assistance is required.

BE3. Start a new conversation with an employee #3

Precondition: Employee is logged into *LockTalk* Account.

VP1. Employee #1

Main Success Scenario

1. Employee selects name or ID of employee they wish to chat with
2. System redirects to existing chat with employee if it exists
3. New chat is created between the two employees

Secondary Scenario

- 1i. Requested employee does not have a valid account
 - 1i.1 System creates chat and logs conversation
 - 1i. 2 System prompts requested employee to create an account and notifies them they have incoming messages
- 3i. System fails to create a new chat
 - 3i. 1 Create chat failed

VP2. Company #2

N/A

VP3. IT Department #3

3i. System should show an error page and notify IT with the issue.

VP4. Legal #4

N/A

VP5. HR #5

N/A

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Employee selects name or ID of employee they wish to chat with
2. System redirects to existing chat with employee if it exists
3. New chat is created between the two employees

Secondary Scenario

- 1i. Requested employee does not have a valid account
 - 1i.1 System creates chat and logs conversation
 - 1i. 2 System prompts requested employee to create an account and notifies them they have incoming messages
- 3i. System fails to create a new chat
 - 3i. 1 Create chat failed
 - 3i. 2 System shows error page and notifies IT with issue

BE4. Access an existing conversation with an employee #4

Precondition: Employee is logged into *LockTalk* Account, and has a conversation history with an employee.

VP1. Employee #1

Main Success Scenario

1. Employee accesses list of existing conversations
2. Employee selects desired conversation
3. Employee views chat history or sends a new message

Secondary Scenario

- 1i. There is no history of chats
 - 1i.1 System prompts user to start a new chat

VP2. Company #2

Main Success Scenario

1. Company, places request chat logs of employee(s) from IT
 - 1i. Company receives requested log

Secondary Scenario

1. Company, places request chat logs of employee(s) from IT
 - 1i. Company gets notified indicating no such logs exist

VP3. IT Department #3

Main Success Scenario

1. IT gets request to send an employee's chat logs
2. IT gathers chat logs (if any) and forwards them to the requesting authorized Company party.

Secondary Scenario

- 1i. Request comes from unauthorized party
 - 1i.1 Request is denied, HR notified

VP4. Legal #4

N/A

VP5. HR #5

Main Success Scenario

1. HR is notified of unauthorized request of logs from IT
2. HR contacts the person(s) in question that made the request

Secondary Scenario

- 1i. No such infraction occurs
- 1i.1 HR is not notified

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario:

- 1. Employee accesses the list of existing conversations.
- 2. Employee selects the desired conversation.
- 3. Employee views chat history or sends a new message.

Secondary Scenario:

- 1i. There is no history of chats:
 - 1i.1 System prompts the user to start a new chat.
- 2. Company places a request for chat logs of employee(s) from IT.
 - 2i. Company receives the requested log, if available.
 - 2ii. If no such logs exist, Company gets notified accordingly.
- 3. IT receives a request to send an employee's chat logs.
 - 3i. IT gathers chat logs (if any) and forwards them to the requesting authorized Company party.
 - 3ii. If the request comes from an unauthorized party, it is denied, and HR is notified.
- 4. HR is notified of unauthorized requests of logs from IT.
 - 4i. HR contacts the person(s) in question that made the request.
 - 4ii. If no such infraction occurs, HR is not notified.

BE5. Attempt screenshot/screen recording of app #5

Precondition: Employee has app installed.

VP1. Employee #1

Main Success Scenario

- 1. Employee opens the app on their device.
- 2. Employee attempts to screenshot/screen record.
- 3. App detects this attempt and blocks it automatically.

VP2. Company #2

N/A

VP3. IT Department #3

Main Success Scenario

- 1. IT is notified a screenshot attempt was made.
- 2. IT is provided with the contents of the attempted screenshot.
- 3. IT decides if the content warrants providing Legal and HR with the screenshot information and the ID of the corresponding employee.

Secondary Scenario

- 1i. No such infraction occurs.
 - 1i.1 IT is not notified.

VP4. Legal #4

1. Legal is notified with the employee ID and screenshot contents.

VP5. HR #5

1. HR is notified with the employee ID and screenshot contents.

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Employee opens the app on their device.
2. Employee attempts to screenshot/screen record.
3. App detects this attempt and blocks it automatically.

Secondary Scenario

- 1i. No such infraction occurs:
 - 1i.1 IT is not notified.
1. IT is notified a screenshot attempt was made.
 - 1i. IT is provided with the contents of the attempted screenshot.
 - 1ii. IT decides if the content warrants providing Legal and HR with the screenshot information and the ID of the corresponding employee.
2. Legal is notified with the employee ID and screenshot contents.
3. HR is notified with the employee ID and screenshot contents.

BE6. Search directory #6

Precondition: Employee is logged into *LockTalk* Account.

VP1. Employee #1

Main Success Scenario

1. Employee searches directory for employee via name/employee id.
2. System shows matching results if any exist.
3. Employee can view employee details and has the option to start a chat.

Secondary Scenario

- 2i. There are no results.
 - 2i.1 Employee must change their search term.

VP2. Company #2

N/A

VP3. IT Department #3

N/A

VP4. Legal #4

N/A

VP5. HR #5

N/A

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Employee searches the directory for an employee via name/employee ID.
2. System shows matching results if any exist.
3. Employee can view employee details and has the option to start a chat.

Secondary Scenario

- 2i. There are no results.
 - 2i.1 Employee must change their search term.

BE7. Editing account details #7

Precondition: Employee is logged into *LockTalk* Account.

VP1. Employee #1

N/A

VP2. Company #2

N/A

VP3. IT Department #3

N/A

VP4. Legal #4

Main Success Scenario

1. Legal finds employee via the directory.
2. Legal can modify internal data fields: salary, contract
3. Legal saves profile.

Secondary Scenario

- 1i. Legal cannot locate the employee via the directory.
 - 1i.1 Desired employee details not found.
- 3i. Save failed.
 - 3i.1 System notifies the user that the message failed to send, with the option to retry.
 - 3i.2 Save successful.

VP5. HR #5

Main Success Scenario

1. HR finds employee via the directory.
2. HR can modify the following fields: position, missing bio information.
3. HR saves profile.

Secondary Scenario

- 1i. HR cannot locate the employee via the directory.
 - 1i.1 Desired employee details not found.
- 3i. Save failed.
 - 3i.1 System notifies the user that the message failed to send, with the option to retry.
 - 3i.2 Save successful.

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Legal finds the employee via the directory.
 - 1i. Legal can modify internal data fields such as salary and contract.
 - 1ii. Legal saves the profile.
2. HR finds the employee via the directory.
 - 2i. HR can modify fields such as position and missing bio information.
 - 2ii. HR saves the profile.

Secondary Scenario

- 1i. Legal cannot locate the employee via the directory:
 - 1i.1 Desired employee details not found.
- 2i. HR cannot locate the employee via the directory:
 - 2i.1 Desired employee details not found.
- 1/2ii. Save failed.
 - 1/2ii.1 System notifies the user that the save failed, with the option to retry.
 - 1/2ii.2 Save successful.

BE8. Sending Message #8

Precondition: Employee is logged into *LockTalk* Account.

VP1. Employee #1**Main Success Scenario**

1. Employee creates a new chat or opens an existing chat.
2. Employee types out a message and presses enter or the send button.
3. Message is sent to the chat recipient.

Secondary Scenario

- 3i. Message fails to send.
 - 3i.1 System notifies the user that the message failed to send, with the option to retry.
- 3ii. Message sends.

Global Scenario:

Precondition: Employee has an existing *LockTalk* account associated with their employee ID.

Main Success Scenario

1. Employee creates a new chat or opens an existing chat.

2. Employee types out a message and presses enter or the send button.

3. Message is sent to the chat recipient.

Secondary Scenario

3i. Message fails to send.

3i.1 System notifies the user that the message failed to send, with the option to retry.

3ii. Message sends.

5 Non-Functional Requirements

5.1 Look and Feel Requirements

5.1.1 Appearance Requirements

LF-A1. The system must use a consistent font across all user interfaces.

Rationale: The system should have consistent font usage across the app to ensure a clear and easy-to-read interface for the users.

LF-A2. The system shall display all buttons in uniform and contrasted colours.

Rationale: Buttons in the system must be uniform and contrasted in colour so that they are easy to view and clear to the user what is an interactive item or not.

LF-A3. The app must use clear and consistent brand elements that align with *LockTalk's* branding.

Rationale: *LockTalk's* branding elements will be used across the app to make it clear to the user that the system is offering a secure and easy-to-use experience.

LF-A4. The system must implement minimalist designs for all user interfaces.

Rationale: By implementing minimalist design through the app, the system ensures that the screens are not distracting, easy to navigate, and intuitive to use.

LF-A5. The system must avoid using highly saturated and bright colours/images in the user interfaces.

Rationale: A system with highly saturated colours and images will be distracting and confusing for the user to follow and use.

LF-A6. The system must display sent versus received messages in clearly distinct fonts and colours.

Rationale: The user must be able to clearly distinguish between the messages they have sent and the messages they have received.

5.1.2 Style Requirements

LF-S1. The system must indicate unread notifications on the home screen app icon

Rationale: Users must be able to see easily when they have unread messages within the app, even if the app is not open. This prevents important messages from being missed by the user.

LF-S2. The system must indicate unread notifications in the conversations menu

Rationale: Users must be able to see which conversations, if any, have unread notifications so that they can easily respond to any important messages they may receive.

LF-S3. Non-standard message types (vanishing, non-screenshot, etc) must be distinct from standard text messages and intuitively identifiable when they are received by the user

Rationale: Users must be able to visually distinguish between a regular text message and a higher priority, non-standard message in order to appropriately react/respond to it.

LF-S4. Timed/vanishing messages must clearly display to the user that they have a limited viewing window

Rationale: To maintain trust in the system, users must never unintentionally lose messages that they believed were permanent. All non-permanent messages must readily display this trait to the user so that they can react appropriately.

LF-S5. Non-standard messaging modes must be simple to use and navigate by the user

Rationale: Users must be able to effectively use all messaging modes intuitively to avoid mistaken data loss or other undesired messaging actions by the user.

LF-S6. The system should replicate icons/animations on existing messaging platforms for shared functions

Rationale: Users are assumed to have some familiarity with messaging applications, and this is leveraged by replicating some existing icons/animations to make system use as intuitive as possible. For example, unread notification icons, “vanish” mode indicators and selective image blurring have fairly universal styles that can be replicated.

LF-S6. The system must scale appropriately for different screen sizes

Rationale: The system must function as expected on varied screen sizes so that any *Android* device given to the user by their company is appropriate for use of this application.

5.2 Usability and Humanity Requirements

5.2.1 Ease of Use Requirements

UH-EU1. The system must provide an intuitive user interface design for easy navigation and operation.

Rationale: Users must be able to intuitively access the system's main features without a tutorial.

UH-EU2. The system must include an easily accessible feedback tool for bugs or other concerns encountered by users

Rationale: Users must have the ability to express any concerns that they feel with app usability, including but not limited to bugs, such that the development team can be made aware of and respond to these concerns.

UH-EU3. System notifications should be modifiable by the user to customize their experience

Rationale: Users must be able to personalize their system to reflect how they wish to use it; notifications can be made more "intrusive" (i.e. popup on screen) or less intrusive (banner at top of screen) depending on user preference. Certain priority conversations/messages can be given unique notification permissions at the user's discretion.

UH-EU4. The system must display clear error messages and prompts to assist users in troubleshooting issues

Rationale: Users must be able to identify when and why an error has occurred to promote maintainability and supportability.

5.2.2 Personalization and Internationalization Requirements

UH-P1. The system must have support for multiple languages

Rationale: The system must not limit its usability only to speakers of certain languages.

UH-P2. The system must allow the user to set their font size and colour preferences in the settings.

Rationale: Users can have varying levels of comfortability reading a certain font size (or font color), so users should be able to modify the font size of the text across all user interfaces.

5.2.3 Learning Requirements

UH-L1. Users shall be able to authenticate their account and log into the app to send a message within 10 mins of installing the application on their company-issued device

Rationale: The system should provide a seamless and user-friendly onboarding process, such that a user can authenticate and send a first message quickly.

5.2.4 Understandability and Politeness Requirements

UH-U1. Users must have the option to have “safe-text” turned on that filters any NSFW text in the texts they send and receive

Rationale: Some users may not be comfortable with explicit words being sent in conversations and should have the option to filter those words out of texts sent and received.

5.2.5 Accessibility Requirements

UH-A1. The system must allow users to activate disability features at their discretion to accommodate visual or auditory disabilities.

Rationale: The system must not limit its usage to users without disabilities, and must accommodate any accessibility requirements its users have.

UH-A2. The system must interface with device-level accessibility features such as screen readers and braille keyboards.

Rationale: Users with disabilities who use existing *Android* accessibility features must be able to maintain the usage of these features within the app to promote ease of use.

5.3 Performance Requirements

5.3.1 Speed and Latency Requirements

PR-SL1. The system should ensure low latency (<1s) for message delivery to ensure real-time communication [4]

Rationale: For sensitive data, users must be able to trust that messages are delivered safely and in a timely manner lest they lose confidence in the application. Any unnecessary delays will diminish user trust in the system.

PR-SL2. Minimal impact on device battery life and system resources

Rationale: The system must be as lightweight as possible so as to last an entire workday on the user’s work phone. Users must be able to rely on this phone for the exchange of important information at any time during the day, and undue battery/system resource usage may diminish this reliance.

PR-SL3. Optimized data compression techniques to reduce bandwidth usage

Rationale: For large companies, the system must still be scalable and responsive in its messaging, and thus it must maintain minimal bandwidth usage on the company network.

5.3.2 Safety-Critical Requirements

N/A

5.3.3 Precision or Accuracy Requirements

PR-PA1. The application's geo-tracking must be accurate to 4.9m to confirm the user's location within the designated area [5].

Rationale: 4.9m is the average accuracy of mobile phone GPS systems.

PR-PA2. The system must not truncate or modify any messages that are sent in the app.

Rationale: Users must be ensured that the messages they send are accurately captured and sent to the other user.

5.3.4 Reliability and Availability Requirements

PR-R1. High availability (>99.99%) to ensure the application is accessible whenever needed [6]

Rationale: The application must be at least as reliable as existing secure messaging applications, and must not experience unavailability for any circumstances within our control (ex. Cell network outages are not within our control, *LockTalk's* servers going down is within our control).

PR-R2. Redundancy and failover mechanisms to mitigate the impact of server or network failures

Rationale: In the event of unexpected server or cell network outages, the system must have mechanisms in place to protect data and promote its supportability for users and *LockTalk* employees.

PR-R3. Data integrity checks to prevent message corruption during transmission

Rationale: Users must not receive bad data via this messenger, as this would diminish their trust in the reliability of the system.

PR-R4. Automated backups and data recovery procedures to prevent data loss

Rationale: The system must back up important data and/or have mechanisms in place to recover it so that it is never lost in the event of unexpected outages.

5.3.5 Robustness or Fault-Tolerance Requirements

PR-RFT1. The system must be able to handle any exceptional or edge-case type text input by the user.

Rationale: It is not certain what input users will be sending to other users, and as such the system should be able to handle as wide a range of inputs as possible.

PR-RFT2. The system must be able to gracefully handle any network or system crashes to minimize any amount of data loss.

Rationale: As the stability of the network is not guaranteed, the system must have checks in place to minimize data/work loss in the case of any outages or crashes.

5.3.6 Capacity Requirements

PR-C1. The system must be able to handle upwards of 1000 users at a time sending messages.

Rationale: Given the context of the scenario, and the likely large size of the company, it must be assumed that the system will have many concurrent users on it, especially during working hours.

5.3.7 Scalability or Extensibility Requirements

PR-SE1. Ability to handle a growing number of users, messages, and concurrent connections

Rationale: The system must be able to handle usage by the entire staff of a large company, as well as be able to adapt to a changing team as employees leave and are hired. The system must be able to reliably handle all security permission changes in these situations.

PR-SE2. Efficient resource utilization to optimize costs and performance as the application scales

Rationale: The system must be built in an efficient manner to ensure smooth and relatively pain-free scaling and updates as the user base grows.

5.3.8 Longevity Requirements

PR-L1. The system must retain and store all sent messages from any user over time.

Rationale: As users will be leaving and joining the company over time, the system must maintain records of any messages sent on the app, even if an account is deleted or updated.

5.4 Operational and Environmental Requirements

5.4.1 Expected Physical Environment

N/A

5.4.2 Requirements for Interfacing with Adjacent Systems

OE-I1. The system must integrate with location-based services for accurate geo-location tracking and enforcement

Rationale: The system must be able to enforce its geotracking functionality by tracking user location.

OE-I2. The system must integrate with other workplace systems or applications as necessary

Rationale: For certain features and management by company staff, the system must be able to integrate into the existing company .

5.4.3 Productization Requirements

OE-P1. The system must be easily packaged and shipped to all applicable company employee devices.

Rationale: The company and its employees should not face any difficulties obtaining, installing, or using the app.

5.4.4 Release Requirements

OE-R1. Compatibility with *Android* operating system versions 8.0 and above [7]

Rationale: User device OS versions may not be standardized. Users must be able to use the application with different versions of *Android* on their devices. (Will depend on the specifics of the company-issued devices)

5.5 Maintainability and Support Requirements

5.5.1 Maintenance Requirements

MS-M1. The system must have a modular and well-documented codebase to facilitate ease of maintenance and future enhancements

Rationale: By following the best practices for large-scale app development the maintainability and consistency of the system will be easier to guarantee [8].

MS-M2. The system must undergo at least 2 monthly patches and updates to the system [9].

Rationale: By undergoing consistent software updates and fixes, the app will be in the best condition possible most of the time, especially refining and fixing bugs that may be inconveniencing users.

5.5.2 Supportability Requirements

MS-S1. Logging and monitoring capabilities to identify and troubleshoot issues quickly

Rationale: The system should provide live and up-to-date system and monitoring logs, with alerts in place to ensure rapid and accurate responses to any issues or faults that may arise.

MS-S2. The system must provide a method for users to easily provide feedback or report any bugs they encounter.

Rationale: If a user encounters an issue with the system or has a suggestion to improve their user experience, the system should provide a method to gather this feedback.

5.5.3 Adaptability Requirements

MS-A1. The system must be compatible and able to run on the most recent *Android* release.

Rationale: The app is expected to run on most *Android* devices, and should be back-compatible up to the oldest company-issued *Android* devices.

5.6 Security Requirements

5.6.1 Access Requirements

SR-AC1. The system requires users to allow GPS access and keep device location tracking on to access any application features.

Rationale: As geo-tracking is required for users to access the application, the device must have location tracking and GPS access for the application at all times.

SR-AC2. Users must set up their account with an approved company email.

Rationale: In order to maintain security, and dictate which users are permitted to message other users, an approved company email must be used to create *LockTalk* accounts and must remain associated with the account indefinitely.

SR-AC3. Users must log in with their approved company email, or set up login biometrics, for subsequent usage of the application

Rationale: User identity must be confirmed at each login, using the approved company email (for reasons outlined in SR-AC2).

5.6.2 Integrity Requirements

SR-I1. The system must provide end-to-end encryption of all messages to ensure confidentiality.

Rationale: All data must be end-to-end encrypted so that even in the event of a data breach, outside actors cannot read any data being sent over *LockTalk*.

SR-I2. The system must use a strong encryption algorithm (e.g., AES-256) to secure data.

Rationale: Outside actors must not be able to decrypt any data that they gain access to, and a strong encryption algorithm is required to enforce this.

SR-I3. The system must provide secure key management to prevent unauthorized access to encryption keys.

Rationale: As the encryption keys ensure the security and integrity of the system, their protection against outside threats must be ensured.

SR-I4. The system must provide protection against common security threats such as data breaches.

Rationale: The system should be secure as much as possible within the context of the app, as some threats are outside of the system's control, but the system should have security checks in place for common and expected security risks.

5.6.3 Privacy Requirements

SR-P1. The system must ensure protection of user privacy by limiting data collection and usage to only what is necessary for application functionality.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by limiting the amount of data being collected [10].

SR-P2. The system must provide a transparent privacy policy and user consent mechanisms for data processing activities

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by providing a clear description of all data being collected and ensure it gathers user consent.

5.6.4 Audit Requirements

SR-A1. The system must provide support for audit trails and compliance reporting to demonstrate adherence to regulatory requirements.

Rationale: If there are any legal requests to access the logs and history of the app, the system must provide an easy way to access these records for auditing.

SR-A2. The system must undergo regular security assessments and compliance audits to maintain compliance

Rationale: To ensure the safety and security offered by the app, the system must be put through regular and frequent security testing and assessments to ensure the system is up to code and meeting compliance requirements.

5.6.5 Immunity Requirements

SR-I1. The system must not accept any input that is not textual (or part of future accepted input types)

Rationale: There must be a strict guard on the types of input the messaging system can handle, so as to minimize the possible malicious acts that could be carried out with a wider range of accepted input types.

5.7 Cultural and Political Requirements

5.7.1 Cultural Requirements

CP-C1. The system must filter any culturally offensive or insensitive language from being sent or received.

Rationale: Using existing offensive language filtering systems, any culturally offensive language can be removed from messages, so that all employees using the app can feel comfortable and safe using the app. This filtering focuses specifically on culture, as there will be a separate filtering option for general offensive language filtering [11].

CP-C2. The system must provide a reporting system for users to report any offensive messages they receive from another user.

Rationale: Users should be able to report another user for using offensive language on the app, as it is a work-based app, and all users should be made to feel comfortable and safe using the app. Reporting also allows management to investigate the messages further.

5.7.2 Political Requirements

N/A

5.8 Legal Requirements

5.8.1 Compliance Requirements

LR-C1. The system must ensure that any data collected is kept secure and protected.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by protecting the data that is collected.

LR-C2. The system must ensure that the user is informed of any data that is being collected from them before it is collected.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by making it clear and well-known to the user what data is being collected by the system before it is collected.

LR-C3. The system must ensure that consent for data collection is acquired.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by ensuring it gathers user consent before collecting/storing data.

LR-C4. The system must ensure that only necessary data is collected.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by ensuring it is only collecting necessary and required data.

LR-C5. The system must ensure that collected data is only used for legal, audit, or company policy-related ways.

Rationale: Given the company's data privacy policies and Google's/*Android's* user data collection policies, the system must ensure it is compliant by ensuring the data gathered is only used for regulatory or legal purposes within the company.

5.8.2 Standards Requirements

LR-S1. The system must not violate any of the Developer Policy Center guidelines on Restricted Content.

Rationale: As the app will be an *Android* app, it must adhere to the Google Play Store Developer Policy Center guidelines [12].

LR-S2. The system must not be deceptive, malicious, or intended to abuse or misuse any network, device, or personal data to adhere to the Developer Policy Center guidelines on Privacy, Deception, and Device Abuse.

Rationale: As the app will be an *Android* app, it must adhere to the Google Play Store Developer Policy Center guidelines [13].

LR-S3. The system must be respectful and provide a minimum level of user experience to adhere to the Developer Policy Center guidelines on Spam and Minimum Functionality.

Rationale: As the app will be an *Android* app, it must adhere to the Google Play Store Developer Policy Center guidelines [14].

LR-S4. The system must not contain any malware, or violate any of the Mobile Unwanted Software principles to adhere to the Developer Policy Center guidelines on Malware & Mobile Unwanted Software (MUwS).

Rationale: As the app will be an *Android* app, it must adhere to the Google Play Store Developer Policy Center guidelines [15,16].

6 Innovative Feature

For LockTalk, our innovative feature lies in the implementation of geofencing management. Geofencing enables the app to track and timestamp when users access the platform based on their geographical location. It tracks and logs when and where a user has accessed a specific chat, and can also restrict access entirely to only designated areas, acting as an additional security measure and protecting company sensitive conversations. By integrating geofencing into LockTalk, we aim to offer users a unique and efficient way to communicate while also enhancing the app's usability and security features.

A Division of Labour

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

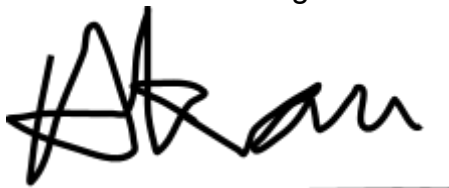
Patel, Aryan

- Final and Initial Writings of sections:
 - 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6
- Section 3 Use Case Diagram
- Discuss with Tarnveer and Matthew regarding Section 4 for Use Case Content
- Section 2.1 System Diagram
- Section 2.2 State Diagram
- Section 3 Use Case Diagram
- Overall view of report for any changes



Hannoufa, Akram

- Initial drafts of the following sections:
 - 1.1, 1.2, 1.3, 1.4, 1.5, 2.3, 2.4
 - Parts of 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8
 - IEEE references for the entire document
- Formatting, final overview
- Unique idea: automatically AI-enhanced messages. Enhance the message before sending it to the conversation



Takhtar, Tarnveer

- Initial Draft of Sections 1.4, 1.5, 2.1
- Formatting
- Section 4

A handwritten signature in black ink on a light gray background. The signature consists of two parts: a stylized 'Tarnveer' at the top and a larger, more complex 'Takhtar' below it, both written in a cursive script.**Bradbury, Matthew**

- Initial Draft of Sections 1.1, 1.5, 2.2
- Section 4

Matthew Bradbury

Damjanovski, Alexander

- Product perspective
- Parts of 5.1, 5.2, 5.3, 5.4, 5.5, 5.6
- Formatting, final overview

A handwritten signature in black ink. The signature is written in a cursive script and appears to read 'Alexander Damjanovski'.