CCSE
University of Jeddah
Ministry of Education
Kingdom of Saudi Arabia

كلية علوم وهندسة الحاسب
جامعة جدة
وزارة التعليم
المملكة العربية السعودية

UJ SECURE CHAT APP

ACKNOWLEDGMENTS

ABSTRACT

UJ Secure Chat (UJSC) application will be one of the helpful apps for students and professors in the university. The UJSC app has the capability to provide different types of communication by sending messages or sharing files and recording voice or video securely and keeping privacy protected.

Malicious users are always interested to hack servers and revealing information about users in a certain system, and this happens almost every day in the Internet world. So, the motivation for this thesis is the need to identify the security services of a UJSC app and to design a secure system. This project proposes to provide End-to-End Encryption to the shared files or messages between the users, in addition to the Integrity checks to ensure the integrity by checking a specific pattern of the messages to ensure it's the original one.

To achieve this goal of the project is We propose to develop an integrated messaging system with the "My Future" app features to provide an advanced level of security.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER I | PROJECT OUTLINES

CHAPTER I | PROJECT OUTLINES

1. Introduction

Technology has become available everywhere in education and is developed very quickly. So, the University of Jeddah is within the initiatives of the digital transformation program, which is one of the programs of the modern Saudi University vision providing smart digital services. "My Future" app enables students to use and follow up on the most important academic services through smartphones.

From this point of view, the idea came to us to create a special application for the university that provides students and faculty members with a means of conversation in a safe, fast, and free manner. In the beginning, we will apply this idea at the level of the College of Computer Science and Engineering, and when it succeeds, we will expand it to achieve our goal to integrate our UJ secure chat application with the "My Future" application to become a comprehensive application for the university. We also seek to spread this idea at the level of universities in the Kingdom.

1.2. Problem Definition

Malicious users are always interested to hack servers and revealing information about users in a certain system, and this happens almost every day in the Internet world. Mobile instant messaging programs, unfortunately, are not an exception. Users can choose from a variety of mobile chat software. Many of these applications claim that they are providing the CIA (confidentiality, integrity, and availability) for users’ information. However, everyday hacking news demonstrates that many developers do not prioritize security in their programs.

On the other hand, the student needs these apps for the communication process which is as important as the other educational processes, every day in the student life involves some communication with the other student as well as the instructor and may include sensitive information, which makes it exposed to the public since the lack of authentication existence in these apps, In addition to the difficulty of the searching process in the first of every semester about the group link or the members.

1.3. Recommended solution

We propose to develop a secure messaging system called UJ secure chat that provides secure communication between a student and an instructor and has a strong authentication method, the developed system will add some main and useful features to provide an advanced level of security and reliable communication channels. We will add in our application all the important features found in the well-known chat applications to produce a comprehensive chat application.

1.4. Aims

The purpose of this project is to help students and improve the efficiency and security of the communication process that are a main part of the learning process, as well as upgrade the education by using new secure communication tools.

1.5. Objectives

The important objectives of our project are:

- To facilitate the sharing of resources that help improve the educational process.
- To provide an encryption service to all files to ensure the security of sensitive shared files such as certificates and personal documents.
- To initiate an authentication-based chat.
- To provide an advanced level of integrity using a new integrity checks technique.
- To provide a user-friendly interface to the students and the faculty members.
- To allow a secure sharing of videos, audio, and photos.

1.6. Project Scope

The project is about developing a secure chatting app designed to provide encrypted and secure communication between the student and faculty members by meeting the goals of Confidentiality, Integrity, Availability (CIA) to help them communicate and share their files securely and to keep their privacy protected.

The authentication process would be more effective and trusted by relying on the UJ email to ensure that is a user from the University of Jeddah and phone number to prevent impersonation and make it much harder than the common chatting apps.

The app will have consisted of several groups one for each course connect all the students of each course including the faculty member, also will support private messaging to provide more privacy and reliability, and to meet all the student needs and communication requirements.

The main feature is to provide End-to-End Encryption to the shared files or messages between the users, in addition to the Integrity checks to ensure the integrity by checking a specific pattern of the messages to ensure it’s the original one.

1.7. Project Plan

As shown in the following figures, to fulfill the purpose of this project in a timely manner, it has been decomposed into several tasks, so that the Microsoft Project Professionals has been used to manage all tasks on weekly basis from the beginning to the end of the project.

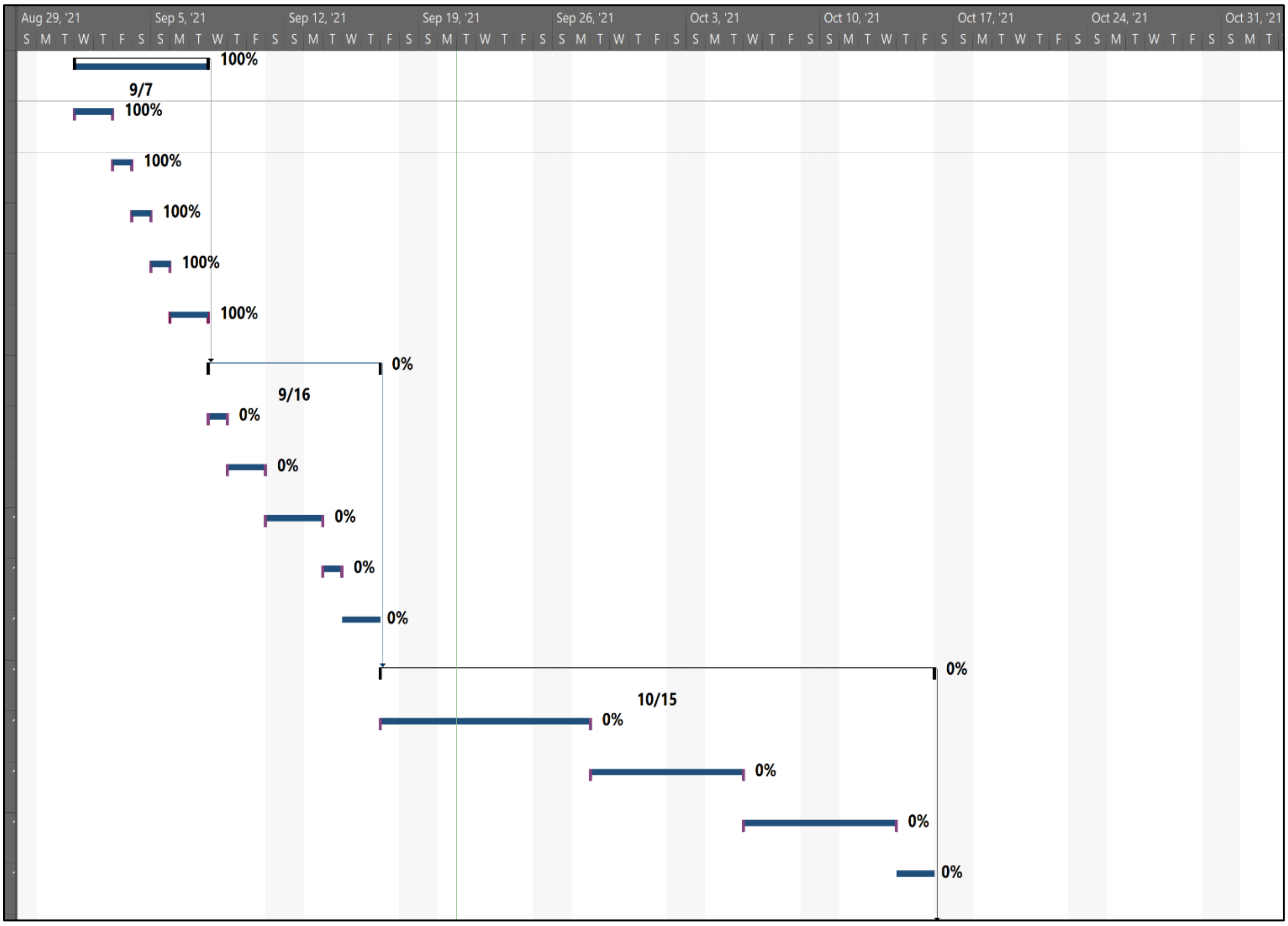


Figure 1 project plan gantt chart-1

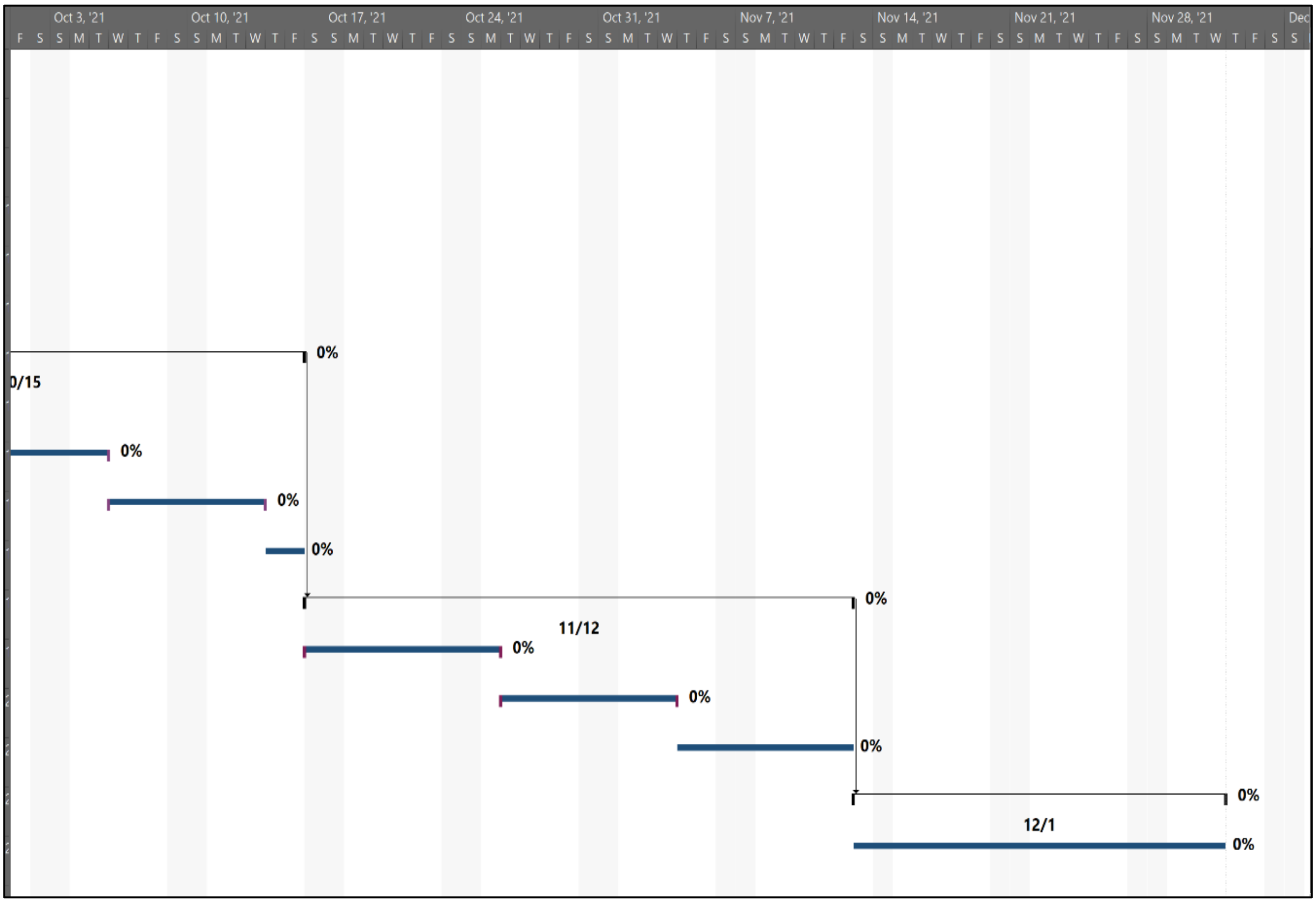
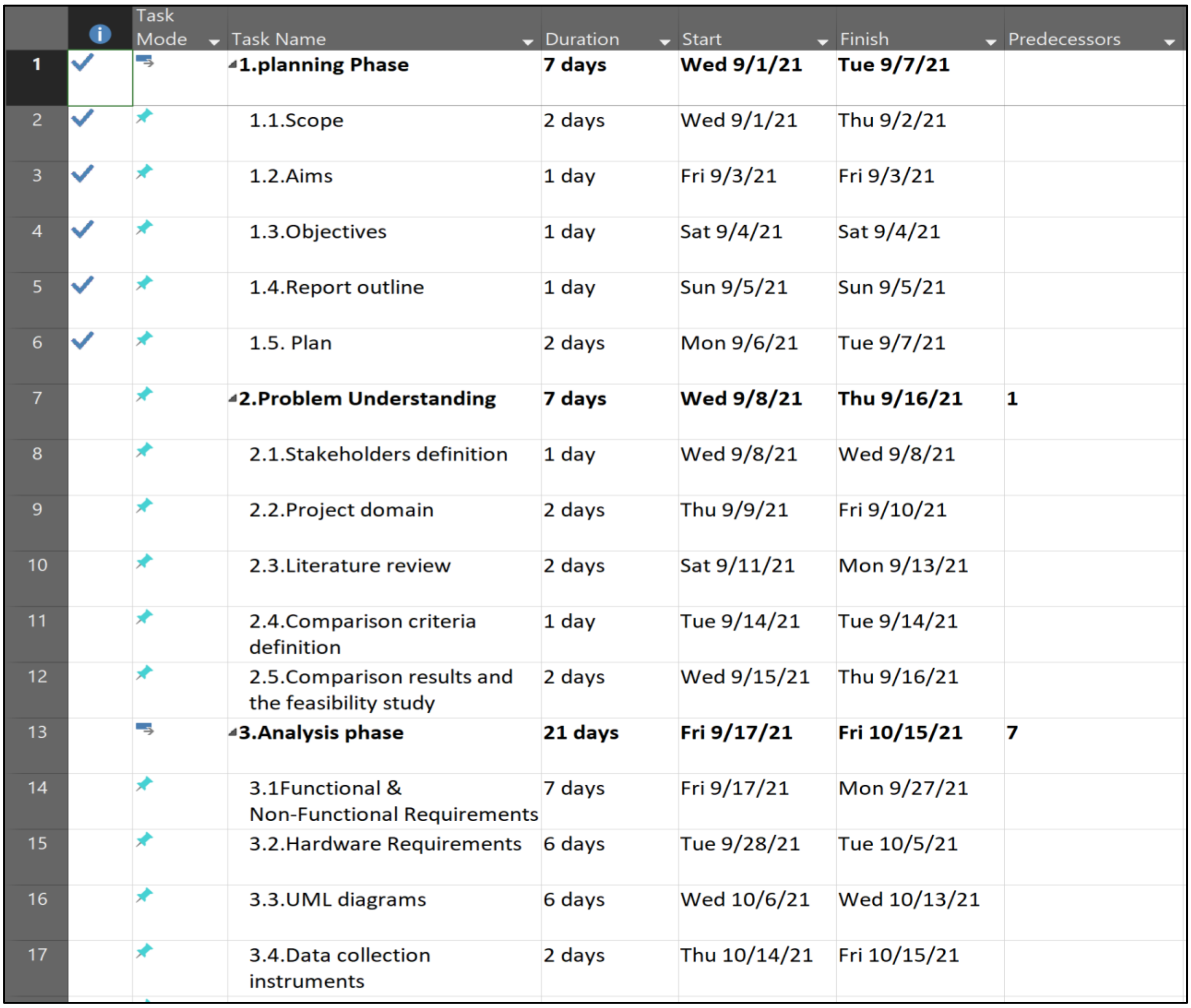
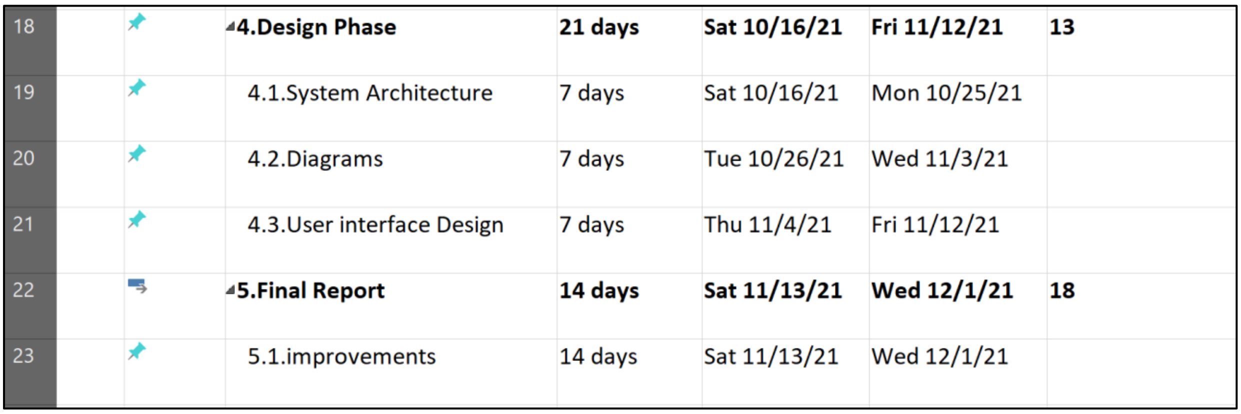


Figure 2 project plan gantt chart-2



	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1	✓	⇒	**1.planning Phase**	**7 days**	**Wed 9/1/21**	**Tue 9/7/21**	
2	✓	📌	1.1.Scope	2 days	Wed 9/1/21	Thu 9/2/21	
3	✓	📌	1.2.Aims	1 day	Fri 9/3/21	Fri 9/3/21	
4	✓	📌	1.3.Objectives	1 day	Sat 9/4/21	Sat 9/4/21	
5	✓	📌	1.4.Report outline	1 day	Sun 9/5/21	Sun 9/5/21	
6	✓	📌	1.5. Plan	2 days	Mon 9/6/21	Tue 9/7/21	
7		📌	**2.Problem Understanding**	**7 days**	**Wed 9/8/21**	**Thu 9/16/21**	**1**
8		📌	2.1.Stakeholders definition	1 day	Wed 9/8/21	Wed 9/8/21	
9		📌	2.2.Project domain	2 days	Thu 9/9/21	Fri 9/10/21	
10		📌	2.3.Literature review	2 days	Sat 9/11/21	Mon 9/13/21	
11		📌	2.4.Comparison criteria definition	1 day	Tue 9/14/21	Tue 9/14/21	
12		📌	2.5.Comparison results and the feasibility study	2 days	Wed 9/15/21	Thu 9/16/21	
13		⇒	**3.Analysis phase**	**21 days**	**Fri 9/17/21**	**Fri 10/15/21**	**7**
14		📌	3.1Functional & Non-Functional Requirements	7 days	Fri 9/17/21	Mon 9/27/21	
15		📌	3.2.Hardware Requirements	6 days	Tue 9/28/21	Tue 10/5/21	
16		📌	3.3.UML diagrams	6 days	Wed 10/6/21	Wed 10/13/21	
17		📌	3.4.Data collection instruments	2 days	Thu 10/14/21	Fri 10/15/21	

Figure 3 project plan



18		📌	**4.Design Phase**	**21 days**	**Sat 10/16/21**	**Fri 11/12/21**	**13**
19		📌	4.1.System Architecture	7 days	Sat 10/16/21	Mon 10/25/21	
20		📌	4.2.Diagrams	7 days	Tue 10/26/21	Wed 11/3/21	
21		📌	4.3.User interface Design	7 days	Thu 11/4/21	Fri 11/12/21	
22		⇒	**5.Final Report**	**14 days**	**Sat 11/13/21**	**Wed 12/1/21**	**18**
23		📌	5.1.improvements	14 days	Sat 11/13/21	Wed 12/1/21	

Figure 4 project plan -2

1.8. Report Outline

This project is consisting of two phases that are organized through two semesters. The first phase that will implement in the first semester includes:

Chapter I: introduce the definition of the problem, the recommended solutions, aims, objectives, project scope, report outline, and project plan.

Chapter II: introduce the stakeholders' definition, project domain, literature review, comparison criteria definition and, comparison results and the feasibility study.

Chapter III: Includes the requirements specifications (Functional and non-functional requirements), hardware requirements, UML diagrams, and data collection instruments (Datalogger).

Chapter IV: Contain the architecture and the design of the system, diagrams, and user interface design

1.9. Conclusion

This project seeks to simplify communication for students and other members of the University of Jeddah because they have difficulty communicating securely. And This is done by creating the application using the most secure approaches to provide the communication needs with a high level of security.

The next chapter will talk about the stakeholders, project domain, literature review, comparison criteria definition and, comparison results and the feasibility study.

CHAPTER II | LECTURE REVIEW

CHAPTER II | LITERATURE REVIEW

2.1 Stakeholders' Definition

Stakeholders are the ones who contribute and support the project to completion, also the ones who are going to benefit from this project directly or indirectly. So, in our project the target users are:

- Faculty members
- Students

As they benefit from our application through instant communication, which will help develop the educational process and get high privacy.

2.2 Background and Overview of Related Work

2.2.1 Background

Communication is the process of exchanging information between individuals, where they exchanged information and ideas are shared through common systems of symbols or letters, it can vary from extremely basic processes of interchange to whole dialogues and mass communication.

This is one of the major needs of a human being and therefore it’s as important as the other needs of life. Since the start of time, even before the development of languages, humans have attempted to communicate, warning each other of danger or showing each other how to hunt.

The history of communication itself can be traced back to the origin of speech circa 500,000 BCE, and the use of technology in the communication goals can be traced back to the earliest usage of symbols around 30,000 years BCE.

Because the default setting of our brains is to understand images better than text, Humans have always been searching for ways to communicate visually, that time we started drawing which was for 32000 years the oldest known form of communication between humans, which started as cave paintings then developed to the pictograms that eventually evolved into ideograms, until the alphabet was developed around 1500 BC by the Phoenicians.

In 3500 BC the first cuneiform writing was developed by the Sumerians, while hieroglyphic writing was developed by the Egyptians, after that, the paper which was the biggest change of the communication was invented by Tsai Lun in 105 AD [1], in addition to the use of smoke signal as a long-distance communication method, even today it is a good signal to say "help", furthermore the Pigeon post was used to send a paper-based message by attaching the paper to their feet, and also the snail mail was used since the paper was invented, Through the ages, transportation of snail mail has included dogsleds, balloons, and submarines what may take up to years to receive a message.

In the early 19th century, some simple inventions were made and then used to send symbols or letters through electrical impulses passing through wires until the telegraph was invented by Samuel Finley in 1823 to send messages that would take days or months to reach their destination.

Finally, the messages just need a few minutes to reach the destination after the great extending of the telegraph over an electric wire in the 1850s, and the newspapers were able to publish news around the world on the same day as it occurred.

Electricity helped Alexander Graham Bell patent the telephone in 1876 AD which helps the world to communicate wirelessly and improved to create the worldwide network that used as the basis of all types of text communication or videos [2], which can be used by the applications to send a mail or instant messages.

2.1.1.1 Chatting apps

The chatting apps are also called “instant messaging apps” which refer to the kind of apps that allows the user to send and receive messages in a real-time manner, unlike the emails the IM service allows the messages to be sent immediately where the receiving of the messages at the same sending time, whereas email can be queued up in a server for seconds or minutes.

2.1.1.2 Chatting apps in daily life

Nowadays most of our communication is by using these apps, where there are 2 billion active users for WhatsApp, with forecasts projecting an audience size of almost 86 million users in 2023 which makes WhatsApp the most popular IM app [3], (82% - 92%) of the users of the user shared their private data throughout this type of apps including their real names, phone number, date of birth and picture of themselves and also their daily life events [4], which makes it the main part of their life and important space for them.

2.1.1.3 Chatting Apps in Education

One of the most important tasks of the First-day of school list to do is joining the class chatting group and that process could take days to find the admin of the group and ask him to send the invite link to join that group and the same process repeated for each course and that long process proves that these kinds of the group are a main and important part of the educational process, each student needs to join these groups with their colleagues as a part of their daily routine either for sharing notes or helpful resources or even for an emergency announcement.

2.1.1.4 Chatting Apps Security

According to the large usage of these types of apps and the type of important data shared through these apps the security is one of the major concerns that affect the people, therefore the chatting apps need a high level of security through authentication, confidentiality, integrity, and other security approaches.

Mobile chat applications are always at risk of attack, from the developer's perspective since security matters became a concern the chatting app developing process became a challenge. for the development of the art and holistic chat applications, the developer should focus on the most secure features to protect the user's privacy using advanced methods such as the end-to end-encryption technique, Authentication, and authorization approaches to provide an appropriate level of protection, in addition to the integration of the art security system so that users can effectively carry out a conversation effortlessly.

We will show in this section that our idea is feasible to be applied in real life by solving a gap in other applications. Also, comparison the criteria definition and results of other chatting applications.

2.2.2 Related Work

Chatting applications have an expansion highly in the technological world around us, where it is difficult to visualize a scenario of our everyday life that could be free of using any chat app, especially since people have recently become preferring to communicate through these applications instead of a phone call. Which requires developers to look for accurate methods to achieve an appropriate rank of security in mobile chat applications [5].

So, in this paper, we document our findings on the most secure chatting apps and comparison results between them:

- A WhatsApp [6]

  Is a cross-platform instant messaging service for phones founded in 2009 by Brian Acton and Jan Koum. their app allows people to exchange messages (including chats, group chats, images, videos, voice messages, and files), share status posts, and make WhatsApp calls around the world. WhatsApp focused more on messaging and neglected privacy at first. Because of the carelessness shown towards securing the application, it became an easy target for attackers.

  After the increasing privacy concerns over encryption, WhatsApp started the deployment of End 2 End encryption using the Signal Protocol developed by the Open Whisper Systems therefore it is no easier for third parties to access the content.

- A Facebook’s chat Application is called Messenger [7]

This App allows for services such as normal chat messages, voice, and video calls in Facebook.

Facebook provides End-to-end encryption and self-destructs of the message using the Signal Protocol developed by the Open Whisper Systems, but the encryption is not enabled by default and must be enabled each time before starting a new chat by selecting the Secret Conversation option and setting the conversation to self-destruct.

▪ The official King Abdulaziz University application MYKAU [8]

This App enables all kinds of users in the university to benefit from the services provided. The application provides general services available to all users whether they were university employees or students. Some services are specific to a certain type of user therefore these services appear according to the authorization after logging in.

The services offered by the App are:

- University map.
- University news.
- Support and communication.
- A guide for communicating with university employees.
- Review and follow-up of the academic schedule, grade transcript, university card, attendance, and absence report also student financial movements.
- Communication between professor and student through messages like mail messages, not instant messaging.
- There is no information found about the security and privacy of the app.

▪ A Telegram [9]

Telegram is a cross-platform that provides an encrypted instant messaging service founded in August 2013. Messages including photos, videos, and documents are stored in cloud-based storage except “secret chats” content is not stored there.

This app has different types of chats:

- **Cloud Chats**

Cloud chats use client-server encryption. All messages from cloud chats are kept on servers, allowing users to retrieve their data at any time without relying on third-party backups.

- **Secret Chats**

Secret chats provide end-to-end encryption using the “MTProto” protocol. Therefore, there is no way for third parties to know the contents of those messages.

- **Public Chats**

Public chats are public channels and public groups. the messages sent in public chats are encrypted, both in storage and in transit [10].

2.3 Research Gap

From our review of related works, there were different applications related to the instant messaging apps. However, these applications were not for educational purposes. Furthermore, all the apps include a phone number-based authentication method that can't be trusted and considered as proof of identity, in addition to the lack of Access control features. On the other hand, secure methodologies were used in educational communication apps, although they were successful in providing messages and announcements to the students within a timeline. Our work will develop a tool that will be an immediate communication channel. Unlike previous works that were broadcast-based, this tool is an iM app (instant messaging) based on the many-to-many communication paradigm, that allows all the parties to participate in the communication.

2.4 Comparison Criteria Definition

After observing some related work or other apps regarding the chatting aspects the following criteria will be considered:

- **Ease of discovery and acquisition:** the ease of access to desired users to begin chatting
- **Group chatting:** the ability to share the chat among various users and to participate in the communication at the same time
- **Broadcasting mode:** the ability to send the message by one master user "instructor "and receive it by many users " students ".
- **Many-to-many communication mode:** the ability to send the message for many users and receive it from many other users.
- **Encryption by default:** enable the encryption service by default to all the data without exclusion
- **Encryption of metadata:** provide the encryption service to the metadata which is known as “data about data” include the file size, the author ...etc.
- **Message self-destruct:** The ability to have messages disappear forever after a fixed amount of time
- **Multimedia Encryption:** provide an encryption service to all the shared media include video, audio, photos during the transmission process.

2.5 Comparison results and the feasibility study (Critical Analysis)

Criteria	WhatsApp	Messenger	MYKAU	Telegram	UJ Secure Chat
Ease of discovery and acquisition	✓	✓	✓	✓	✓
Group chatting	✓	✓	X	✓	✓
Broadcasting mode	✓	X	✓	✓	✓
Many to many	✓	✓	X	✓	✓
Encryption by default	✓	X	-	X	✓
Encryption of metadata	X	X	-	X	✓
Message self-destruct	X	✓	-	✓	✓
Multimedia Encryption	✓	✓	X	✓	✓

Table 1, Critical Analysis of related works

Based on the critical analysis table above, we can say that our proposed secure chat application will gain an advantage by the development of the lack in other applications.

2.6 Overview of Implementation Tools

-Java for the Back-End implementation.

- React Native (JavaScript) for the Front-End implementation.
- Extensible Messaging and Presence Protocol (XMPP) to transmit the messages.
- DES encryption

CHAPTER III |SYSTEM REQUIRMENTS

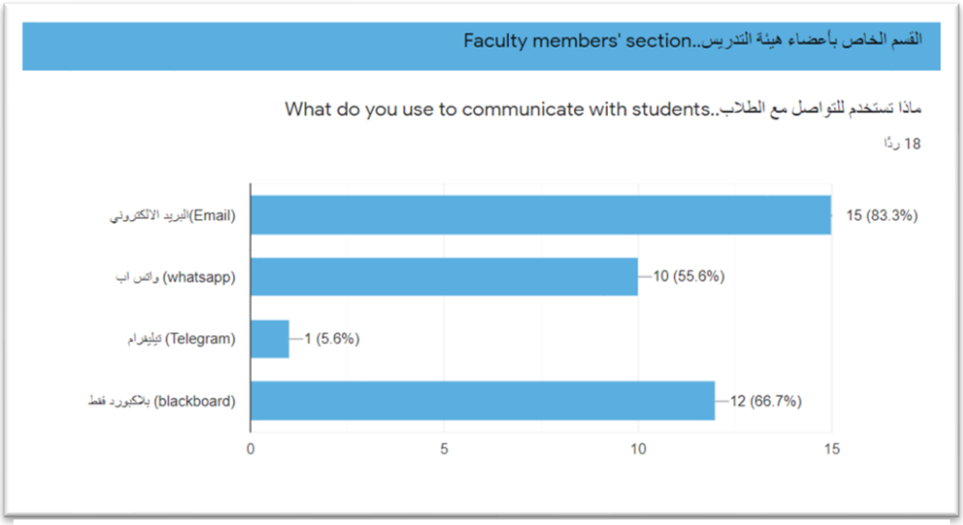
Chapter 3 | System Requirements

3. Introduction

This chapter will present the functional, non-functional, hardware, and security requirements of our UJ Secure Chat for a secure catting system. Also, it covers a set of security perimeters by defining the domain of applicability and the needful safeguards to secure a system from attacks. It defines the (Physical or logical) security services, this is followed by the UML diagram that visualizes a software program using a collection of diagrams.

3.1 Data collection instruments (Datalogger)

We have created a questionnaire and distributed it to academics and students of the University of Jeddah because our project focuses on them. We need this questionnaire to gather data about their current communication platforms and to clarify the need to design our app. The following charts display the results with the questions of the questionnaire conducted over users, we received (126) responses.

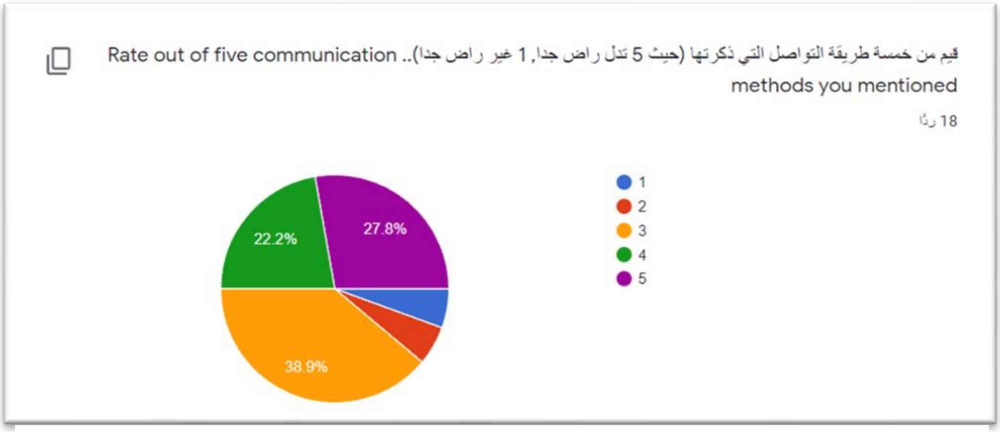


Faculty members' section..القسم الخاص بأعضاء هيئة التدريس

What do you use to communicate with students..ماذا تستخدم للتواصل مع الطلاب

18 ردًا

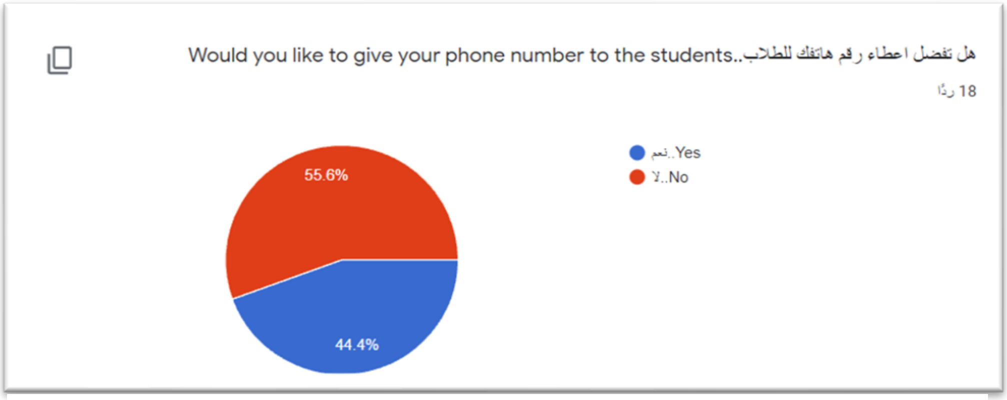
Figure 5 Question 1



قيم من خمسة طريقة التواصل التي ذكرتها (حيث 5 تدل راض جدا, 1 غير راض جدا)..Rate out of five communication methods you mentioned

18 ردًا

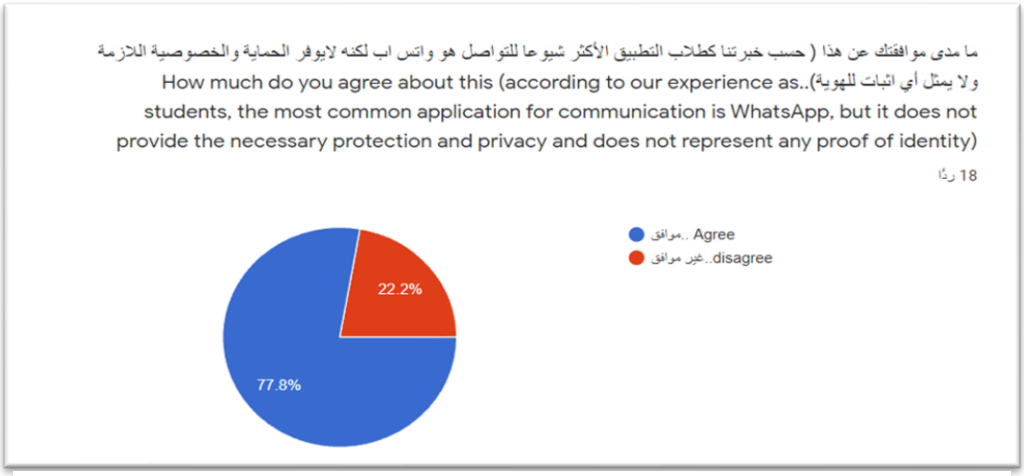
Figure 7 Question 2



هل تفضل اعطاء رقم هاتفك للطلاب..Would you like to give your phone number to the students

18 ردًا

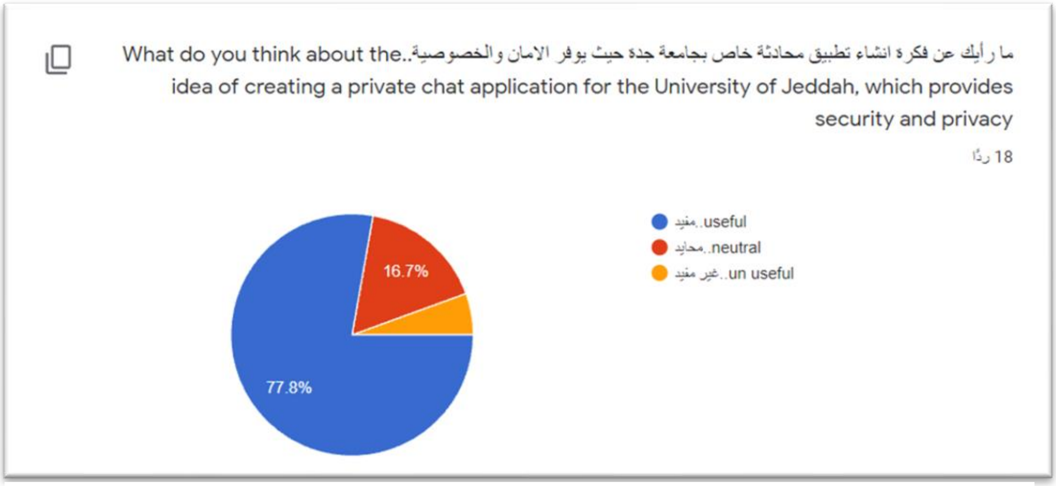
Figure 6 Question 3



ما مدى موافقتك عن هذا (حسب خبرتنا كطلاب التطبيق الأكثر شيوعا للتواصل هو واتس اب لكنه لايوفر الحماية والخصوصية اللازمة ولا يمثل أي اثبات للهوية)..How much do you agree about this (according to our experience as students, the most common application for communication is WhatsApp, but it does not provide the necessary protection and privacy and does not represent any proof of identity)

18 ردًا

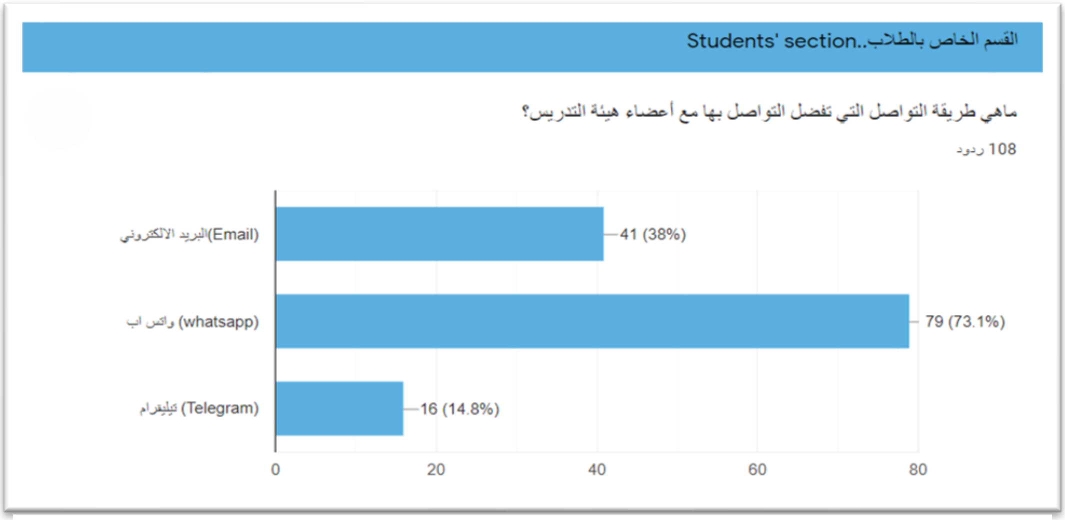
Figure 8 Question 4



What do you think about the..ما رأيك عن فكرة انشاء تطبيق محادثة خاص بجامعة جدة حيث يوفر الامان والخصوصية
idea of creating a private chat application for the University of Jeddah, which provides security and privacy

18 ردًا

Figure 9 Question 5

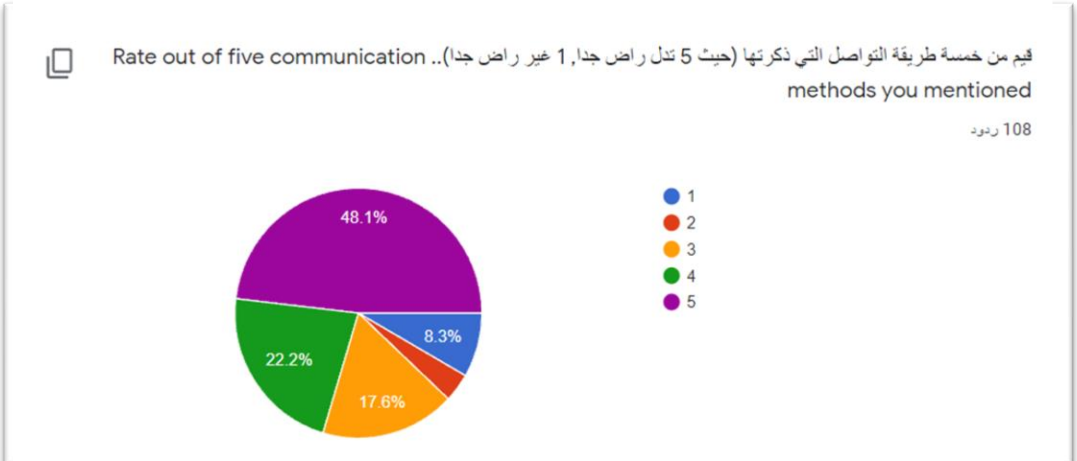


Students' section..القسم الخاص بالطلاب

ماهي طريقة التواصل التي تفضل التواصل بها مع أعضاء هيئة التدريس؟

108 ردود

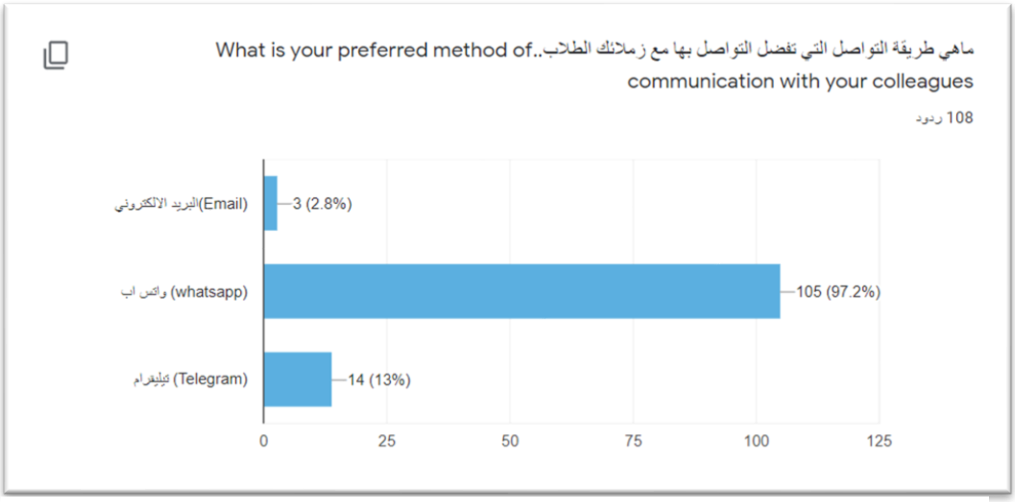
Figure 10 Question 6



Rate out of five communication ..(قيم من خمسة طريقة التواصل التي ذكرتها (حيث 5 تدل راض جدا, 1 غير راض جدا
methods you mentioned

108 ردود

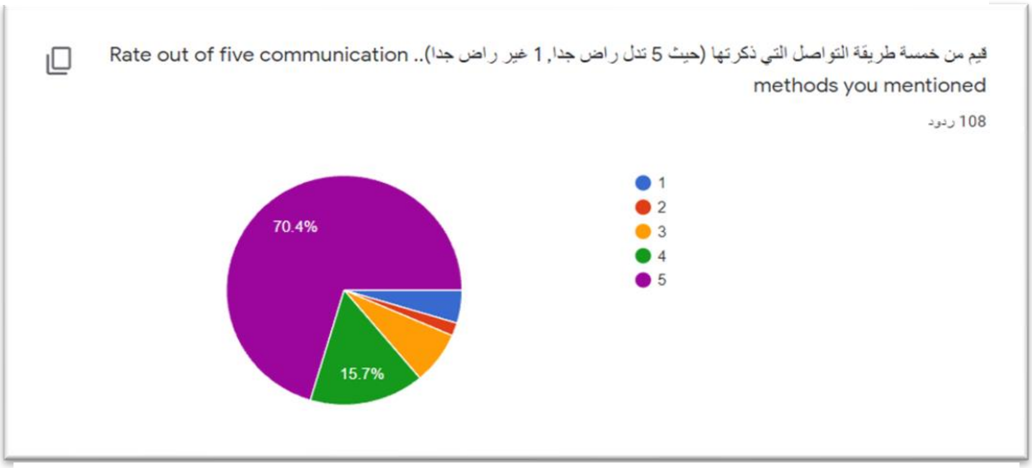
Figure 11 Question 7



ماهي طريقة التواصل التي تفضل التواصل بها مع زملائك الطلاب..What is your preferred method of communication with your colleagues

108 ردود

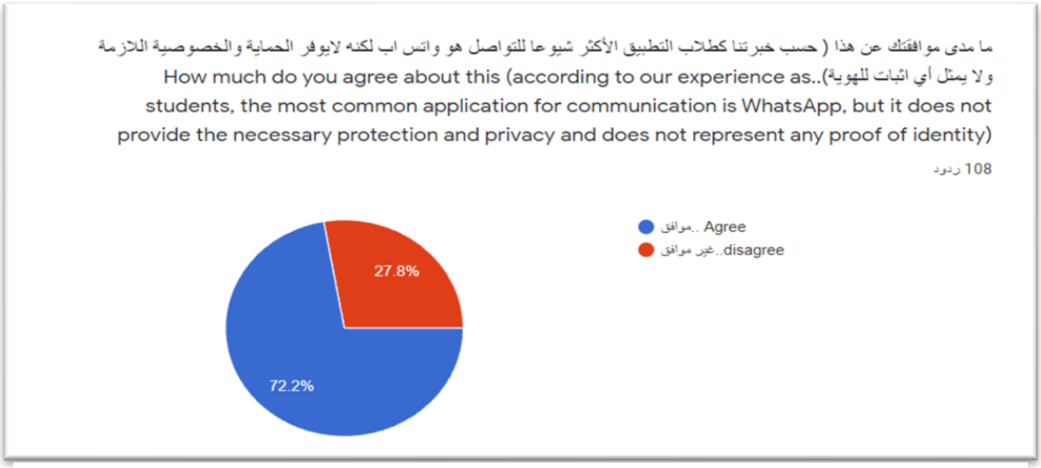
*Figure*12 *Question 8*



قيم من خمسة طريقة التواصل التي ذكرتها (حيث 5 تدل راض جدا, 1 غير راض جدا).. Rate out of five communication methods you mentioned

108 ردود

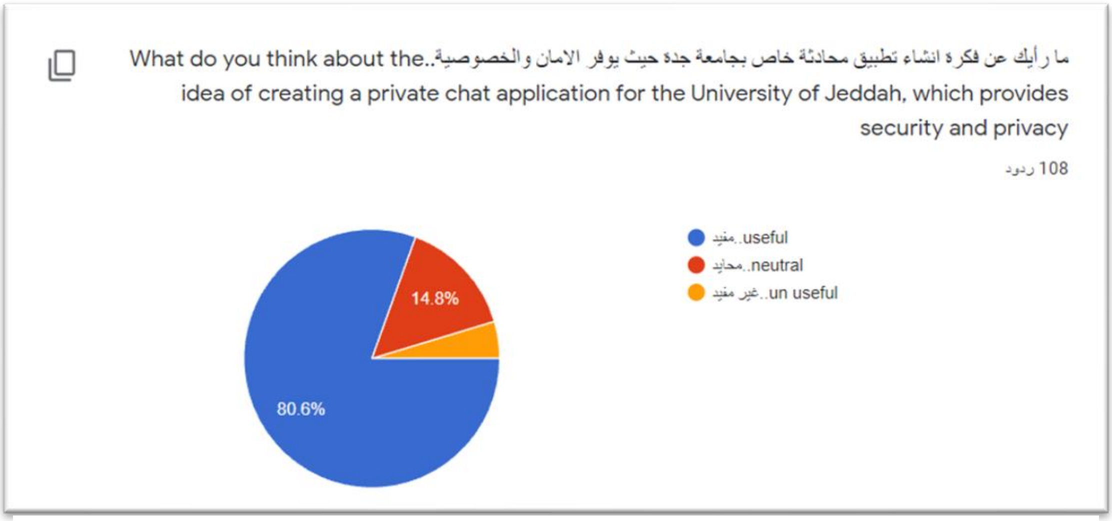
Figure 12 Question 9



ما مدى موافقتك عن هذا (حسب خبرتنا كطلاب التطبيق الأكثر شيوعا للتواصل هو واتس اب لكنه لايوفر الحماية والخصوصية اللازمة ولا يمثل أي اثبات للهوية)..How much do you agree about this (according to our experience as students, the most common application for communication is WhatsApp, but it does not provide the necessary protection and privacy and does not represent any proof of identity)

108 ردود

Figure 13 Question 10



ما رأيك عن فكرة انشاء تطبيق محادثة خاص بجامعة جدة حيث يوفر الامان والخصوصية..What do you think about the idea of creating a private chat application for the University of Jeddah, which provides security and privacy

108 ردود

Figure 14 Question 11

It was one of the most prominent things we noticed after analyzing the results of the questionnaire, that most of the faculty members 55.6% do not prefer to give their phone numbers to students, but rather prefer to communicate by e-mail. On the other hand, the students preferred to communicate through the WhatsApp application 97.2%. Also, that users, in general, are not completely satisfied with the applications currently used to communicate therefore we have encountered high demand for the idea of our application UJ Secure Chat by faculty members by (77%) and students by (80.6%) as shown in the screenshots above.

3.2 System Requirements

3.2.1 Functional Requirements

- The user shall be able to register first by his email, name, phone number, and ID number.
- The user identity shall be verified during the registration by asking the user to enter the one-time Passcode sent to his/her UJ email address.
- The user shall be able to log in using his/her UJ ID and password entered during registration.

- The home page of the application shall display several groups for the courses by default.
- The integrity and secrecy of each message shall be protected by applying an integrity check before displaying and message.
- The app shall provide end-to-end encryption be encrypt each message on the user device before any transmission over the network, the encryption process shall be done using the user private key, and the decryption on the recipient’s device using the public key of the sender.
- The user shall be able to send a new message to any of the students who enrolled in the same course.
- The user shall be notified when a message is successfully delivered to the recipient by displaying a tick sign next to the message sent.
- The user shall be able to send any type of multimedia as attachments.
- The user's profile shall not include any detailed information for the user's privacy.
- The user shall be able to display his profile.
- The instructor shall be able to create a list of contact to send broadcast messages privately.
- The user shall be able to view the message status that shows a blue or grey tick to obtain whether the message sent has been read or not by the intended recipient, the blue tick indicates that the message has been read the grey indicate the unread messages, display the time of receiving and reading.
- The user shall be able to create a destructive message that enables the receiver to read it once and for a given time specified by the sender.

3.2.2 Non-Functional Requirements

- UJ secure chat must be able to provide instant messaging services to many users at the same time.

- UJ Secure chat must be comfortable, easy, and straightforward to use for all types of users.
- The system must be operational 24 hours a day, seven days a week.
- If a user's device fails, a backup of their conversation history must be saved on distant database servers to allow for recovery.
- The program must be able to accommodate 500,000 users without compromising performance.
- After the first successful login, the teacher must update the initially issued login password. Furthermore, the beginning should never be used again.

3.3 Use Case Diagrams

The figure below represents the use case model that explains all possible actions of the users (UJ students and instructors) in our project.

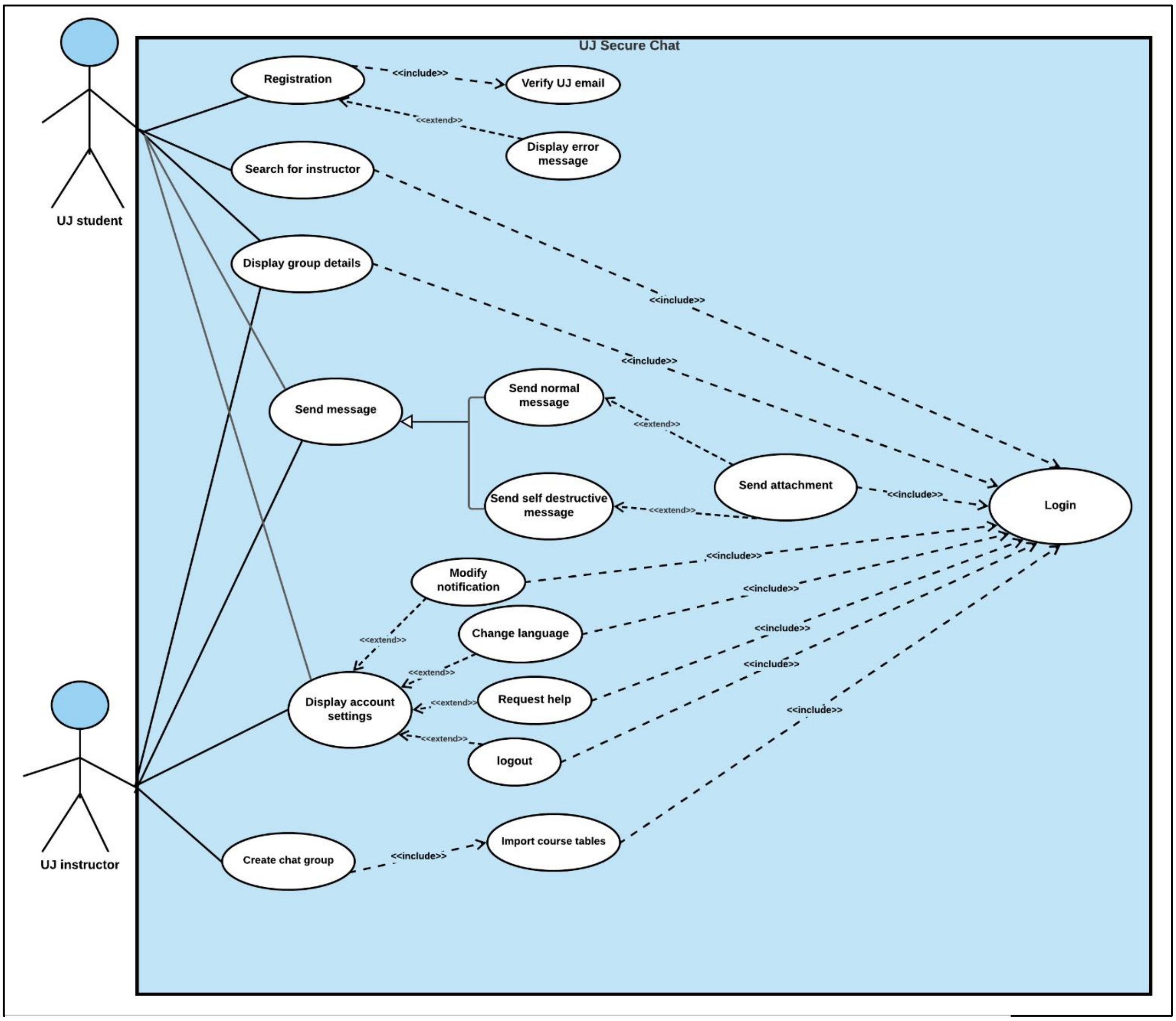


Figure 15 use case diagram

Actor	Use case	Description
	▪ **Registration**	The students will have to fill in information about themselves and must verify the link sent to their UJ email to authenticate themselves as UJ students. Otherwise, an error message will appear.
	▪ **Login**	It is an important case that enables a user to interact with the application services.

Student/Instructor	▪ **Display group details**	After login, the user can view group name, members, and group picture.
	▪ **Send message**	After login, the user can choose between sending a self-destructive message or a normal message and it is possible to contain an attachment.
	▪ **Search for instructor**	After login, the student can search for any instructor by full name.
	▪ **Create chat group**	After login, the instructor can create a chat group after importing the course table that contains students' information.
	▪ **Display account setting**	After login, the menu bar will contain an icon for the setting page, the user will be able to change the setting according to his/her needs.
	▪ **Change language**	After login, from the account settings menu, the menu bar will contain an icon that enables the user to change the language between Arabic and English.
	▪ **Notification**	After login, from the account settings menu, the user can manage notifications of the application such as muting or others.
	▪ **Help**	After login, from the account settings menu, the user will get all information about the application when clicking on help and get technical support.

	- **Logout**	After login, from the account settings menu, the user can log out at any time and terminate the connection.

Table 2 use case description

3.4 Hardware requirements

- The computer on which will be used for development as a minimum must meet or exceed the following requirements:
  - RAM of 4-GB
  - 1.8 GHz x64-bit dual-core processor.
  - Windows version 8 or later/MacOS V10.10 or later.
  - hard disk space of 15 MB.
  - SSD (Solid State Drive) at least 120GB for storage.

- The computer on which will be used for development must meet the following requirements for better performance:
  - RAM of 32-GB.
  - 2.8 GHz or faster, x64-bit quad-core or better.
  -Windows version 10/MacOS V10.14.4 or later.
  - hard disk space of 265 GB.
  - SSD (Solid State Drive) 1 TB for storage.

CHAPTER IV | DESIGN

Chapter 4 | design

4 Introduction

This section analyses the system's design by breaking it down into parts to show how each component interacts with the others to achieve its goal and achieve the desired result. This chapter also explains how the entire system works to accomplish that goal. Furthermore, it shows how the user interface will be.

4.1 System Architecture

The figure below represents the UJ chatting app composed of an application server, database, and user device connected to the server through the internet to provide a reliable service to the users by building a secure communication channel defined as client-server architecture.

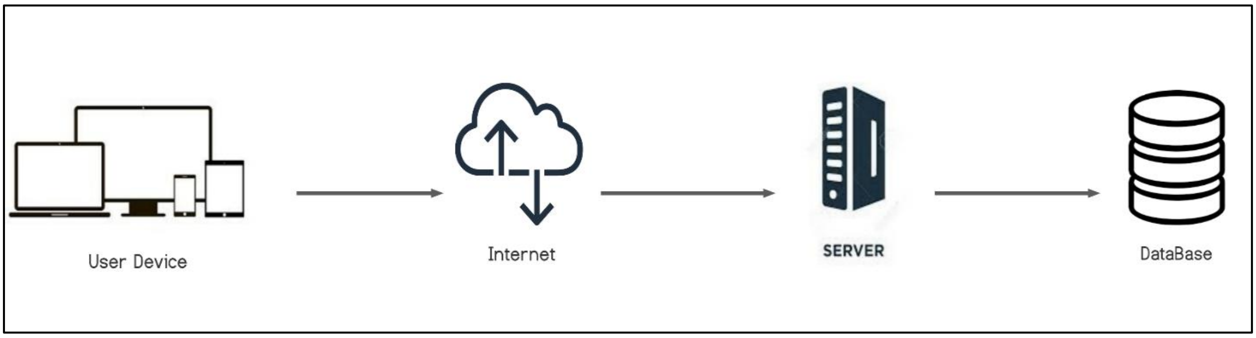


Figure 16 system architcture diagram

4.2 Diagrams

4.2.1 Structural Modeling (Class Diagram)

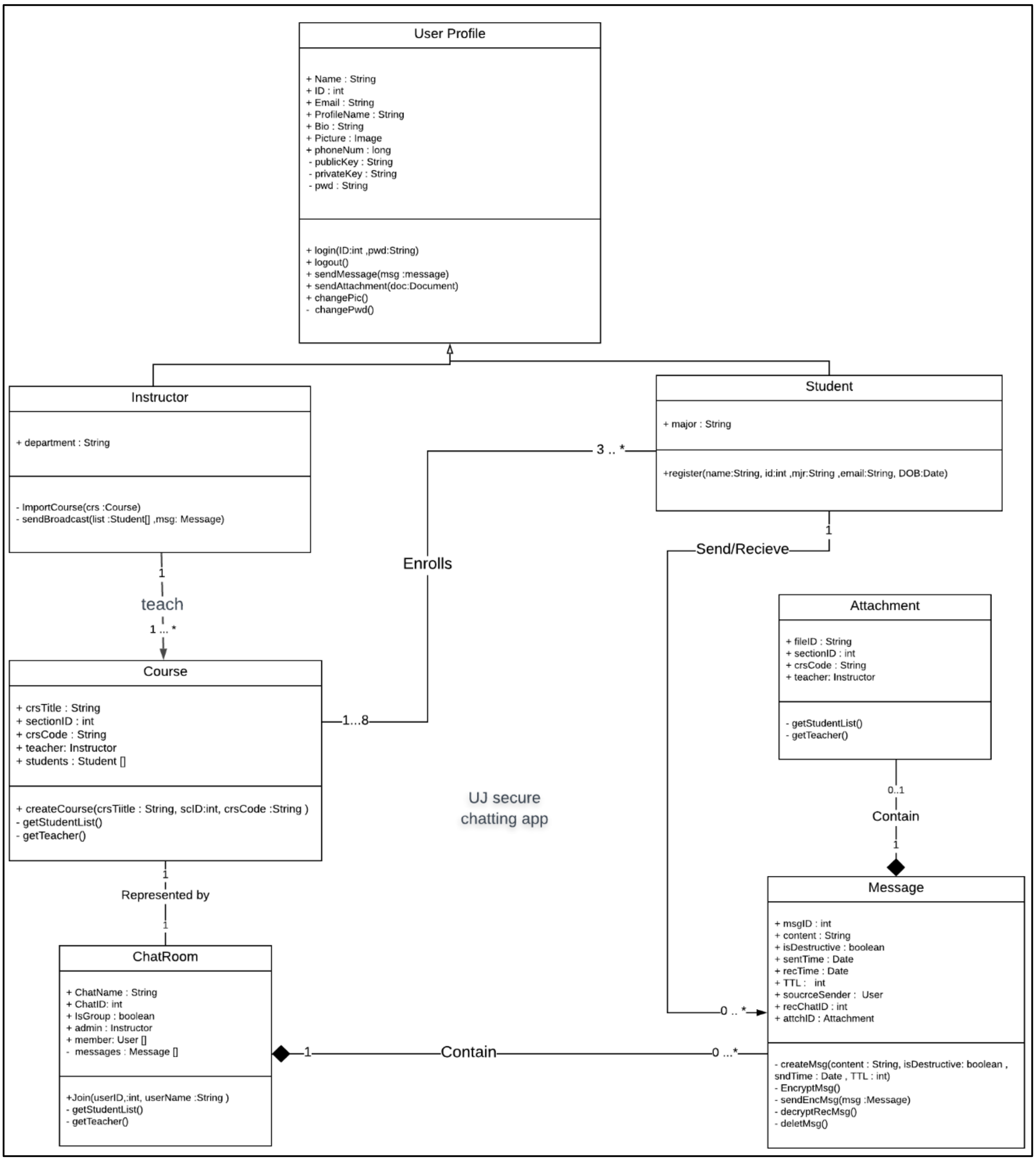


Figure 17 class diagram

The figure above represents the class diagram that shows the classes and the relationships among them. Our system consists of 7 classes.

<u>Classes and their attributes of UJ secure chat app class diagram:</u>

- **UserProfile class**: Name, ID, Email, phoneNum, profileName, Bio, pwd, Picture, publicKey, and privateKey.
- **Instructor class**: department.
- **Student class**: major.
- **Course class**: crsTitle, sectionID, crcCode, teacher, and students.
- **Attachment class**: fileID, sectionID, crcCode, and teacher.
- **ChatRoom class**: ChatName, ChatID, IsGroup, admin, member, and messages.
- **Message class**: msgID, content, isDestructive, sentTime, recTime, TTL, sourceSender, recChatID, and attchID.

Classes and their methods of UJ secure chat app class diagram:

- **UserProfile methods**: login (), logout (), sendmessage (), sendAttachment(), changePic (), changePwd ()
- **Student method**: register ()
- **Instructor methods**: importCourse (), SendBroadcast ()
- **Course methods**: createCourse (), getStudentList (), getTeacher ()
- **ChatRoom methods**: Join (), getStudentList (), getTeacher ()
- **Message methods:** createMsg (), EncryptMsg (), sendEncMsg(), decryptRecMsg() ,deleteMsg()
- **Attachment methods**: getStudentList (), getTeacher ()

The relationships between classes are as follows:

- The UserProfile is a superclass of Instructor and Student classes (children).
- Each instructor can teach and import many courses and the student can enroll in many courses, 8 as maximum.
- The student can send and receive multiple messages.

- The Attachment has a composition relationship with the Message class which means that the attachment file is part of the message and can't be a stand-alone object.
- The Message has a composition relationship with the ChatRoom class which means that the message is part of the chat room and can't be a stand-alone object.

4.2.1 Behavioral Modeling (Sequence Diagram)

The sequence diagram was chosen to describe how different users can interact with the application because the sequence diagram shows the sequence of interactions that take place during a particular use case or use case instance.

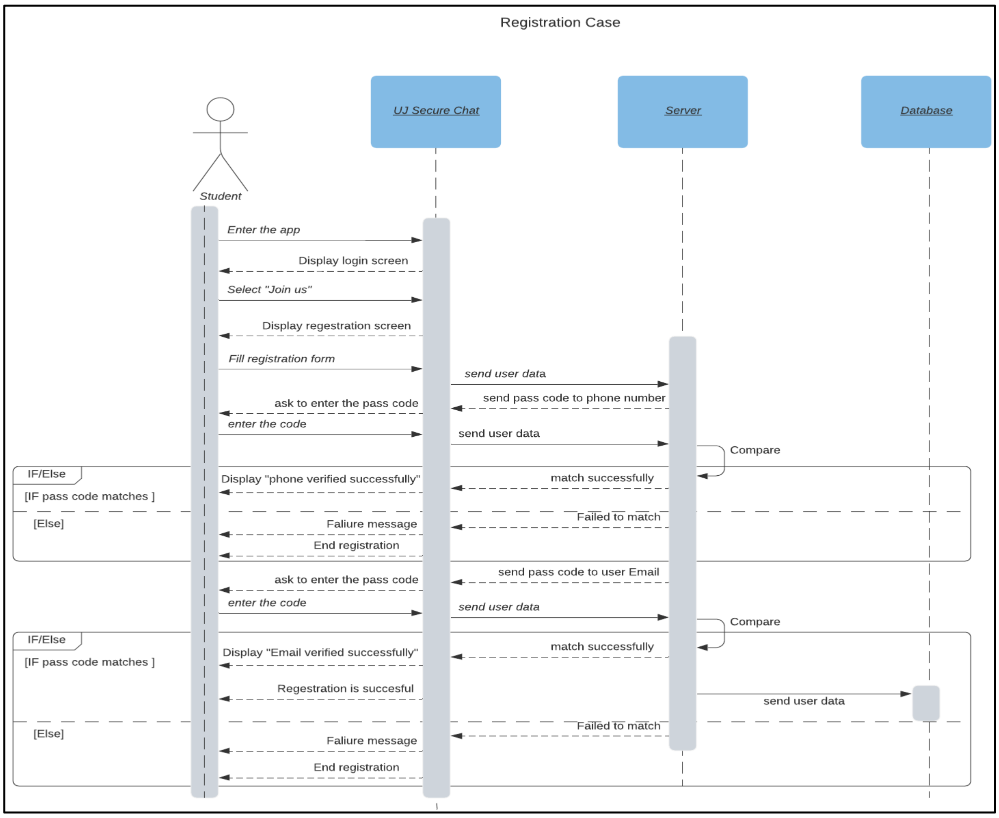


Figure 19 student's Registration sequence diagram

In the figure above the sequence diagram shows how the student user interacts with our application, where a student will be able to register by providing the information needed and verifying their phone number and UJ email by entering the code sent to them.

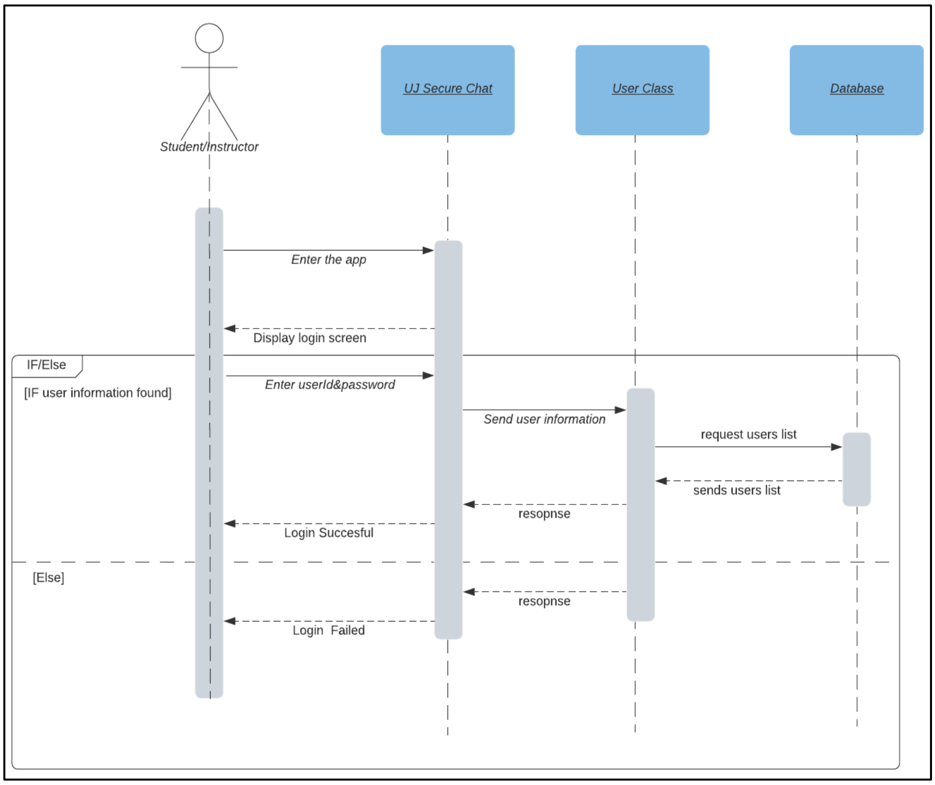


Figure 18 Users login sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can log in to the application using their credentials then by checking the credential from the database, we can process their login if it's successful or not.

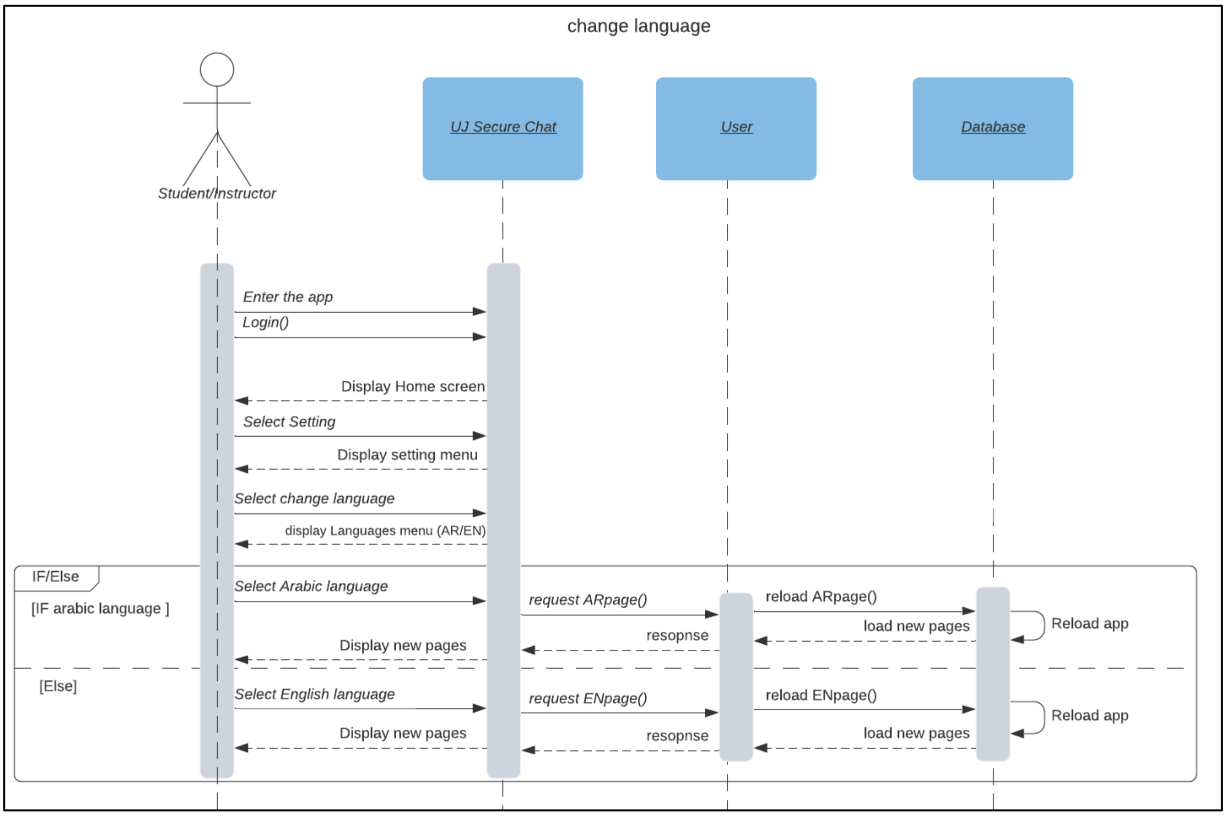


Figure 19 Change language sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can switch languages between English and Arabic from the setting and select change language then the user request will be processed. Then, the application will be updated to the language chosen by the user.

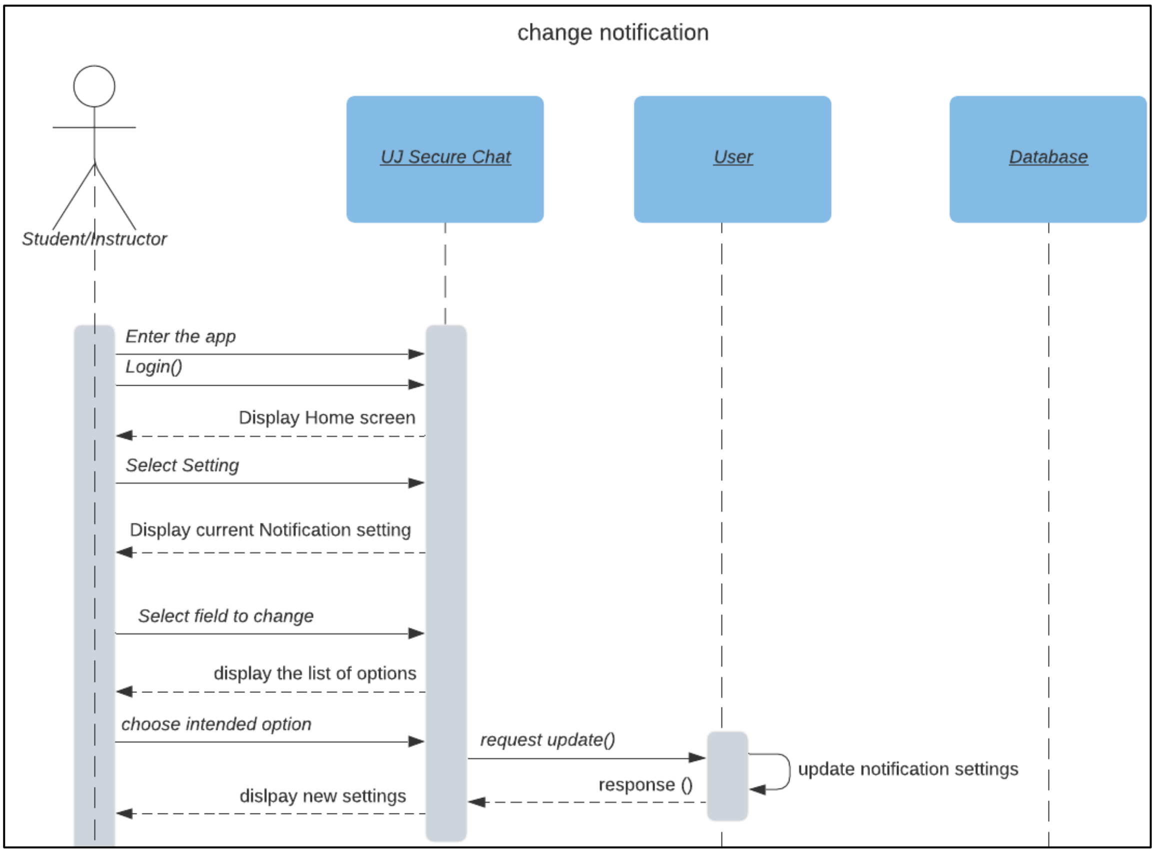


Figure 20 Change notification sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can turn off or turn on notifications, upon their choice our application will process their request and update their notification settings.

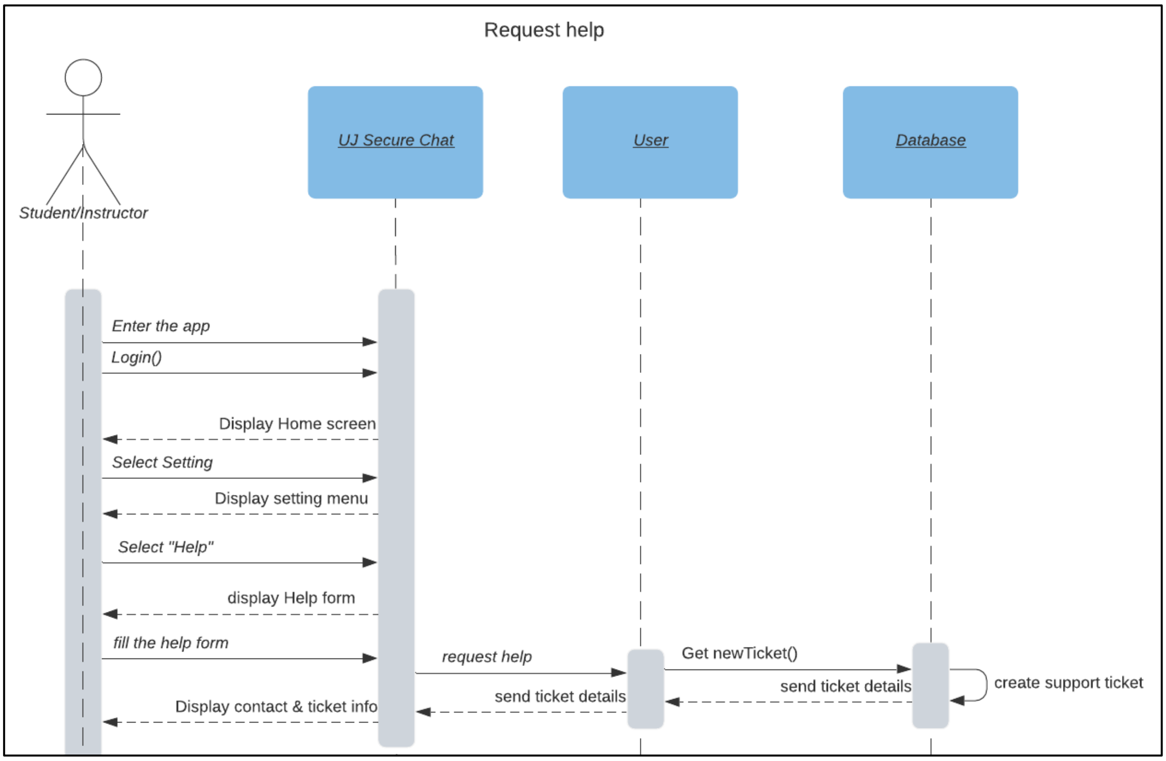


Figure 21 Request help sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can request help from the technical team by filling a form describing their issue then their request will be processed by our application and then the user will get a ticket number and contact information.

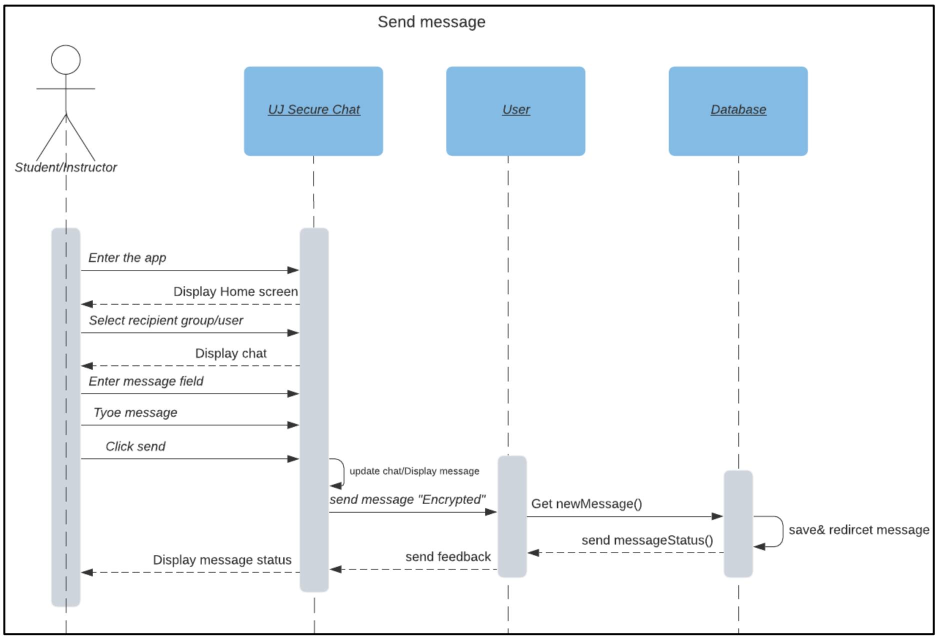


Figure 22 Send message sequence diagram

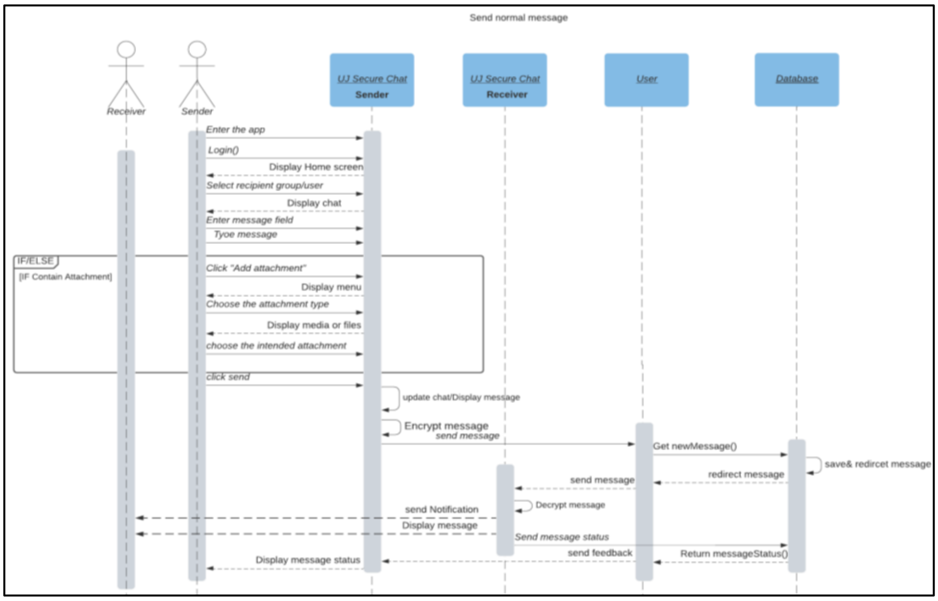


Figure 23 Send normal message sequence diagram

In the figures above the sequence diagram shows how users can interact with our application, after login, the user can choose to send a normal message before sending the message to the receiver the application will encrypt the message and stores it in the database then at the receiver the application will decrypt the message, also it is possible to contain an attachment.

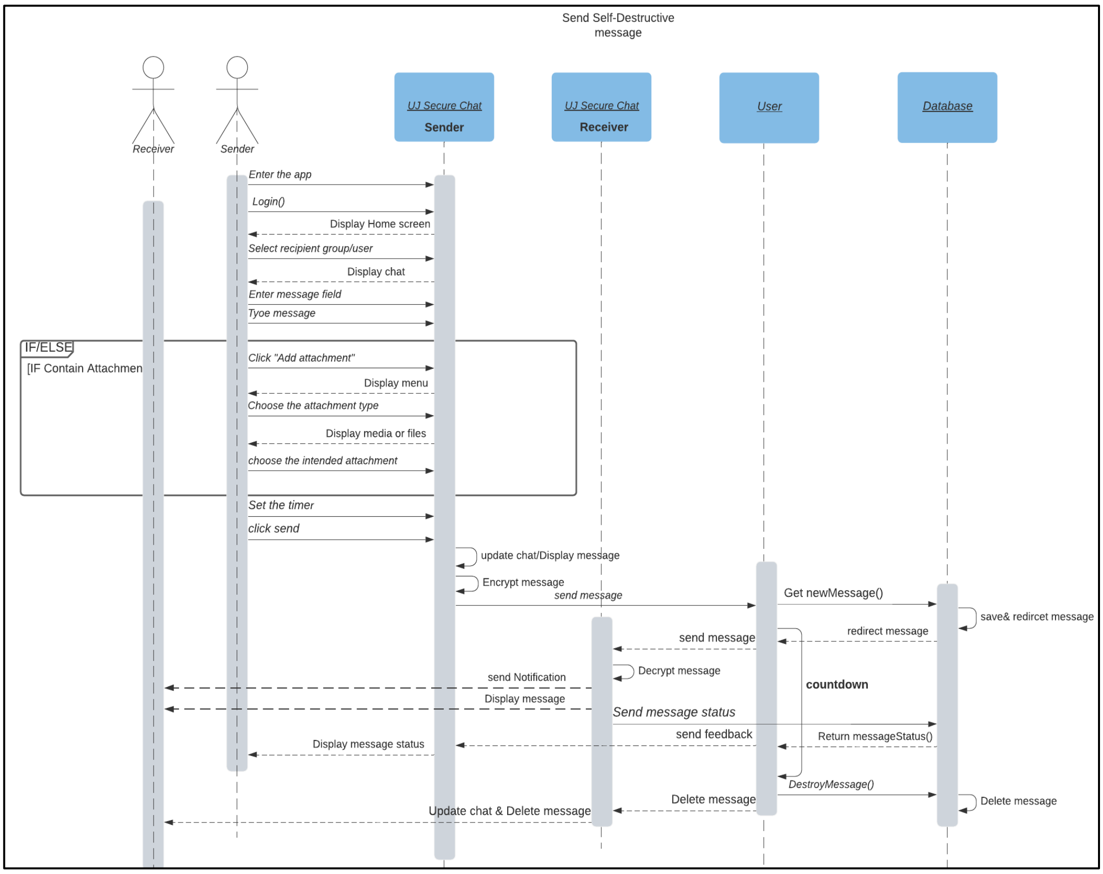


Figure 24 Send destructive message sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, after login, the user can choose to send a self-destructive message which means that this message is available for a specific time determined by the user, before sending the message to the receiver the application will encrypt the message, stores it at the database then at the receiver the application will decrypt the message, and after the time specified by the user have passed then the message will be deleted from the chat and database also it is possible to contain an attachment.

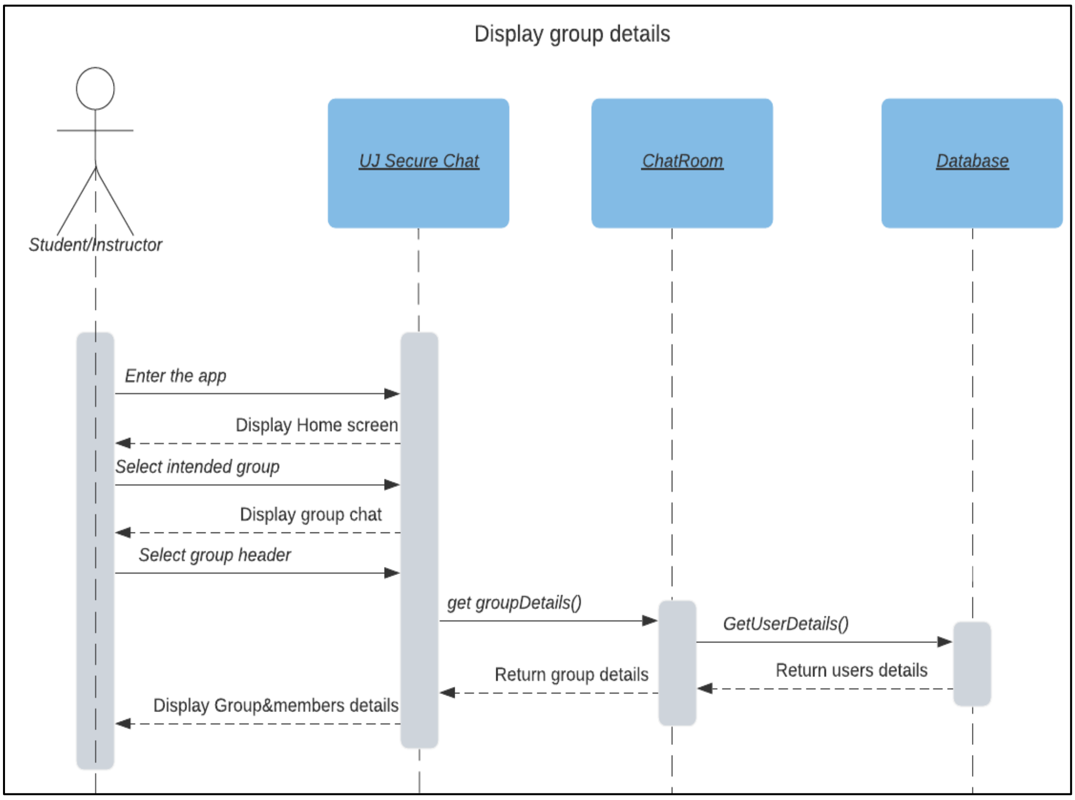


Figure 25 Display group details sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can get group details by clicking on a group header, and then our application will request the group details such as members of the group from the database and return it to the user.

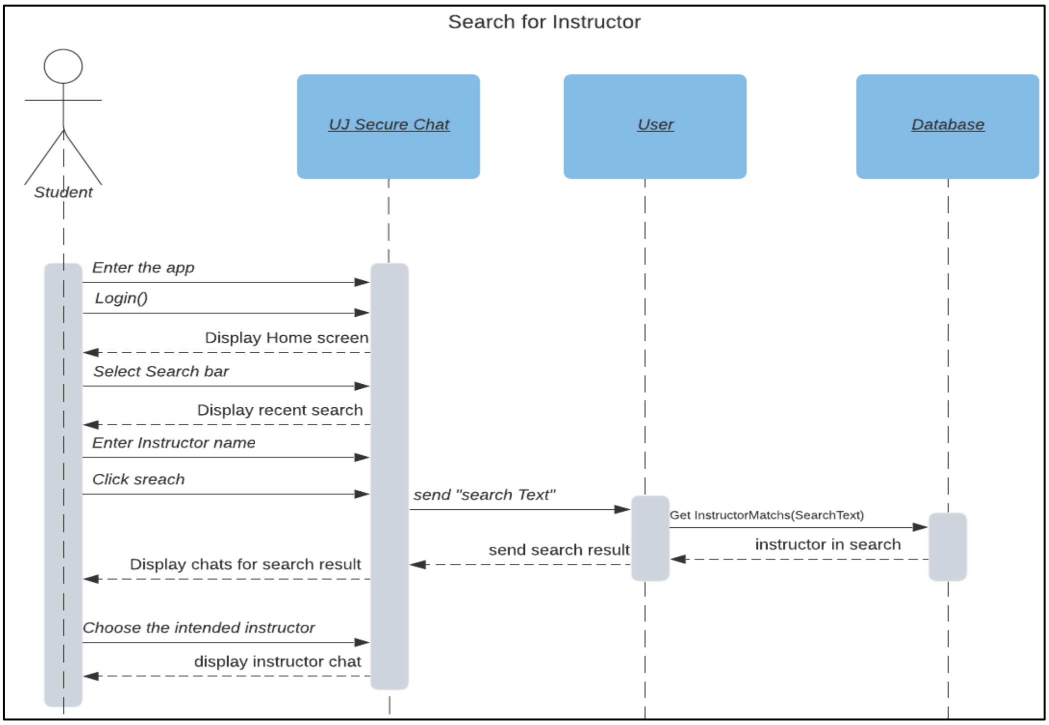


Figure 26 Search for Instructor sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, students can search for a specific instructor by name then our application will search the returned information from the database for the specified instructor.

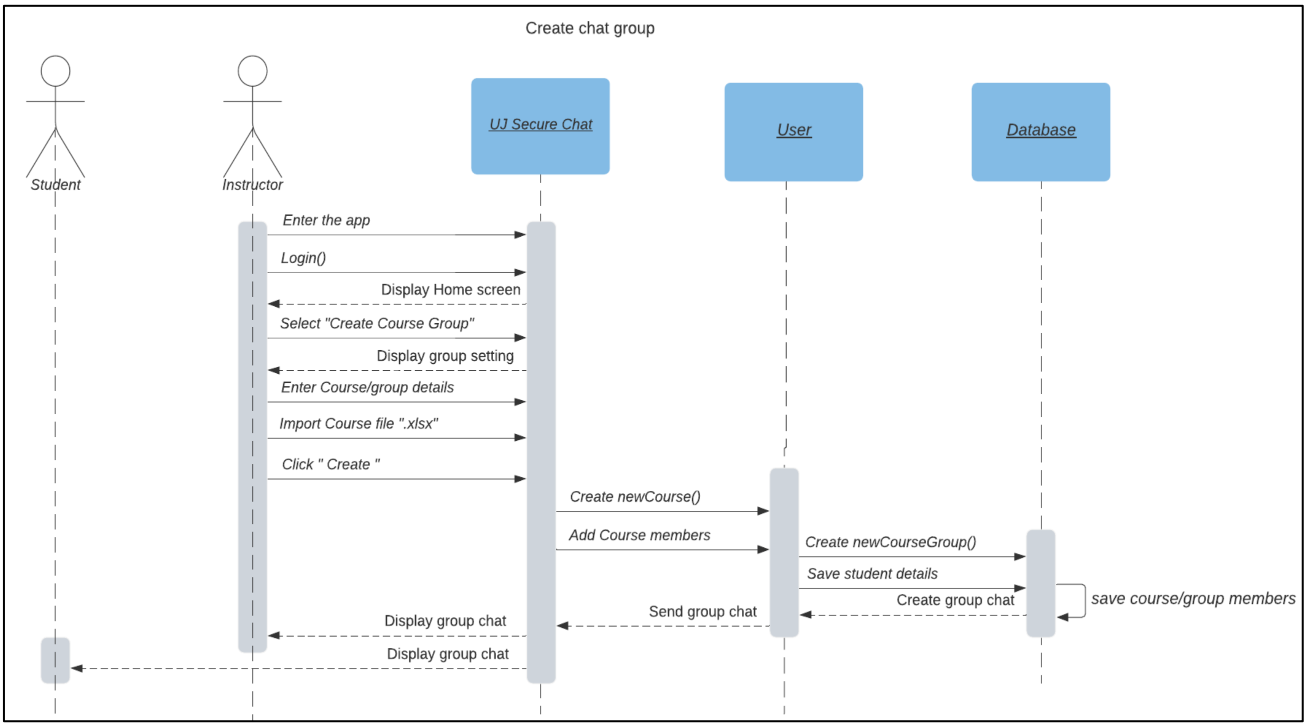


Figure 29 Create chat group sequence diagram

In the figure above the sequence diagram shows how instructor user can interact with our application, the instructor can create a group chat by clicking on create a group chat and providing course name and importing Excel file that contains students to be added to the group then the application will process the request from the instructor, store the group details in the database, and creates the group.

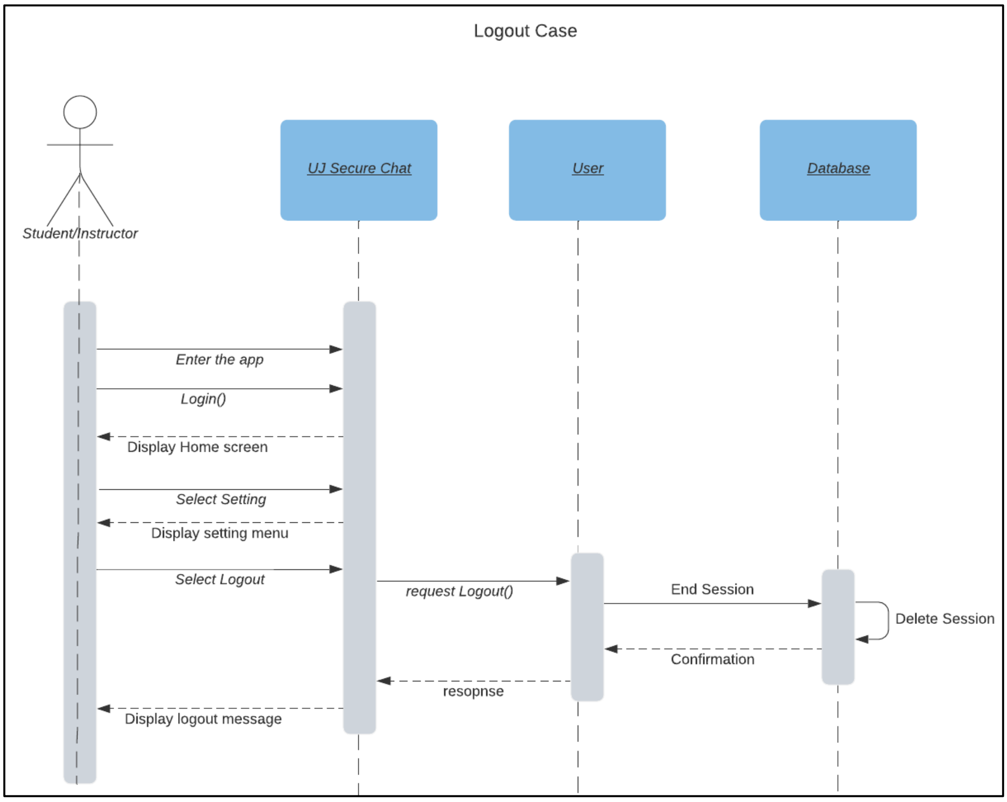


Figure 30 Logout sequence diagram

In the figure above the sequence diagram shows how users can interact with our application, users can log out by selecting logout from the setting menu then after the logout is processed the database will end their session.

4.2.3 Data Modeling (ERD Diagram)

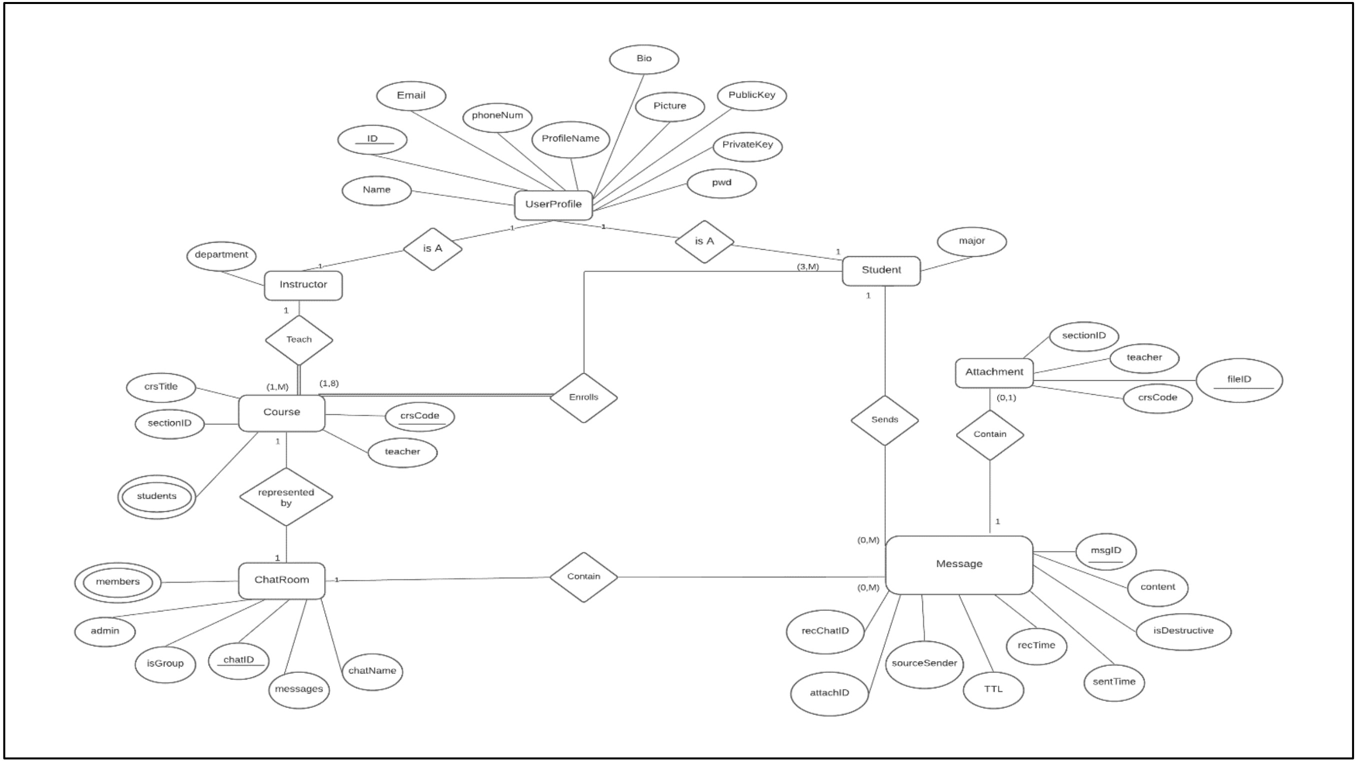


Figure 31 ERD diagram

The figures above represent the logical ERD (Entity Relationship Diagram) that shows the system database, including the attributes of each table and the relationship between them. Our database consists of 7 tables, starting with a UserProfile table that can be a student or an instructor, where that contains the following attributes: Name, ID (where it has unique value), PhoneNum, Email, Publickey, pwd, Picture, Bio, and Privatekey. The student or instructor can have many courses that represent in course table with attributes: crsTitle, sectionID, crsCode (where it has unique value), teacher, and students (where it is a multivalued attribute). The Course table has total participation with the Student and Instructor tables that means the course can not open if no student registers in it and if no instructor can teach the course. Furthermore, each course has one chat room that represents in chatRoom table with attributes: chatName, chatID (where it has unique value), IsGroup, admin, members (where it is a multivalued attribute), and messages. Message can contain attachment where the Message table attributes: recChatID, attachID, sourseSender, TTL, recTime, sentTime, isDestructive, content, msgID (where it has unique value) and the Attachment table attributes: crsCode, fileID (where it has unique value), teacher, sectionID.

4.3 User Interfaces

In the designing and visualization of the system structure the user interfaces represent the design of the screens in which the user interacts with the system, in the following figures there will be all intended interfaces presented with an overall detail of the processes performed by all functions.

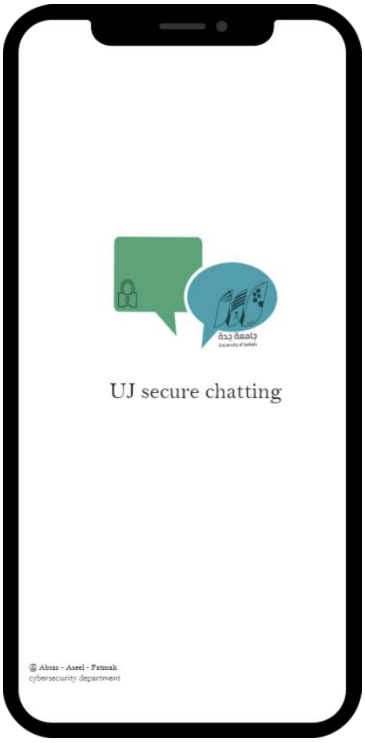
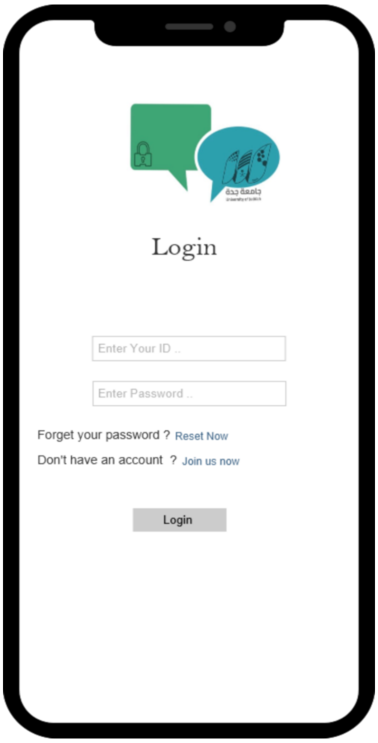


Figure 32 Default page



Forget your password ? Reset Now

Don't have an account ? Join us now

Figure 33 Login page

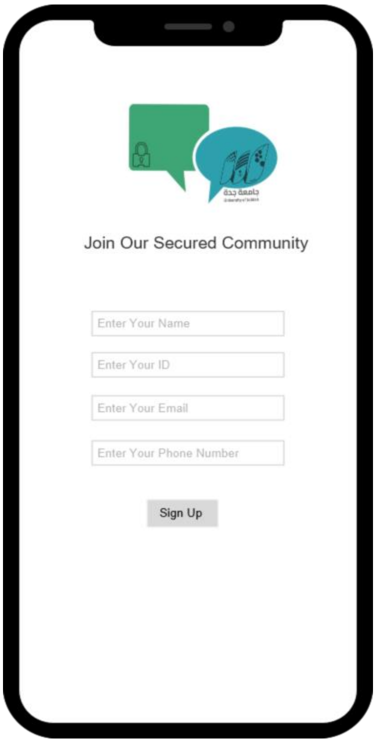
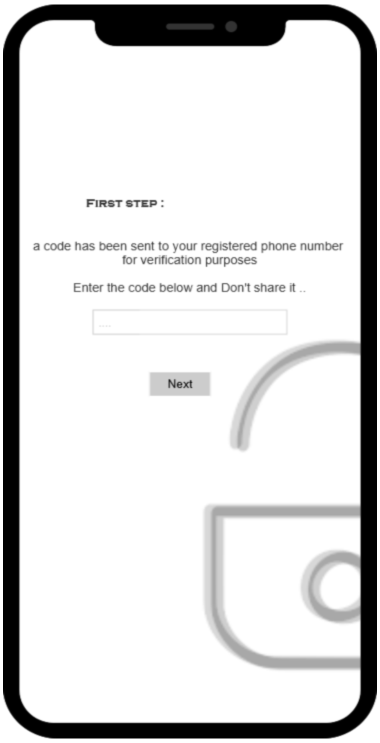


Figure 27 SignUp page

Figure 32 present a proximate design of the first page that will be displayed when the user opens the app and will contain the application logo as well as the copyrights of the system’s owners, it will have a timeout in which the next page will be displayed after 5 seconds.

Figure 33 presents the login page in which the user has 3 options, first, is the login using his ID and password if he is already registered, and if not, the registration will be the option to sign in, the third option is the “forget password “which the user will receive a link on his registered phone number to reset the password.

Figure 34 represents the registration process and its requirement, it will ask the user to enter his name, email, phone number ...etc. to enjoy the app's feature securely.

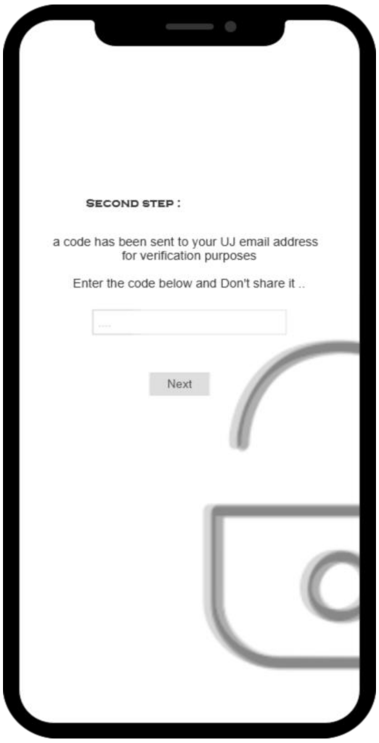


FIRST STEP :

a code has been sent to your registered phone number for verification purposes

Enter the code below and Don't share it ..

Figure 35 phone verification page

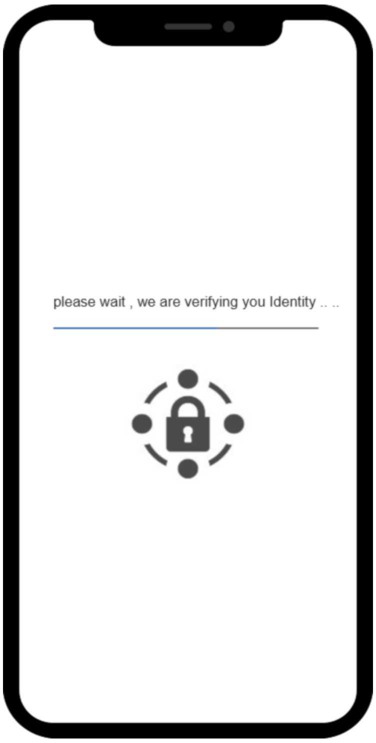


SECOND STEP :

a code has been sent to your UJ email address for verification purposes

Enter the code below and Don't share it ..

Figure 36 *email verification page*

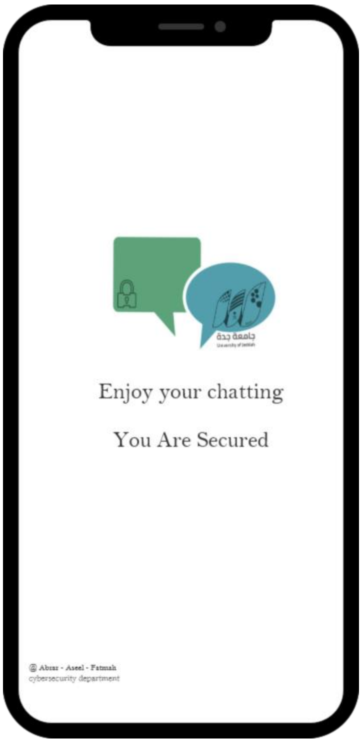


please wait , we are verifying you Identity .. ..

Figure 37 *progress page*

The registration process will require additional 2 steps represented in figure 35 and 36 the first one will represent the phone number verification by sending a one-time passcode to the user's phone number and asking the user to enter that code, also in the second step the verification will be by sending a one-time passcode to the user's UJ email.

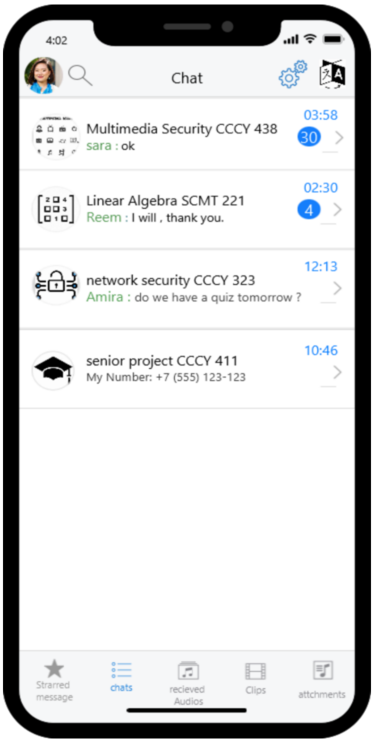
(Figure 37) will ask the user to wait a few seconds and show the verification progress.


Enjoy your chatting

You Are Secured

@ Abrar - Aseel - Fatmah
cybersecurity department

Figure 28 welcome page


4:02

Chat

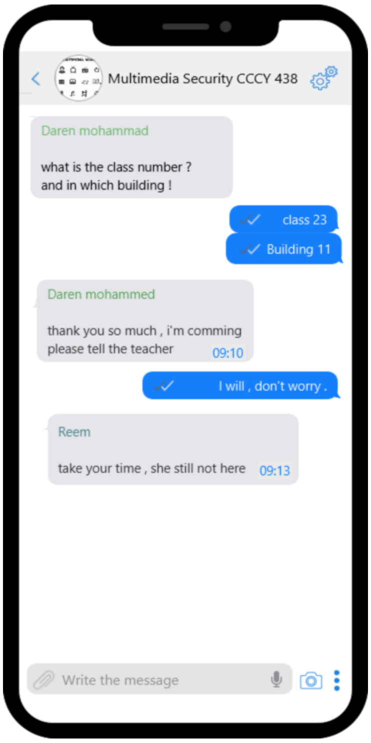
Multimedia Security CCCY 438 — 03:58 — 30
sara : ok

Linear Algebra SCMT 221 — 02:30 — 4
Reem : I will , thank you.

network security CCCY 323 — 12:13
Amira : do we have a quiz tomorrow ?

senior project CCCY 411 — 10:46
My Number: +7 (555) 123-123

Figure 29 Home page


Multimedia Security CCCY 438

Daren mohammad
what is the class number ?
and in which building !

class 23

Building 11

Daren mohammed
thank you so much , i'm comming
please tell the teacher 09:10

I will , don't worry .

Reem
take your time , she still not here 09:13

Figure 40 *chat page*

(Figure 38) represents the welcome page with a 4-second timeout, will appear after the registration or login process has been completed successfully. otherwise, the error message will appear to ask the user to try again.

The next figure 39 represents the home page of the application, which displays the group chats of the courses enrolled to each student with his colleagues the group admin will be the course instructor, and the name is represented by the course code and title.

Figure 40 is a proximate design of the inner style of the group chat, each message will contain the sender's name, time, and message.

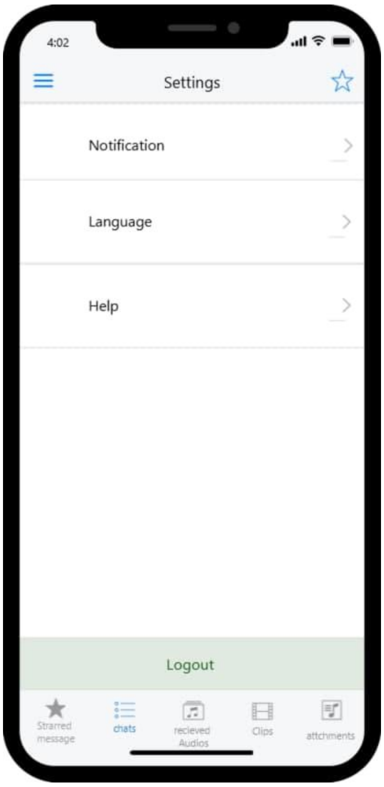


Figure 41 setting page

Figure 41 represents the account settings where the user can control the notification, change language, request help, and log out from the application.

References

[1] "How Did Human Communication Start?," AUG 2015. [Online]. Available: https://www.myevideo.com/how-did-human-communication-start/.

[2] K. Zhang, "Then & now: communication through the ages," *Queens Journal,* 2015.

[3] S. R. Department, "Daily active users of WhatsApp Status 2019," 28 Jan 2021. [Online]. Available: https://www.statista.com/statistics/730306/whatsapp-status-dau/.

[4] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith and M. Beaton, "Teens, Social Media, and Privacy," Pew Research Center's Internet & American Life Project, Washington, D.C., 2013.

[5] P. Dashtinejad, "Security System for Mobile Messaging Applications," Department of ICT,KTH University, Stockholm,Sweden, 2015.

[6] WhatsApp IT department, "WhatsApp Encryption Overview," 2020. [Online]. Available: https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=ZwwHFMAkqOkAX8yv6Q3&_nc_ht=scontent.whatsapp.net&oh=61ade4b60784c304a1f573ba0feb2652&oe=61635219.

[7] c. website, "Messenger Secret Conversations," 18 MAY 2017. [Online]. Available: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

[8] K. A. u. I. d. team, "About "MY KAU"," 7 AUG 2018. [Online]. Available: https://mykau.kau.edu.sa/Default-223111-AR.

[9] Telegram, "Telegram Privacy Policy," 14 August 2018. [Online]. Available: https://telegram.org/privacy#3-3-2-secret-chats.

[10] D. FROST, "Informatics University of California, Irvine," spring ,2016. [Online]. Available: https://frost.ics.uci.edu/inf43/SampleSRS5.pdf.