

SyrenApp (Application chat)

**Software Engineering Department
Senior Project (2)**

Under The Supervision of:
Dr. Baseem Barhoum

By Students:
Abdullah Alabullah
Zakwan Alhassani
Ibrahim al dabaj

ABSTRACT

Teleconferencing or Chatting, is a method of using technology to bring people and ideas together despite of the geographical barriers. The technology has been available for years but the acceptance it was quite recent.

Our project is an example of a chat server.

It is made up of 2 applications the client application, which runs on the users Android Device and server application, which runs on any Android Device on the network.

To start chatting client should get connected to server where they can do private and group chat security

Introduction	7
Problem Statement	8
Project Scheduling.....	8
Business Requirement Documentation	9
Overview	9
Appplication	9
WhatsApp	11
Abstract	11
Introduction	12
Review of Literature	13
Research Methods.....	15
Results and Discussion	16
Its characteristics and advantages:	21
Conclusion	26
Telegram	27
Abstract	27
Its characteristics and advantages:	28
How is Telegram different from WhatsApp?	30
PROJECT SUMMARY	32
Functional and Non-Functional Requirements	32
Functional Requirements	32
User Registration	32
Adding New Contacts	32
Send Message	33
Broadcast Message.....	33
Message Status	33
Requirement ID	33
Statement	33
Non-Functional Requirements	34
Privacy	34
Robustness	34
Performance	34
Statement	34
Use Case Table	35
Use Case Diagram	36
Authentication System	37
Contacts Form	38
Chat Form	39
Activity Diagram	40
Contacts Form, Chat Form	40

Entity Relationship Diagram.....	40
Project Risk Management	42
Identification	42
User Manual.....	46
Registration for new Member	46
Login Features.....	47
Private Chatting	48
Adding Friend	49
Chat Forms.....	50
Block Friend	51
Account Settings	52
MD5	53
History and cryptanalysis	54
Security	55
Overview of security issues.....	56
Collision vulnerabilities	56
Preimage vulnerability	58
Applications	59
Algorithm	61
Conclusion	63
Troubleshooting.....	63
References	64

Figure 1 Project Scheduling.....	8
Figure 2. Growth of WhatsApp users 2013 to 2016.....	12
Figure 3. Age and Gender of Participants.....	16
Figure 4. Everyday Usage of WhatsApp among Different Gender.....	17
Figure 5. Maturity of WhatsApp Users with Gender Distribution.	17
Figure 6 :Participants Opinion on Usage of WhatsApp as Calling or Messaging.....	18
Figure 7: Opinion on Usage of WhatsApp as Calling or Phone for Calling.	18
Figure 8: Participants Age and Duration of Usages.	19
Figure 9: Participants Everyday Usages of WhatsApp and Age.	20
Figure 10:Participants Involvement in WhatsApp Groups and Gender.....	20
Figure 11:GROUP CHAT.....	21
Figure 12: WHATSAPP ON WEB AND DESKTOP.....	22
Figure 13:WHATSAPP VOICE AND VIDEO CALLS.....	22
Figure 14:END-TO-END ENCRYPTION.....	23
Figure 15:PHOTOS AND VIDEOS.....	24
Figure 16:Document Sharing.....	25
Figure 17:Document Sharing.....	25
Figure 18:Cloud-Based.....	28
Figure 19:open API and protocol.....	29
Figure 20: Use Case Table of Chat Application.....	35
Figure 21:Use cacse Diagram.....	36
Figure 22:e Case Diagram of Authentication System.....	37
Figure 23: Use Case Diagram of Contacts Form.....	38
Figure 24: Use Case Diagram of Chat Form.	39
Figure 25: Activity Diagram of Contacts Form, Chat Form.	40
Figure 26: Entity Relationship Diagram of Chat Application.	41
Figure 27: Registration for new Member.....	46
Figure 28: Login Features.....	47
Figure 29: Private Chatting.	48
Figure 30: Adding Friend.....	49
Figure 31: Chat Forms.....	50
Figure 32:Block Friend.	51
Figure 33: Account Settings.	52
Figure 34: MD5 digests	59
Figure 35: MD5 Algorithm.....	61

الفصل الأول

التعريف بالمشروع

1. Introduction

Communication is a mean for people to exchange messages.

It has started since the beginning of human creation.

Distant communication began as early as 1800 century with the introduction of television, telegraph and then telephony.

Interestingly enough, telephone communication stands out as the fastest growing technology, from fixed line to mobile wireless, from voice call to data transfer.

The emergence of computer network and telecommunication technologies bears the same objective that is to allow people to communicate.

All this while, much efforts has been drawn towards consolidating the device into one and therefore indiscriminate the services.

Chatting is a method of using technology to bring people and ideas together despite of the geographical barriers.

The technology has been available for years but the acceptance it was quit recent. Our project is an example of a chat server.

It is made up of applications the client application which runs on the users mobile and server application which runs on any pc on the network.

To start chatting our client should get connected to server where they can do Group and private chatting.

2. Problem Statement

This project is to create a chat application with a server and users to enable the users to chat with each others.

To develop an instant messaging solution to enable users to seamlessly communicate with each other.

The project should be very easy to use enabling even a novice person to use it.

3. Project Scheduling

This document provides a scalable scheduling tool and associated schedule development, analysis, and monitoring methods to prepare, monitor, and report project schedules.

Our Project is not that complex so we will not use very complex scheduling method.

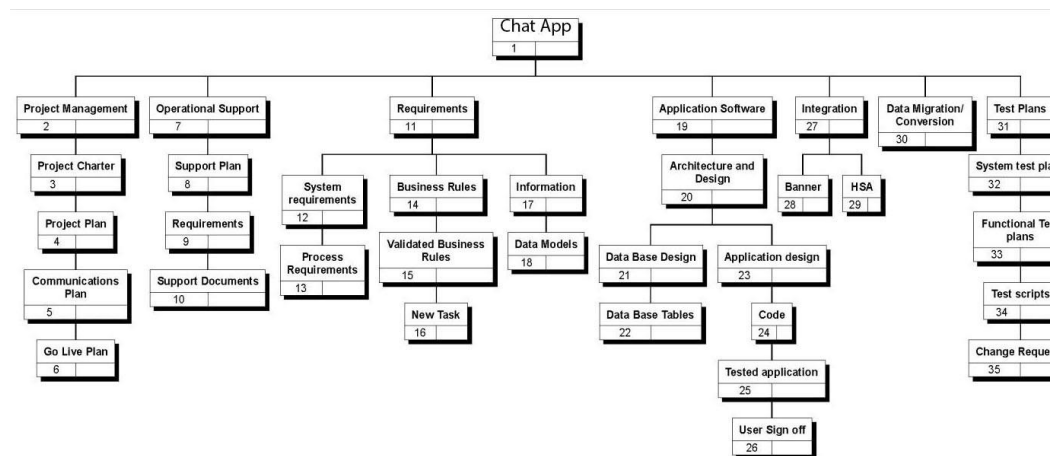


Figure 1 Project Scheduling

4. Business Requirement Documentation

11. Overview

This Requirements Document will provide the requirements for a Chat Application.

Both functional and non requirements will be documented.

functional requirements will be documented.

12. Application

Chat Applications are in scope.

الفصل الثاني

الدراسة المرجعية

WhatsApp

Abstract

WhatsApp is a popular mobile application for providing instant messaging service in smartphones. It uses Internet services to communicate different type of text and multimedia messages between users or groups.

Its users worldwide have crossed the figure of one billion in February 2016.

The effect of WhatsApp on our lives, culture, and society keeps on increasing.

It is also becoming popular tool for marketing in businesses and publicity in politics. This growth has also drawn the attention of researchers to understand the implications and effect of WhatsApp on its user's social and personal life.

We investigated the usage and effect of WhatsApp in the regions of Northern India. We performed an internet based survey using open source Lime survey software and obtained responses.

Total 460 responses had been received in which only 136 responses were considered for analysis those have completed all questions and having more than 18 years of age. The users in India made a slow shift from all social networking sites to WhatsApp in a quick span of time. This survey results show that there is a significant impact of WhatsApp on its users. Around 66% of WhatsApp users believe that WhatsApp has improved their relationship with friends.

More than 63% of its users think it is not harmful for them.

There are several other analyses presented in this paper based on age-groups and gender of WhatsApp users.

This survey analysis may be useful for academicians and researchers for understanding the behavior of WhatsApp users and reflect the possibility of using WhatsApp in education, social services and governance.^[1]

1. Introduction

The world is dynamically changing due to the advancement in the mobile technology. These days it is almost impossible to avoid the presence of mobile applications or called Mobile Apps.

Most of the People can praise the various mobile applications that they use in their everyday lives.

Several people are heavily dependent of the usage of such applications for their day to day activities⁶. Technology is evolving at a really quick rate, and what are its impacts on the general public need to be studied and analyzed.

WhatsApp is one among the major change in mobile apps communication in the recent past, it users is growing very fast on mobile phones and also on the computers. The graph below shows its grown of users in recent years. This statistic shows a timeline with the amount of monthly active WhatsApp users worldwide as of February 2016.

As of that month, the mobile messaging app announced more than 1 billion monthly active users, up from over 700 million in January 2015. The service is one of the most popular mobile apps worldwide¹.^[1]

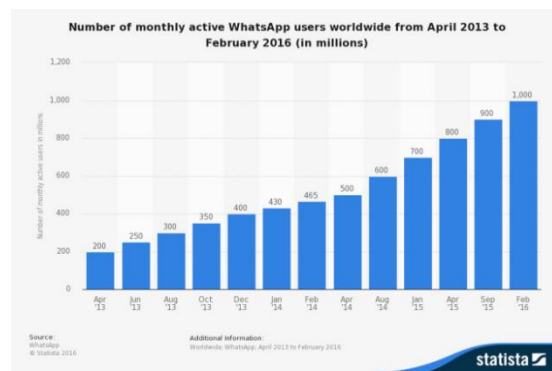


Figure 2. Growth of WhatsApp users 2013 to 2016.

WhatsApp has been around for a short while however its regular updates have been improving it's the functionality since its release date.

Some of its features are also updated recently after initiating this online survey, hence these feature could not be addressed appropriately.

Mainly WhatsApp was started to interchange SMS with a cross-platform feature. If

you have got unlimited text, it's still helpful. WhatsApp uses mobile network data or local area network to send and receive messages.

In addition to text communication, users can also send pictures, video and audio media messages easily.

Since the Smartphones became common, several electronic communication services for smartphones were launched however WhatsApp has become highly popular among them. Mobile messaging applications like WhatsApp have emerged as largely free alternatives to standard SMS messaging.

Besides text electronic messaging they additionally support the exchange of pictures, videos, or voice records^{2,3}. Besides all, this Application is very addictive and might produce an excellent impact on regular users, and with the exception of that it will leave a trace that becomes tough to manage and cure. ^[5]

2. Review of Literature

Various studies and analysis has been done on the usage and impact of WhatsApp. Some of these studies are for finding the impact of WhatsApp on the students and some are based on for the general public in a local region.

However, any widespread survey analysis for general public is not found during our literature review.

Some of these papers details are discussed below.

According to Financial Times, "WhatsApp Messenger, an app which allows unlimited free text-messaging between users, has done to SMS on mobile phones what Skype did to international calling on landlines.

It has become a top-selling iPhone, Android and BlackBerry app in dozens of markets, without a penny spent on promotion or advertising."^{2,3}

In a paper entitled "What Makes Smartphone Users Satisfied with the Mobile Instant Messenger?: Social Presence, Flow, and Self-disclosure"⁵ Author has studied and analyzed factors affecting user satisfaction by conducting a survey on 220 users of mobile instant messengers in smartphones. The survey results showed that self-disclosure, flow, and social presence significantly affected user satisfaction.

Authors of “Privacy Implications of Presence Sharing in Mobile Messaging Applications”⁷ conducted a user study with two independent groups (19 participants in total), in which we collected and analyzed their presence information over four weeks of regular WhatsApp use and conducted follow-up interviews.

Their results show that presence information alone is sufficient to accurately identify, for example, daily routines, deviations, times of inappropriate mobile messaging, or conversation partners. Another study is done on the WhatsApp Usage on the Students Performance in Ghana⁸.

The results of this study showed the following: WhatsApp takes much of students study time, results in procrastination related problems, destroys students’ spellings and grammatical construction of sentences, leads to lack of concentration during lectures, results in difficulty in balancing online activities (WhatsApp) and academic preparation and distracts students from completing their assignments and adhering to their private studies time table.

In a study of southern part of India (Chennai region) was conducted on the age group of between 18 to 23 years to investigate the importance of WhatsApp among youth⁹.

Through this study, It was found that students spent 8 hours per day on using WhatsApp and remain online almost 16 hours a day.

All the respondents agreed that they are using WhatsApp for communicating with their friends. They also exchange images, audio and video files with their friends using WhatsApp. It was also proved that the only application that the youth uses when they are spending time on their smart phone is WhatsApp.

In a paper “Smartphone application usage amongst students at a South African University”, a study is performed to evaluate the usage of social networking applications in South African University.

According to this study, it is proved that students spend an average of five hours per day on their smartphones communicating with others through social networking applications¹⁰.

An article of Times of India Online newspaper dated June 16, 2013, covered a survey, which was conducted by Tata Consultancy Services in the years 2012-2013. The target group of this survey was 17,500 high school students of age around 14-15 years across 14 Indian cities.

The result shows that almost 70% of the students possess smart phones and have started utilizing the full potential of smart phones⁹.

According to Business Standard in its news on March 3, 2014, the combined usage of WhatsApp and Facebook contributes to over half an hour per day to the overall time spent on smartphones, says a study^{11[6]}

3. Research Methods

The study uses Lime survey, open source software for conducting online survey.

A form was developed with both close-ended and open ended questions to assess the demographics of users, usage of WhatsApp options, intensity of usage, reasons of using, and impact on social and private life of users.

This study examines the usage and impact of WhatsApp mobile application among the users in the regions of Northern India.

The objectives for the study are:

1. To analyze the intensity of WhatsApp usage and its popular services
2. To identify the degree of positive or negative impacts of using WhatsApp
3. To seek the frequency and interactivity of WhatsApp among its users.
4. To explore the options of WhatsApp used the foremost by adults (more than 18 years of age).
5. To find out whether or not users are satisfied with the WhatsApp.
6. To explore the impact of WhatsApp on individual personal and social life.

The open ended questions gave the samples an opportunity to express their views regarding WhatsApp messenger and to list out a number of the options that they just like the most within the app.

This gave the researcher to collect additional data relating to WhatsApp messenger and users viewpoint.

The researcher used judgmental sampling to identify the samples for the study. Some questions were designed to ascertain the validity of answers and seriousness of users toward the filling of the form.

Survey was distributed to various regions of India.

The researchers made use of each primary and secondary data, that were gathered from diverse sources, including, archival sources, text books, journals/ articles (both publish and unpublished), and websites^[7]

4. Results and Discussion

A survey was conducted on actual users of smartphone instant messengers. The questionnaire was performed an internet based survey using open-source Lime survey software and obtained responses. Total 460 responses had been received in which only 136 responses were considered for analysis those have completed all questions and having more than 18 years of age.

In total valid 136 entries 36 female and 100 males entries are distributed in different age groups as shown below in the Figure

2. This shows that most of adult WhatsApp users belong to age group of 18 to 50 years. We have not received any entry apart from male and female. The gender distribution reflects that only 36% of women candidates have participated in the survey compared to male candidates. However, it may not be sufficient to draw such conclusion.^[2]

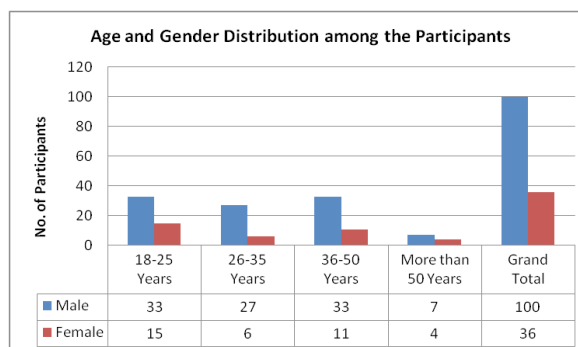


Figure 3. Age and Gender of Participants

To know the maturity of our participants of using WhatsApp, we have collected information. So that opinions of these participants can be justified. The Figure 3 given below shows that most of the participants including male and female are using WhatsApp since one year.

The Figure 4 given below depicts the everyday usage of WhatsApp among different gender. Overall we can see that most of the participants are using WhatsApp 15 to 60 minutes daily. This figure also indicates that both male and female are equally involved in using WhatsApp daily,

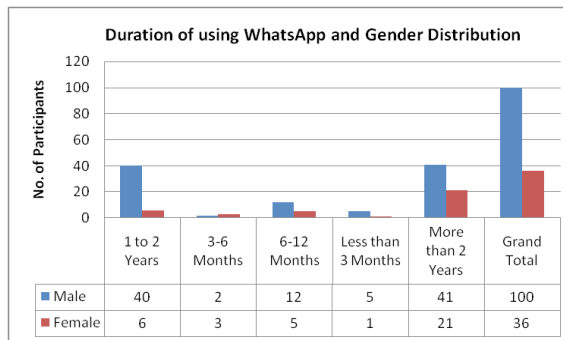


Figure 4. Everyday Usage of WhatsApp among Different Gender.

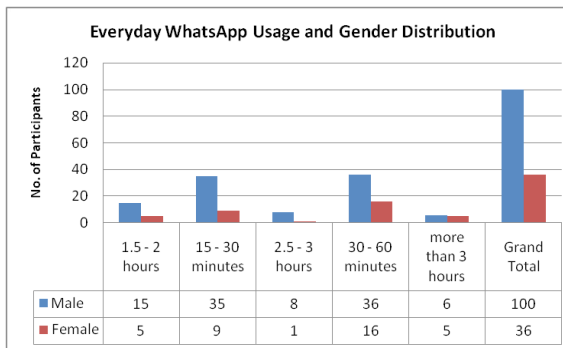


Figure 5. Maturity of WhatsApp Users with Gender Distribution.

One of the objectives of our survey is to find the WhatsApp services preferred by the users. To know this direct question of using WhatsApp compared to normal SMS/Calling of mobile phone is asked to the users. The Figure 5 shows that participants are not giving direct indication towards one opinion.

However, participants those are preferring WhatsApp over mobile phone is slightly high. Considering the minor difference, we are unable to make and conclusion from this result.

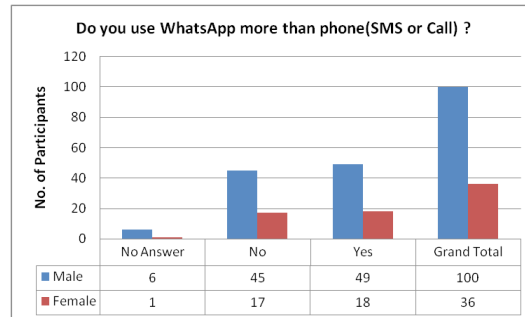


Figure 6 :Participants Opinion on Usage of WhatsApp as Calling or Messaging

To know which service of WhatsApp is more used, we have asked to the participants whether they like WhatsApp calling feature or not. As shown in Figure 6 below, 83% of our participants mentioned that they do not like calling service of WhatsApp in comparison to normal talking using mobile phone. This result gives strong indication that the internet based calling service of WhatsApp need more improvement for its wider acceptance.

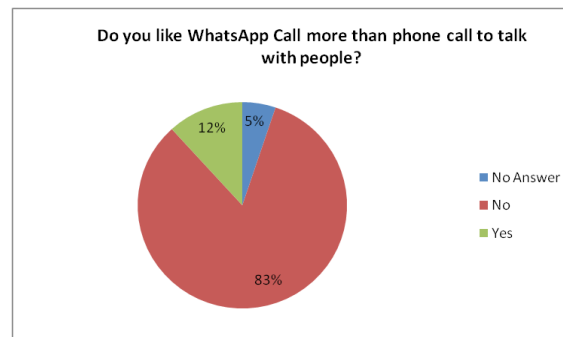


Figure 7: Opinion on Usage of WhatsApp as Calling or Phone for Calling.

To understand the involvement of different age groups and gender groups with the WhatsApp following chart is generated.

This Figure 7 depicts that 73% of our participants are using this App for more than a year and fall between 18-50 years.

Considering the maturity of using WhatsApp, the opinion of our participants seek through this questionnaire would be more significant.

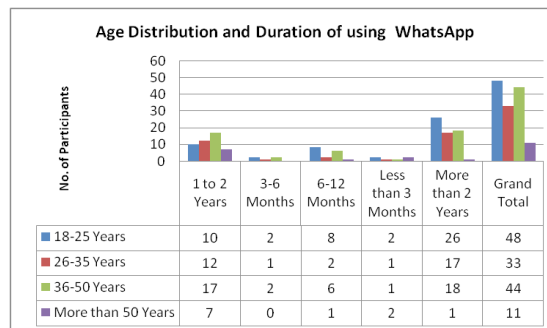


Figure 8: Participants Age and Duration of Usages.

The Figure 8 below shows the age distribution and everyday usage of WhatsApp by participants. It shows that 79% of our participants of between 18-50 years are using WhatsApp 15 to 60 minutes daily.

Figure 9 shows that 57% male and 55% females are member of 3 to 6 groups on the WhatsApp. 37% males are 38% females are having membership of 1 to 3 groups.

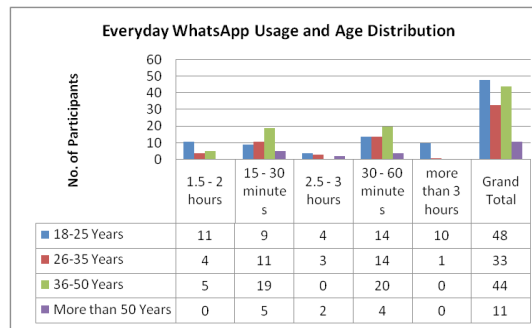


Figure 9: Participants Everyday Usages of WhatsApp and Age.

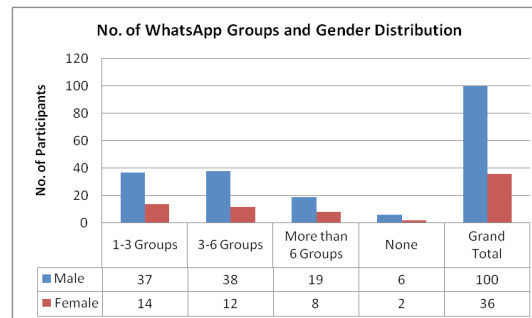


Figure 10: Participants Involvement in WhatsApp Groups and Gender.

Age distribution and people involvement on the WhatsApp groups is reflected in the Figure 10 given below. It shows that 57% of population is having membership of 3 to 6 groups and 37% of people are members of 1 to 3 groups between 18 to 59 years of age.

Mostly people of 18 to 25 years are involved in the groups, however people of 36 to 50 years are also having high involvement in the WhatsApp groups.^[3]

Its characteristics and advantages:

GROUP CHAT:

Groups to keep in touch

Keep in touch with the groups of people that matter the most, like your family or coworkers. With group chats, you can share messages, photos, and videos with up to 256 people at once.

You can also name your group, mute or customize notifications, and more.

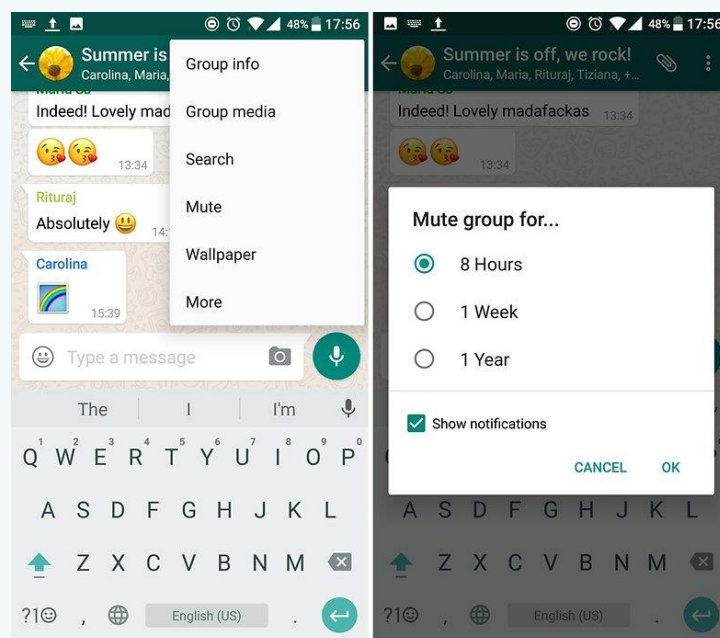


Figure 11:GROUP CHAT

WHATSAPP ON WEB AND DESKTOP:

Keep the Conversation Going With WhatsApp on the web and desktop, you can seamlessly sync all of your chats to your computer so that you can chat on whatever device is most convenient for you.



Figure 12: WHATSAPP ON WEB AND DESKTOP

WHATSAPP VOICE AND VIDEO CALLS:

Speak Freely

With voice calls, you can talk to your friends and family for free*, even if they're in another country. And with free* video calls, you can have face-to-face conversations for when voice or text just isn't enough. WhatsApp voice and video calls use your phone's Internet connection, instead of your cell plan's voice minutes, so you don't have to worry about expensive calling charges.

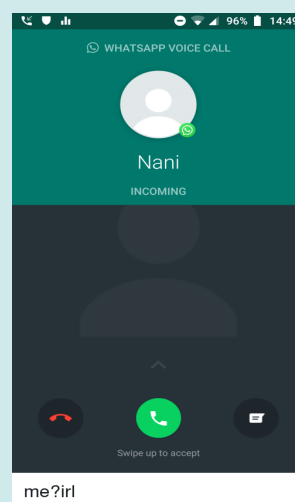


Figure 13: WHATSAPP VOICE AND VIDEO CALLS

END-TO-END ENCRYPTION:

Security by Default

Some of your most personal moments are shared on WhatsApp, which is why we built end-to-end encryption into the latest versions of our app. When end-to-end encrypted, your messages and calls are secured so only you and the person you're communicating with can read or listen to them, and nobody in between, not even WhatsApp.

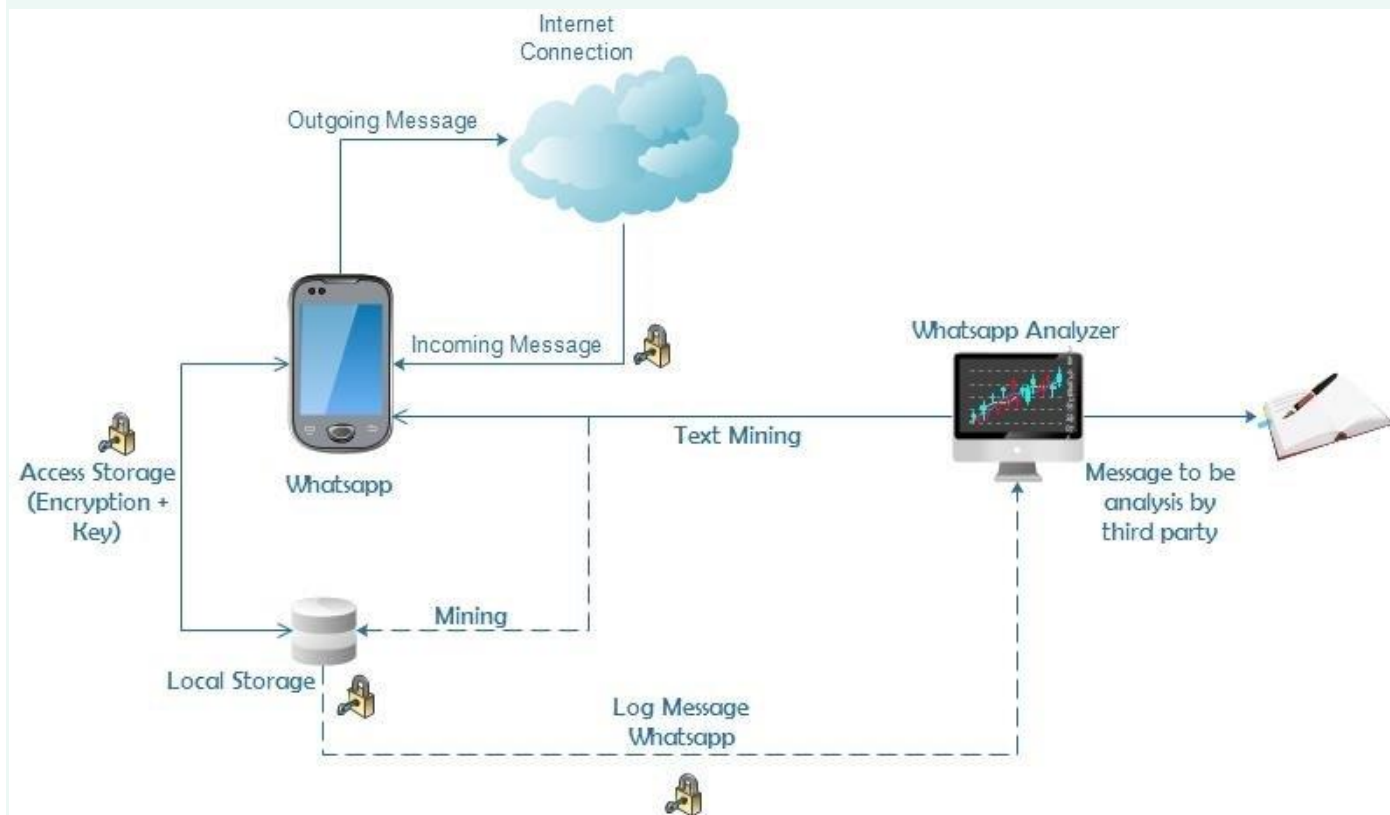


Figure 14:END-TO-END ENCRYPTION

PHOTOS AND VIDEOS:

Share Moments that Matter

Send photos and videos on WhatsApp instantly. You can even capture the moments that matter to you most with a built-in camera. With WhatsApp, photos and videos send quickly even if you're on a slow connection.

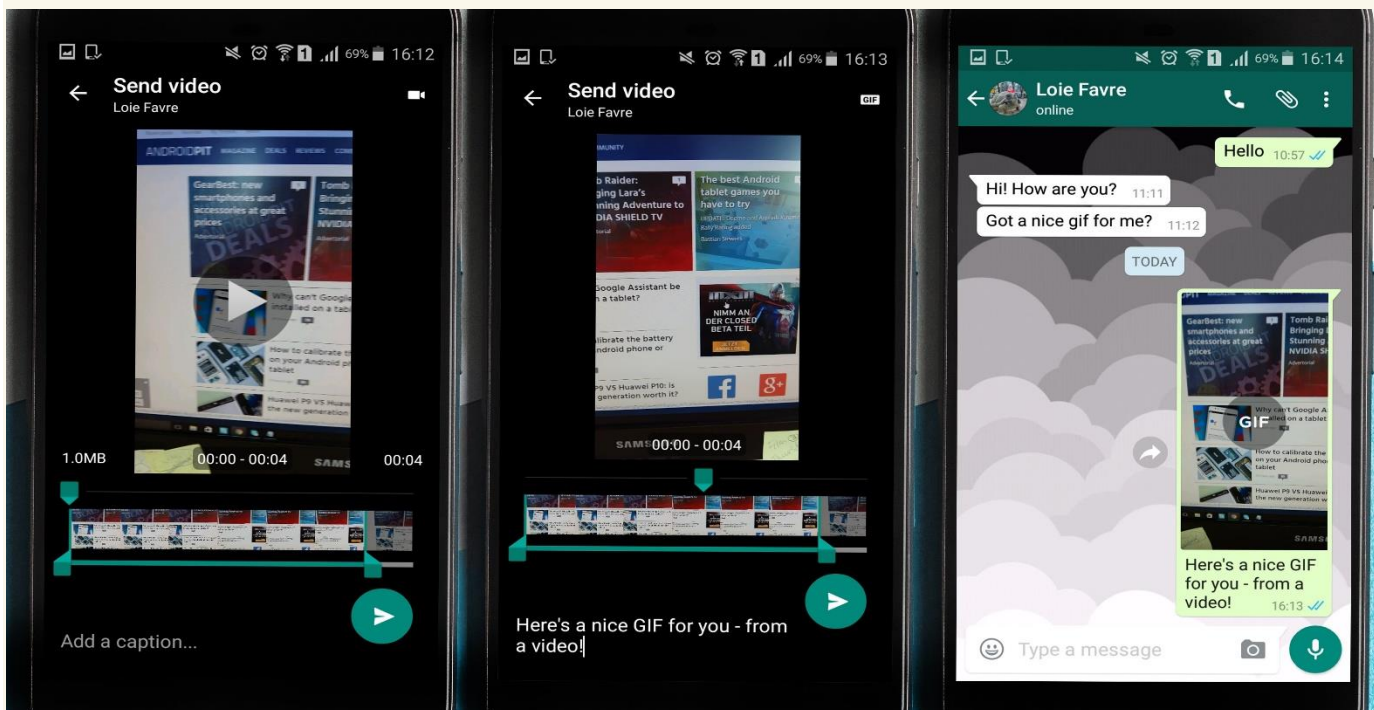


Figure 15:PHOTOS AND VIDEOS

VOICE MESSAGES:

Say What's on Your Mind

Sometimes, your voice says it all. With just one tap you can record a Voice Message, perfect for a quick hello or a longer story.

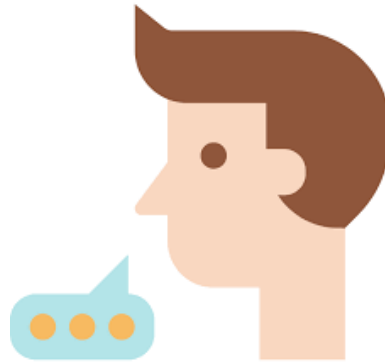


Figure 16: Document Sharing

DOCUMENTS:

Document Sharing Made Easy

Send PDFs, documents, spreadsheets, slideshows and more, without the hassle of email or file sharing apps. You can send documents up to 100 MB, so it's easy to get what you need over to who you want.^[9]

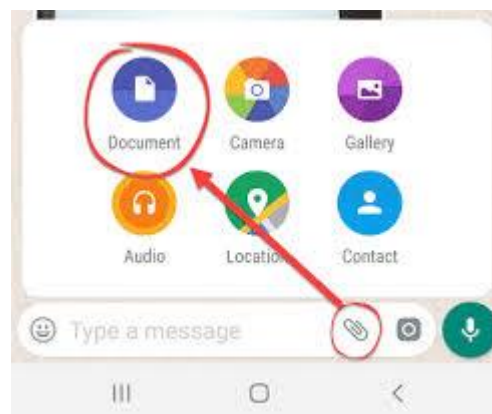


Figure 17: Document Sharing

5. Conclusion

The sample for this study was limited to a 136 respondents in India.

The study may be extended to additional cities with more respondents.

The study ought to have enclosed alternative apps like Viber and Hyke messenger that is gaining quality in today's state of affairs.

There is limited literature review available in Indian context, with relation to WhatsApp usage. Several studies were done on foreign context than in India.

Many studies conducted in India by taking the users as respondents have discovered that smart devices and unprecedented levels of online access are creating this generation the foremost connected.

Previously, only friends and lovers tend to possess robust relationships with intimate conversations.

However currently whoever you chat through WhatsApp, you develop intimate conversations. WhatsApp has created a way of belongingness, distance and intimacy with friends and relatives.

it's created a psychological expertise of being shut and caring.

Currently WhatsApp is getting used by youth for creating, sharing and exchanging information.^[8]

Telegram

Abstract

Telegram is a messaging app with a focus on speed and security, it's superfast, simple and free. You can use Telegram on all your devices at the same time — your messages sync seamlessly across any number of your phones, tablets or computers.

With Telegram, you can send messages, photos, videos and files of any type (doc, zip, mp3, etc), as well as create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. You can write to your phone contacts and find people by their usernames.

As a result, Telegram is like SMS and email combined and can take care of all your personal or business messaging needs.

In addition to this, we support end-to-end encrypted voice calls.

The alpha version of Telegram for Android officially launched on October 20, 2013.

More and more Telegram clients appear, built by independent developers using Telegram's open platform.

Telegram is supported by Pavel Durov and his brother Nikolai. Pavel supports Telegram financially and ideologically while Nikolai's input is technological. To make Telegram possible, Nikolai developed a unique custom data protocol, which is open, secure and optimized for work with multiple data-centers. As a result, Telegram combines security, reliability and speed on any network. ^[11]

1. Its characteristics and advantages:

Private

Telegram messages are heavily encrypted and can selfdestruct.

Cloud-Based

Telegram lets you access your messages from multiple devices.



Figure 18:Cloud-Based

Fast

Telegram delivers messages faster than any other application.

Distributed

Telegram servers are spread worldwide for security and speed.

Open

Telegram has an open API and protocol free for everyone.

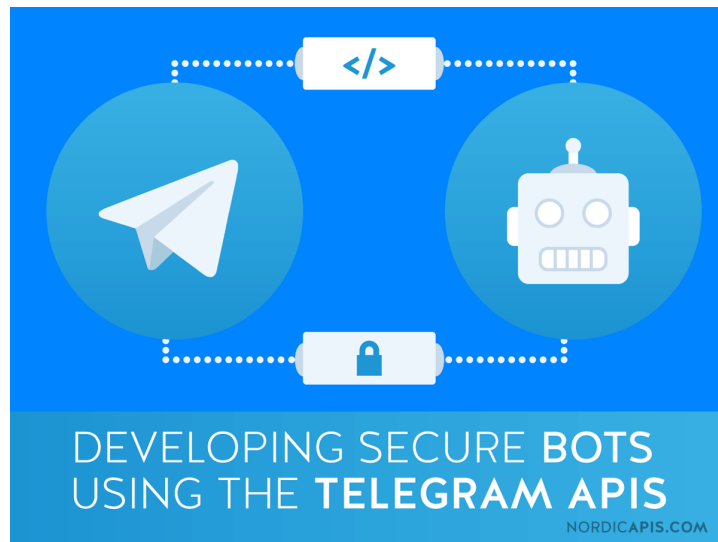


Figure 19: open API and protocol

Free

Telegram is free forever. No ads. No subscription fees.

Secure

Telegram keeps your messages safe from hacker attacks.

Powerful

Telegram has no limits on the size of your media and chats.

We Can do It!

Help make messaging safe again spread the word about Telegram. ^[11]

How is Telegram different from WhatsApp?

Unlike WhatsApp, Telegram is a cloud based messenger with seamless sync. As a result, you can access your messages from several devices at once, including tablets and computers, and share an unlimited number of photos, videos and files (doc, zip, mp3, etc.) of up to 1,5 GB *each*. And if you don't want to store all that data on your device, you can always keep it in the cloud.

Thanks to our multi-data center infrastructure and encryption, Telegram is faster and way more secure. On top of that, Telegram is free and will stay free no ads, no subscription fees, forever.

Our API is open, and we welcome developers to create their own Telegram apps. We also have a Bot API, a platform for developers that allows anyone to easily build specialized tools for Telegram, integrate any services, and even accept payments from users around the world.

And that's just the tip of the iceberg. Don't forget to check out this paragraph for even more exclusive stuff.^[11]

الفصل الثالث

تحليل وتصميم النظام

PROJECT SUMMARY

1. Functional and Non-Functional Requirements

11. Functional Requirements

i. User Registration

User must be able to register for the application through a valid phone number.

On installing the application, user must be prompted to register their phone number.

If user skips this step, application should close.

The users phone number will be the unique identifier of his/her account on Chat Application.

ii. Adding New Contacts

The application should detect all contacts from the users phone book. If any of the contacts have user accounts with Chat Application, those contacts must automatically be added to the users contact list on Chat Application.

If any of the contacts have not yet registered on Chat Application, user should be provided with an invite option that sends those contacts a regular text message asking them to join Chat Application along with a link to the Chat Application on GooglePlaystore.

iii. Send Message

User should be able to send instant message to any contact on his/her Chat Application contact list.

User should be notified when message is successfully delivered to the recipient by displaying a tick sign next to the message sent.

iv. Broadcast Message

User should be able to create groups of contacts. User should be able to broadcast messages to these groups.

v. Message Status

User must be able to get information on whether the message sent has been read by the intended recipient. If recipient reads the message, 2 ticks must appear next to the message read.

Requirement ID	Requirement
FR001	App must have Privacy for user
FR002	App Should have Friend List
FR003	User shall be able to clear chat history
FR004	User shall be able to add friend
FR005	User shall be able to block or remove friend
FR006	User shall be able to Contact with Maintenance team

2. Non-Functional Requirements

i. Privacy

Messages shared between users should be encrypted to maintain privacy.

ii. Robustness

In case users device crashes, a backup of their chat history must be stored on remote database servers to enable recoverability.

iii. Performance

Application must be lightweight and must send messages instantly.

Non-Functional Requirements

ID	Statement
NFR001	Chat App should be secure from hackers
NF002	All data must be backed up
NF003	Chat Application will be ready to launch within 60 days

1. Use Case Table








Level 0	Level 1	Level 2	Actor
Chat Application	Authentication System	Registrar Login Logout	  User Admin
	Contacts Form	Friend List Find Friend Add Friend Remove Friend Block Friend	 User
	Chat Form	Send Message Group Chat Best Friend	 User
	Maintenance	User's Profile Database	 Admin
	Monitor	Check History Feedback	  Admin User

Figure 20: Use Case Table of Chat Application.

1. Use Case Diagram

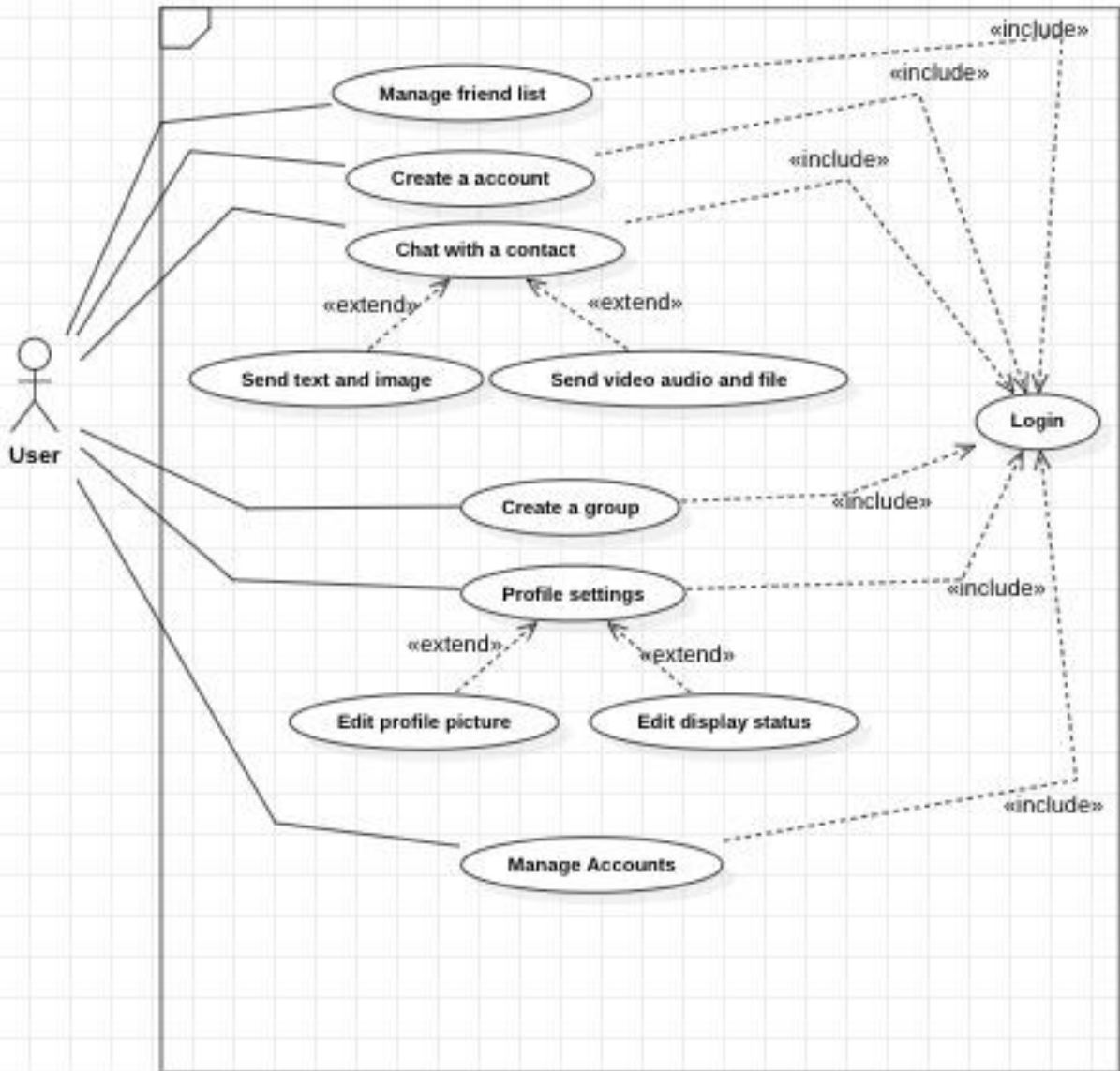


Figure 21:Use cacse Diagram

11.Authentication System

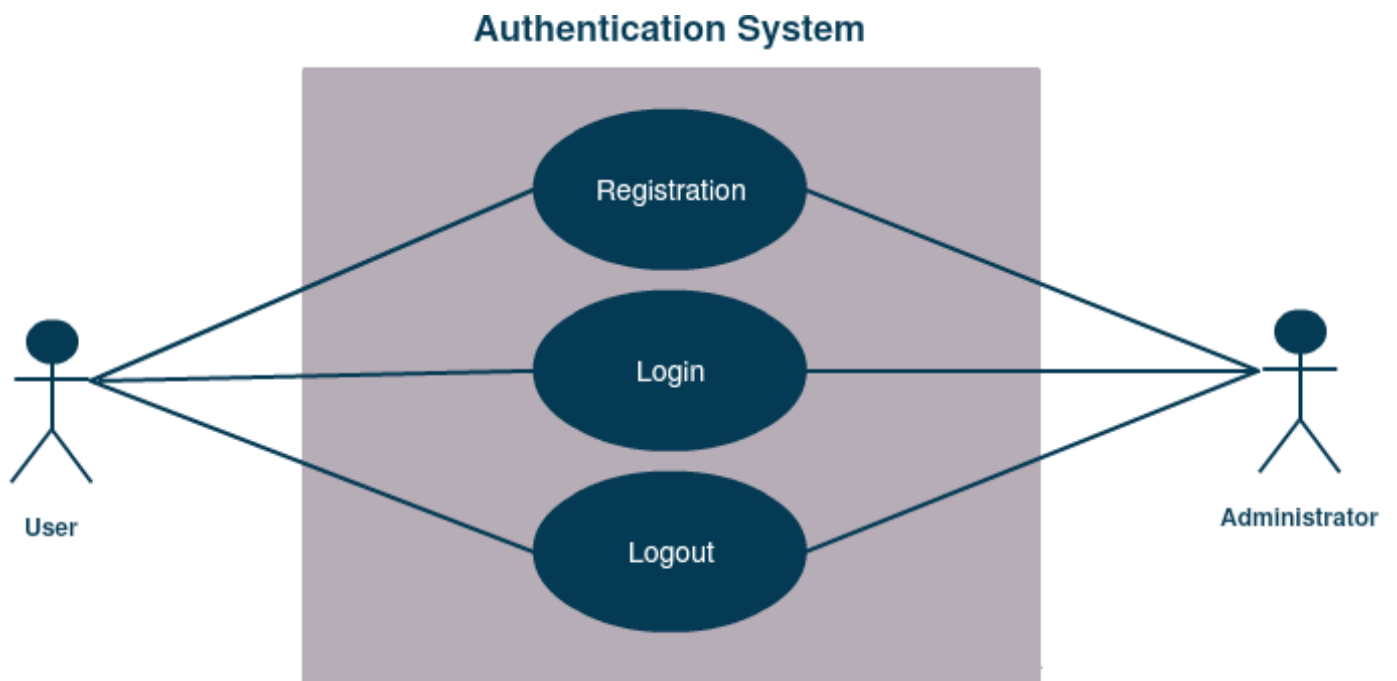


Figure 22:e Case Diagram of Authentication System

12. Contacts Form

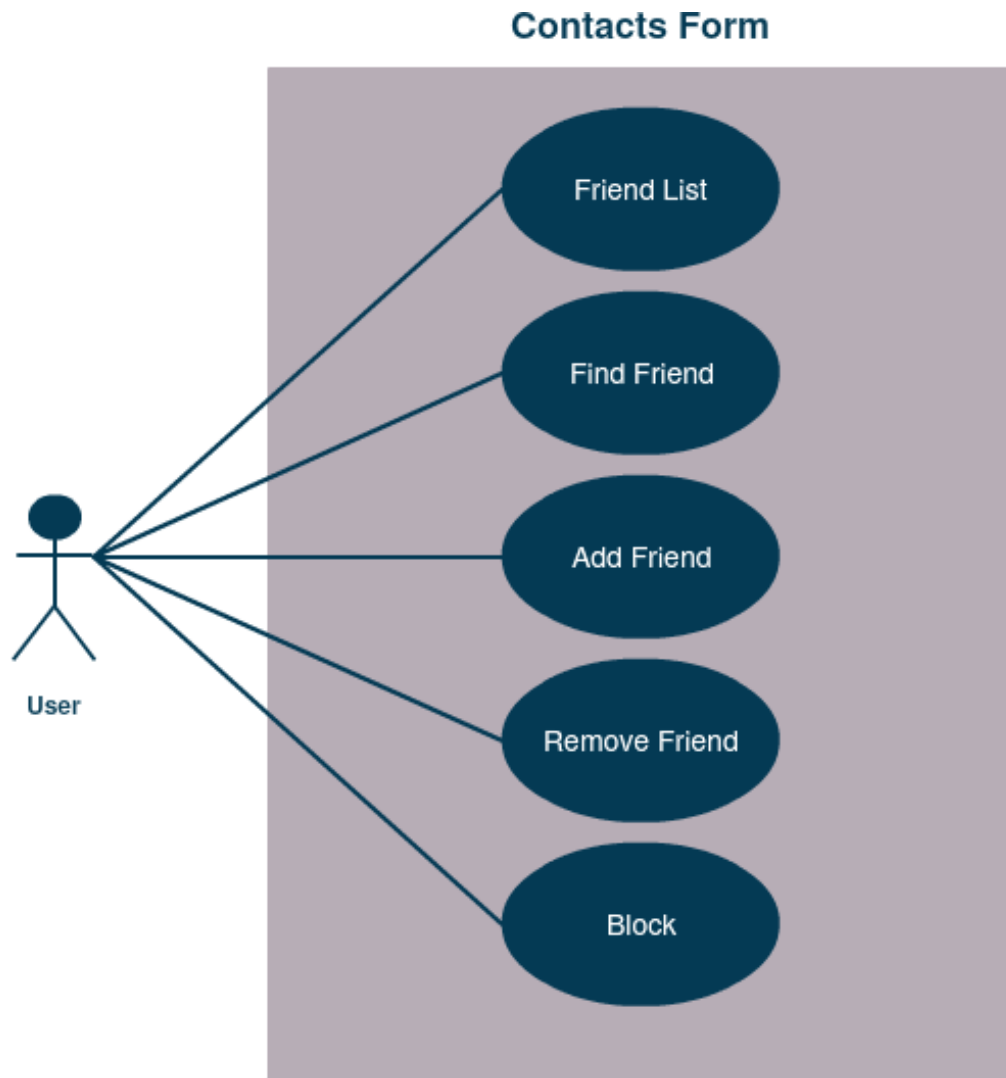


Figure 23: Use Case Diagram of Contacts Form

13.Chat Form

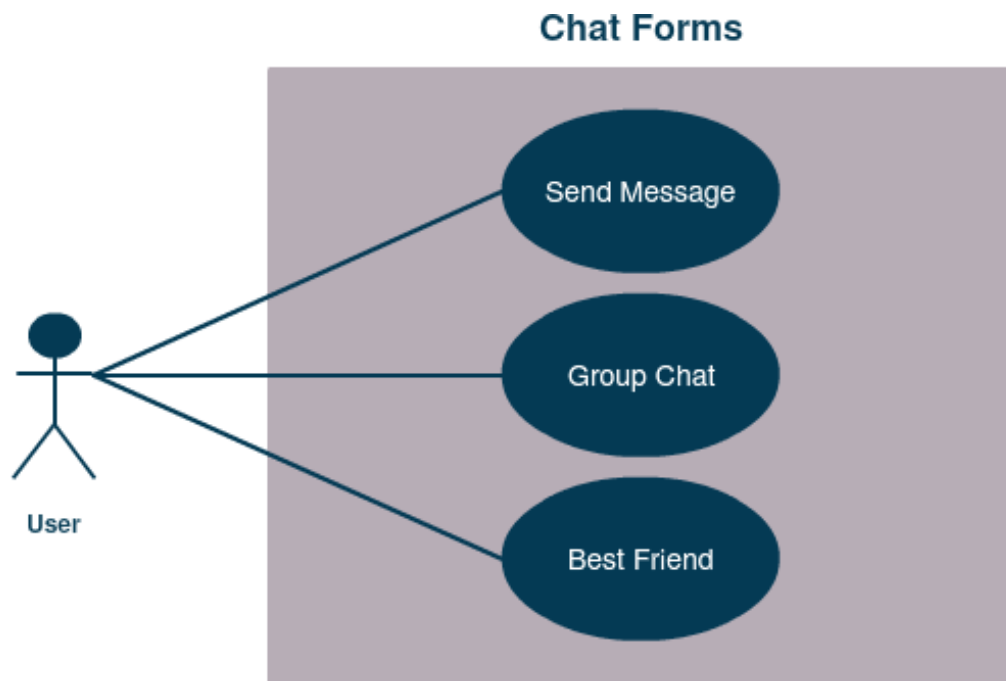


Figure 24: Use Case Diagram of Chat Form.

2. Activity Diagram

11. Contacts Form, Chat Form

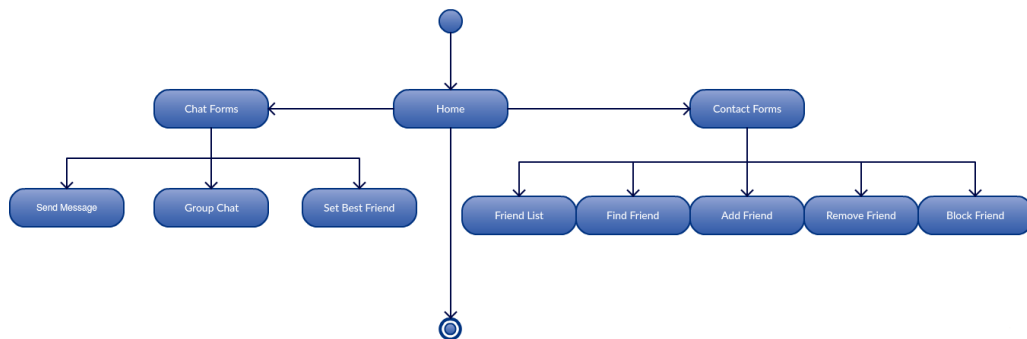


Figure 25: Activity Diagram of Contacts Form, Chat Form.

3. Entity Relationship Diagram

E-R Diagram of Chat Application

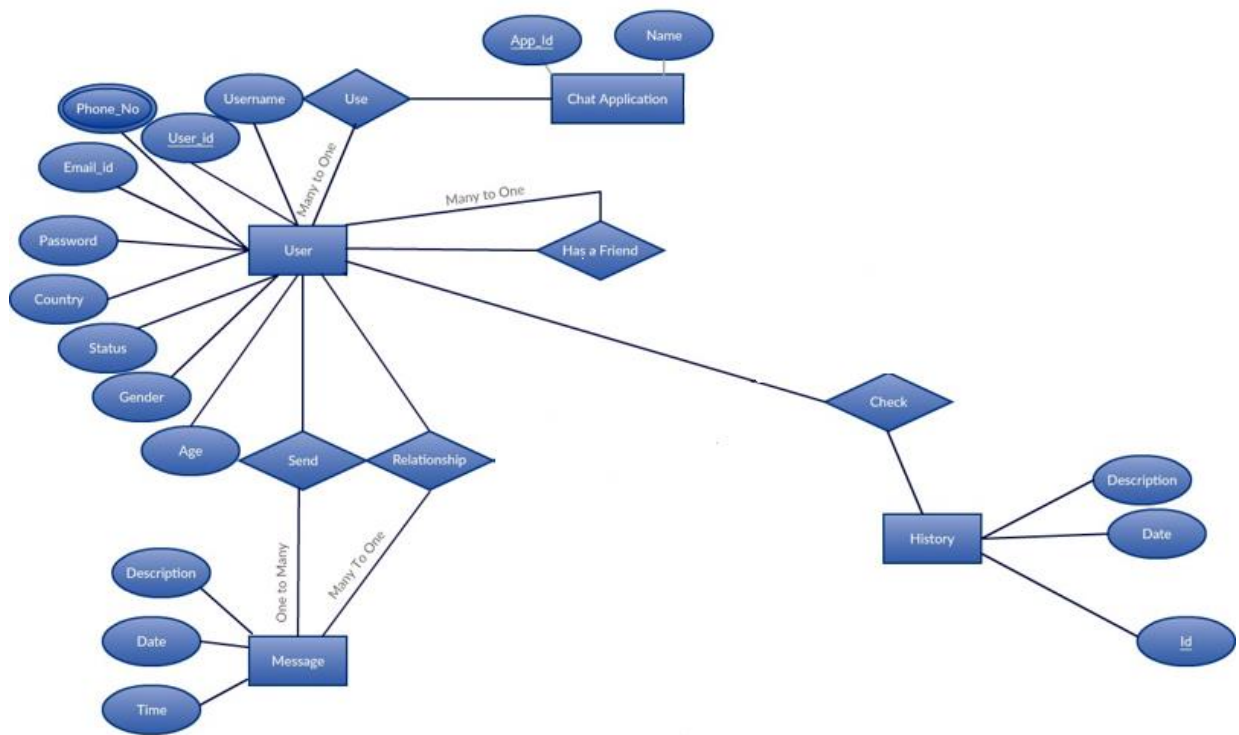


Figure 26: Entity Relationship Diagram of Chat Application.

Project Risk Management

Identification

Risk identification involves determining which risks or threats are likely to affect the project.

It involves the identification of risks or threats that may lead to project outputs being delayed or reduced, outlays being advanced or increased and/or output quality (fitness for purpose) being reduced or compromised.

For most large/complex projects, a number of high level risks should have been identified during the project initiation stage these should be used as the basis for a more thorough analysis of the risks facing the project.

One of the most difficult things is ensuring that all major risks are identified.

A useful way of identifying relevant risks is defining causal categories under which risks might be identified.

For example, corporate risks, business risks, project risks and infrastructure risks.

These can be broken down even further into categories such as environmental, economic, political, human, etc.

Another way is to categorise in terms of risks external to the project and those that are internal.

See the Project Management Risk Identification Tool for some useful prompts in identifying project risks.

The Australian Standard for Risk Management AS/NZS 4360: 2004 Appendix D refers to generic sources of risk.

The wording or articulation of each risk should follow a simple two-step approach:

1. Consider what might be a trigger event or threat (eg. poor quality materials causes costs to rise) several triggers may reveal the same inherent risk then.

2. Identify the risk use a newspaper headline style statement short, sharp and snappy (eg. budget blow out) then describe the nature of the risk and the impact on the project if the risk is not mitigated or managed (eg. project delayed or abandoned, expenditure to date wasted, outcomes not realised, government embarrassed etc).

Use the Risk Register (see Appendix A) to document the results. For large or complex projects it can be beneficial to use an outside facilitator to conduct a number of meetings or brainstorming sessions involving (as a minimum) the Project Manager, Project Team members, Steering Committee members and external key stakeholders.

Preparation may include an environmental scan, seeking views of key stakeholders etc.

For a small project, the Project Manager may develop the Risk Register perhaps with input from the Project Sponsor/Senior Manager and colleagues, or a small group of key stakeholders.

It is very easy to identify a range of risks that are outside the project and are actually risks to the business area during output delivery, transition or once operational mode has been established.

These are not project risks and should not be included in the Project Risk Register, but referred to the relevant Business Owner.

It may be appropriate to submit an Issues Paper to the Steering Committee recommending formal acceptance by the relevant Business Owner for ongoing monitoring and management of specific risks.

See the Project Management Fact Sheet: Developing a Risk Management Plan and the Risk Identification Tool for more information on how to undertake risk identification.

In this section specify

Risk identification process that we followed are Brainstorm, facilitated session, scan by Project Manager etc.

الفصل الرابع

تنفيذ النظام

1. User Manual

12.Registration for new Member

Open Chat Application & Click on Sign Up. Then This window will pop up.

Then You have to submit valid info to Successfully register.

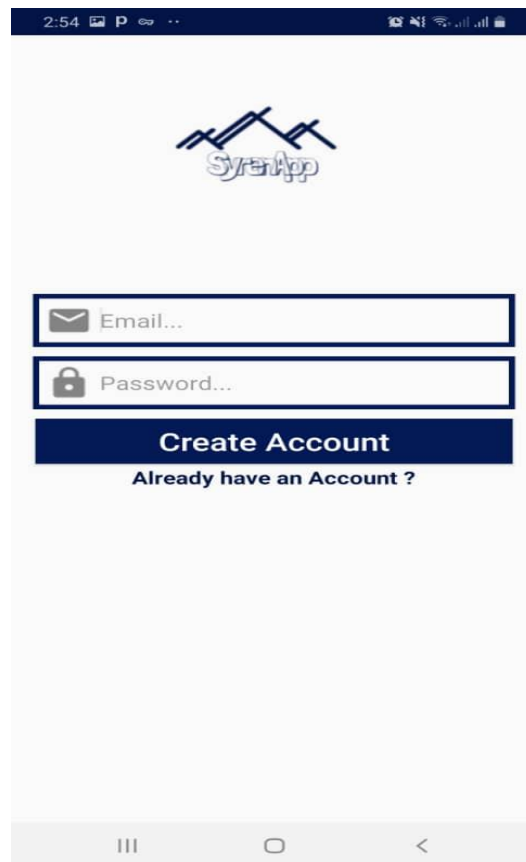
A screenshot of a mobile application interface for registration. At the top, there is a status bar with the time 2:54 and various icons. Below the status bar is a header with the SyrenApp logo, which consists of a stylized mountain range above the text "SyrenApp". The main content area contains two input fields: the first is labeled "Email..." with an envelope icon, and the second is labeled "Password..." with a lock icon. Below these fields is a blue button with the text "Create Account". Underneath the button is a link that says "Already have an Account ?". At the bottom of the screen is a navigation bar with three icons: a hamburger menu, a home icon, and a back arrow.

Figure 27: Registration for new Member.

13.Login Features

Open Chat App then click on Log In Button. Then Submit Valid Info to access your account.

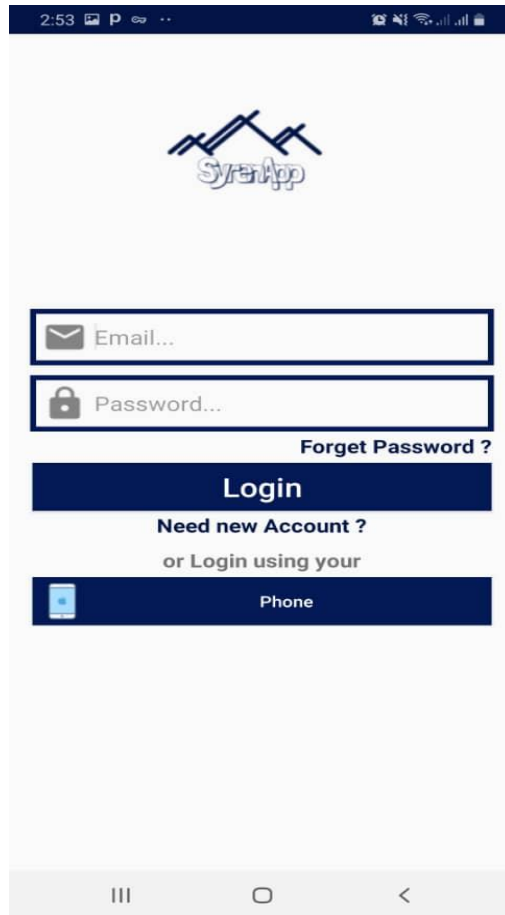


Figure 28: Login Features.

14.Private Chatting

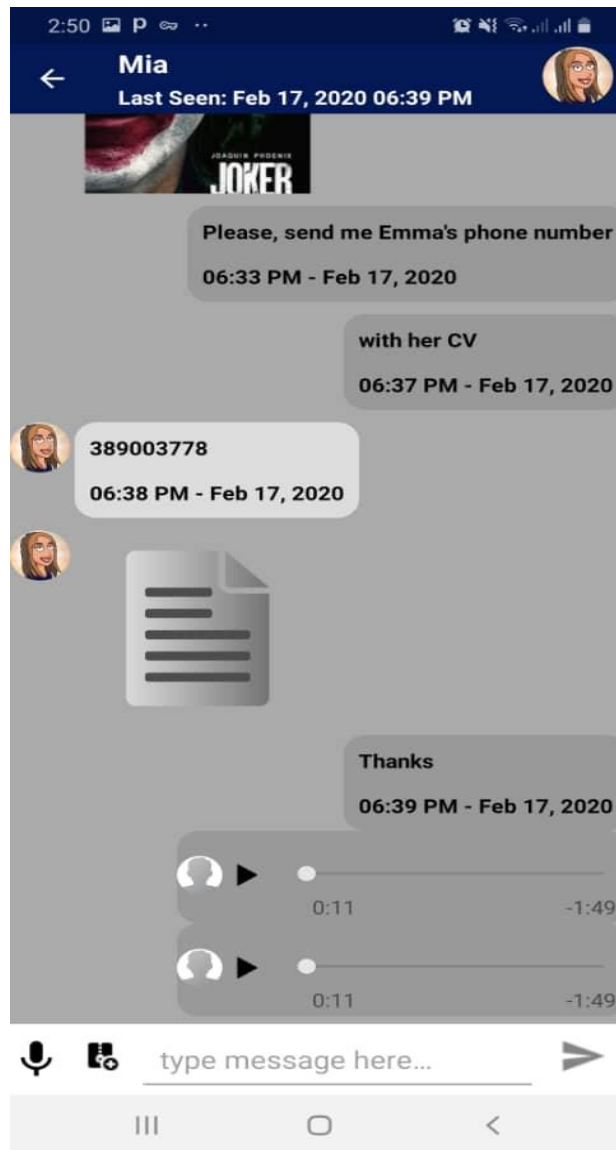


Figure 29: Private Chatting.

15.Adding Friend

Open chat app then click on more options then click on add friend. There you will be able to search for friend.

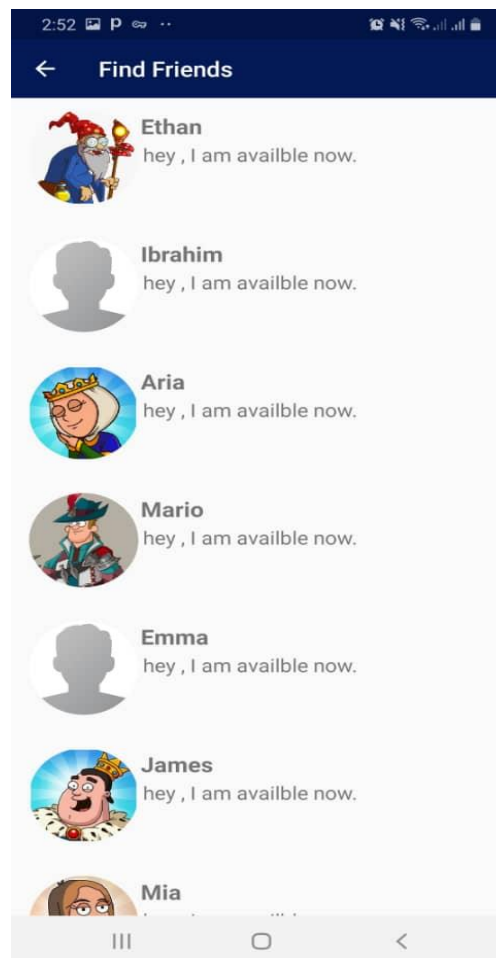


Figure 30: Adding Friend.

16.Chat Forms

After Login you will automatically redirected to Chat Forms

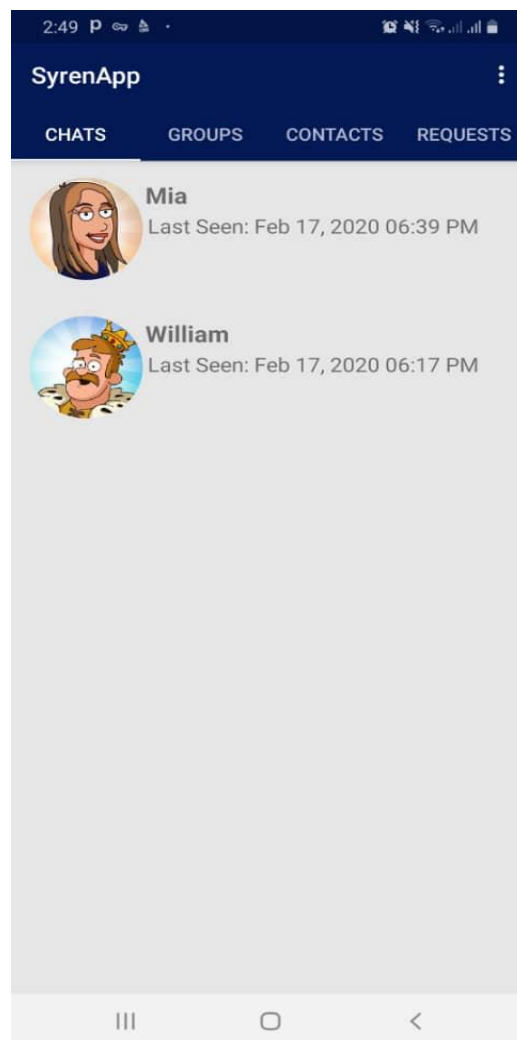


Figure 31: Chat Forms.

17. Block Friend

Go to setting Edit Friend List then You will see Block Button underneath the layout

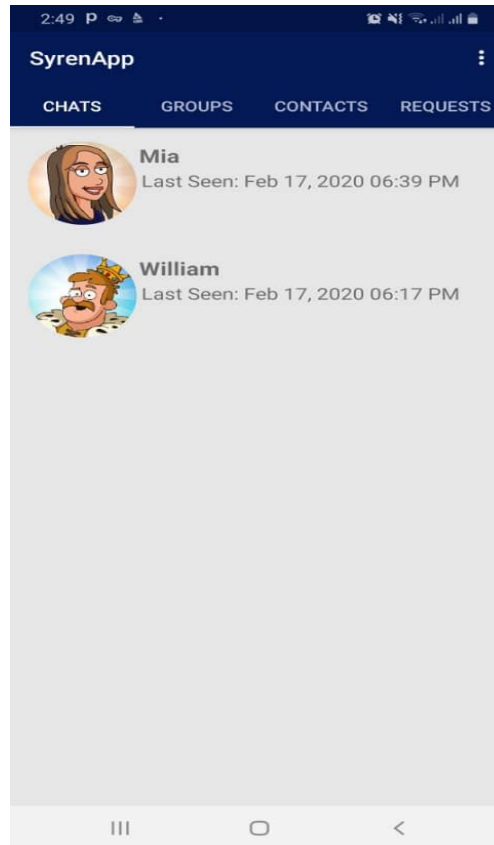


Figure 32:Block Friend.

18.Account Settings

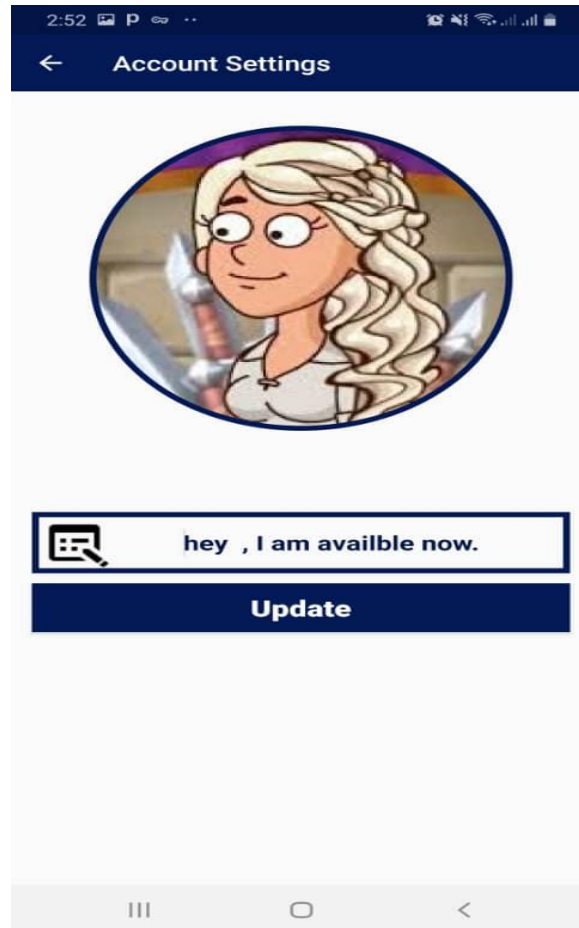


Figure 33: Account Settings.

1. MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.

It can still be used as a checksum to verify data integrity, but only against unintentional corruption.

It remains suitable for other noncryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

One basic requirement of any cryptographic hash function is that it should be computationally infeasible to find two distinct messages that hash to the same value. MD5 fails this requirement catastrophically; such collisions can be found in seconds on an ordinary home computer.

The weaknesses of MD5 have been exploited in the field, most infamously by the Flame malware in 2012.

The CMU Software Engineering Institute considers MD5 essentially "cryptographically broken and unsuitable for further use".

As of 2019, MD5 continues to be widely used, in spite of its well-documented weaknesses and deprecation by security experts.^[12]

11. History and cryptanalysis

MD5 is one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1992). When analytic work indicated that MD5's predecessor MD4 was likely to be insecure, Rivest designed MD5 in 1991 as a secure replacement. (Hans Dobbertin did indeed later find weaknesses in MD4.)

In 1993, Den Boer and Bosselaers gave an early, although limited, result of finding a "pseudo-collision" of the MD5 compression function; that is, two different initialization vectors that produce an identical digest.

In 1996, Dobbertin announced a collision of the compression function of MD5 (Dobbertin, 1996).

While this was not an attack on the full MD5 hash function, it was close enough for cryptographers to recommend switching to a replacement, such as SHA-1 or RIPEMD-160.

The size of the hash value (128 bits) is small enough to contemplate a birthday attack. MD5CRK was a distributed project started in March 2004 with the aim of demonstrating that MD5 is practically insecure by finding a collision using a birthday attack.

MD5CRK ended shortly after 17 August 2004, when collisions for the full MD5 were announced by Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu.

Their analytical attack was reported to take only one hour on an IBM p690 cluster.

On 1 March 2005, Arjen Lenstra, Xiaoyun Wang, and Benne de Weger demonstrated construction of two X.509 certificates with different public keys and the same MD5 hash value, a demonstrably practical collision.

The construction included private keys for both public keys. A few days later, Vlastimil Klima described an improved algorithm, able to construct MD5 collisions in a few hours on a single notebook computer.

On 18 March 2006, Klima published an algorithm that could find a collision within one minute on a single notebook computer, using a method he calls tunneling.

Various MD5-related RFC errata have been published. In 2009, the United States Cyber Command used an MD5 hash value of their mission statement as a part of their official emblem.

On 24 December 2010, Tao Xie and Dengguo Feng announced the first published single-block (512-bit) MD5 collision.

(Previous collision discoveries had relied on multi-block attacks.) For "security reasons", Xie and Feng did not disclose the new attack method.

They issued a challenge to the cryptographic community, offering a US\$10,000 reward to the first finder of a different 64-byte collision before 1 January 2013. Marc Stevens responded to the challenge and published colliding single-block messages as well as the construction algorithm and sources.

In 2011 an informational RFC 6151 was approved to update the security considerations in MD5[17] and HMAC-MD5.

12.Security

The security of the MD5 hash function is severely compromised. A collision attack exists that can find collisions within seconds on a computer with a 2.6 GHz Pentium 4 processor (complexity of $2^{24.1}$).

Further, there is also a chosen-prefix collision attack that can produce a collision for two inputs with specified prefixes within seconds, using off-the-shelf computing hardware (complexity 2^{39}). The ability to find collisions has been greatly aided by the use of off-the-shelf GPUs. On an NVIDIA GeForce 8400GS graphics processor, 16–18 million hashes per second can be computed.

An NVIDIA GeForce 8800 Ultra can calculate more than 200 million hashes per second.

These hash and collision attacks have been demonstrated in the public in various situations, including colliding document files and digital certificates. As of 2015, MD5 was demonstrated to be still quite widely used, most notably by security research and antivirus companies.

As of 2019, one quarter of widely used content management systems were reported to still use MD5 for password hashing.

13. Overview of security issues

In 1996, a flaw was found in the design of MD5.

While it was not deemed a fatal weakness at the time, cryptographers began recommending the use of other algorithms, such as SHA-1, which has since been found to be vulnerable as well.

In 2004 it was shown that MD5 is not collision-resistant.

As such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property for digital security.

Also in 2004 more serious flaws were discovered in MD5, making further use of the algorithm for security purposes questionable; specifically, a group of researchers described how to create a pair of files that share the same MD5 checksum.

Further advances were made in breaking MD5 in 2005, 2006, and 2007. In December 2008, a group of researchers used this technique to fake SSL certificate validity.

As of 2010, the CMU Software Engineering Institute considers MD5 "cryptographically broken and unsuitable for further use", and most U.S. government applications now require the SHA-2 family of hash functions.

In 2012, the Flame malware exploited the weaknesses in MD5 to fake a Microsoft digital signature.

14. Collision vulnerabilities

Further information: Collision attack

In 1996, collisions were found in the compression function of MD5, and Hans Dobbertin wrote in the RSA Laboratories technical newsletter, "The presented attack does not yet threaten practical applications of MD5, but it comes rather close ... in the future MD5 should no longer be implemented ... where a collision-resistant hash function is required."

In 2005, researchers were able to create pairs of PostScript documents and X.509 certificates with the same hash. Later that year, MD5's designer Ron Rivest wrote that "md5 and sha1 are both clearly broken (in terms of collision-resistance)".

On 30 December 2008, a group of researchers announced at the 25th Chaos Communication Congress how they had used MD5 collisions to create an intermediate certificate authority certificate that appeared to be legitimate when checked by its MD5 hash. The researchers used a cluster of Sony PlayStation 3 units at the EPFL in Lausanne, Switzerland to change a normal SSL certificate issued by RapidSSL into a working CA certificate for that issuer, which could then be used to create other certificates that would appear to be legitimate and issued by RapidSSL. VeriSign, the issuers of RapidSSL certificates, said they stopped issuing new certificates using MD5 as their checksum algorithm for RapidSSL once the vulnerability was announced.

Although Verisign declined to revoke existing certificates signed using MD5, their response was considered adequate by the authors of the exploit (Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger). Bruce Schneier wrote of the attack that "we already knew that MD5 is a broken hash function" and that "no one should be using MD5 anymore".

The SSL researchers wrote, "Our desired impact is that Certification Authorities will stop using MD5 in issuing new certificates. We also hope that use of MD5 in other applications will be reconsidered as well.

In 2012, according to Microsoft, the authors of the Flame malware used an MD5 collision to forge a Windows code-signing certificate.

MD5 uses the Merkle Damgård construction, so if two prefixes with the same hash can be constructed, a common suffix can be added to both to make the collision more likely to be accepted as valid data by the application using it.

Furthermore, current collision-finding techniques allow to specify an arbitrary prefix: an attacker can create two colliding files that both begin with the same content.

All the attacker needs to generate two colliding files is a template file with a 128-byte block of data, aligned on a 64-byte boundary that can be changed freely by the collision-finding algorithm. An example MD5 collision, with the two messages differing in 6 bits, is:

```
d131dd02c5e6eec4 693d9a0698aff95c 2fcab58712467eab 4004583eb8fb7f89
55ad340609f4b302 83e488832571415a 085125e8f7cdc99f d91dbdf280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e2b487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080a80d1e c69821bcb6a88393 96f9652b6ff72a70
d131dd02c5e6eec4 693d9a0698aff95c 2fcab50712467eab 4004583eb8fb7f89
55ad340609f4b302 83e4888325f1415a 085125e8f7cdc99f d91dbd7280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e23487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080280d1e c69821bcb6a88393 96f965ab6ff72a70
```

Both produce the MD5 hash 79054025255fb1a26e4bc422aef54eb4.[41] The difference between the two samples is that the leading bit in each nibble has been flipped. For example, the 20th byte (offset 0x13) in the top sample, 0x87, is 10000111 in binary.

The leading bit in the byte (also the leading bit in the first nibble) is flipped to make 00000111, which is 0x07, as shown in the lower sample.

Later it was also found to be possible to construct collisions between two files with separately chosen prefixes. This technique was used in the creation of the rogue CA certificate in 2008. A new variant of parallelized collision searching using MPI was proposed by Anton Kuznetsov in 2014, which allowed to find a collision in 11 hours on a computing cluster.

15.Preimage vulnerability

In April 2009, an attack against MD5 was published that breaks MD5's preimage resistance. This attack is only theoretical, with a computational complexity of $2^{123.4}$ for full preimage.

16.Applications

MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact.

For example, file servers often provide a pre-computed MD5 (known as md5sum) checksum for the files, so that a user can compare the checksum of the downloaded file to it.

Most unix-based operating systems include MD5 sum utilities in their distribution packages; Windows users may use the included PowerShell function "Get-FileHash", install a Microsoft utility, or use third-party applications.

Android ROMs also use this type of checksum.

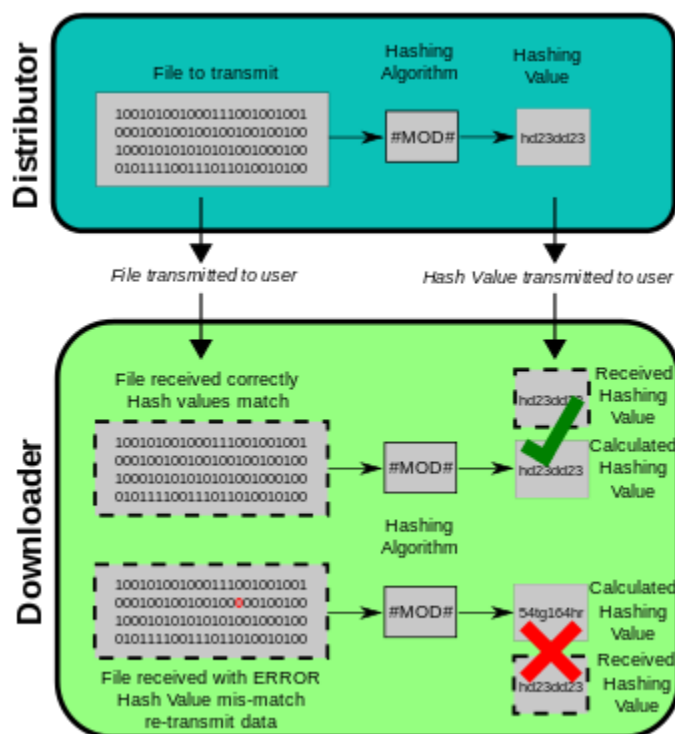


Figure 34: MD5 digests .

As it is easy to generate MD5 collisions, it is possible for the person who created the file to create a second file with the same checksum, so this technique cannot protect against some forms of malicious tampering.

In some cases, the checksum cannot be trusted (for example, if it was obtained over the same channel as the downloaded file), in which case MD5 can only provide error-checking functionality: it will recognize a corrupt or incomplete download, which becomes more likely when downloading larger files.

Historically, MD5 has been used to store a one-way hash of a password, often with key stretching.

NIST does not include MD5 in their list of recommended hashes for password storage.

MD5 is also used in the field of electronic discovery, in order to provide a unique identifier for each document that is exchanged during the legal discovery process.

This method can be used to replace the Bates stamp numbering system that has been used for decades during the exchange of paper documents.

As above, this usage should be discouraged due to the ease of collision attacks.

17. Algorithm

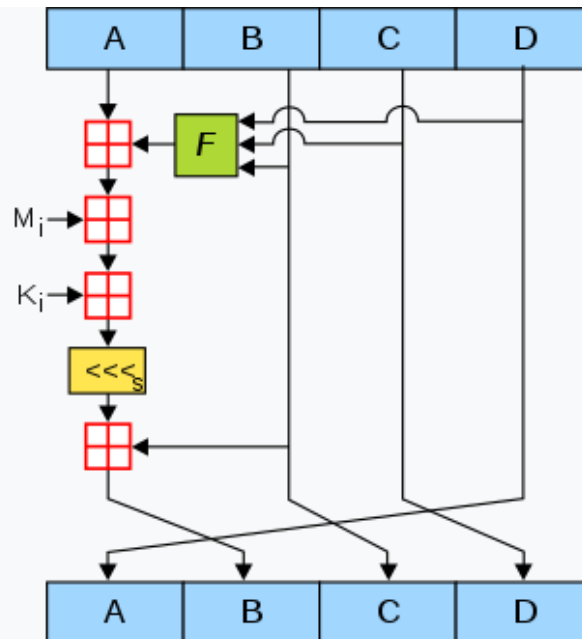


Figure 35: MD5 Algorithm.

One MD5 operation.

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations.

F is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. $\lll s$ denotes a left bit rotation by s places; s varies for each

operation. \boxplus denotes addition modulo 232.

MD5 processes a variable-length message into a fixed-length output of 128 bits.

The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512.

The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264.^[12]

الفصل الخامس الخاتمة والمراجع

1. Conclusion

There is always a room for improvements in any apps.

Right now we are just dealing with text communication.

There are several android apps which serve similar purpose as this project, but these apps were rather difficult to use and provide confusing interfaces.

A positive first impression is essential in human relationship as well as in human computer interaction.

This project hopes to develop a chat service Android app with high quality user interface.

In future we may be extended to include features such as:

- 1.VideoMessag
- e 2.Audio Call
- 3.Video Call
- 4.Group Call

Troubleshooting

Problem	Cause	Solution
Cannot Registrar	1. The Required Information field was not filled out entirely. 2. User name Invalid or Already Exists. 3. Password too short.	Enter all information in the Required Information field. Select a user name that is unique, something besides your name. Choose a password at least
Can't Add Friend	Maybe your device Getting wrong reference	Restart or reinstall chat app

2. References

1. Number of monthly active WhatsApp users worldwide from April 2013 to February 2016 (in millions). Available from: <http://www.statista.com/statistics/260819/number-of-monthly-active-WhatsApp-users/>
2. Available from: <https://www.theguardian.com/technology/short-cuts/2012/dec/04/WhatsApp-new-text-messaging>
3. Available from: <http://www.ft.com/cms/s/2/30fd99a2-0c60-11e1-88c6-00144feabdc0.html>
4. Available from: <http://www.speakingtree.in/blog/WhatsApp-addictive-dangerous-read-how-to-overcome>
5. What Makes Smartphone Users Satisfied with the Mobile Instant Messenger? Social Presence, Flow, and Self-disclosure Seongwon Park¹, Kwangsu Cho¹ and Bong Gyou Lee International Journal of Multimedia and Ubiquitous Engineering. 2014; 9(11):315–24.
6. Jang YJ, Kim CW. The Evolution of Smartphone Market and the Effect by Android. Journal of KIIE. 2010; 28(5):48–56.
7. Privacy Implications of Presence Sharing in Mobile Messaging Applications Andreas Buchenscheit,¹ Bastian Könings,² Andreas Neubert,³ Florian Schaub,⁴ Matthias Schneider,³ Frank Kargl
8. The Impact of WhatsApp Messenger Usage on Students Performance in Tertiary Institutions in Ghana Johnson Yeboah (Lecturer)*, George Dominic Ewur (Lecturer) Journal of Education and Practice. Available from: www.iiste.org. 2014; 5(6). ISSN 2222- 1735 (Paper) ISSN 2222-288X (Online) Vol.5, No.6, 2014
9. WhatsApp: A Trend Setter in Mobile Communication among Chennai Youth Ms. Jisha K1, Dr. Jebakumar , IOSR Journal Of Humanities And Social Science (IOSR-JHSS). 2014 Sep; 19(9), VII:01-06 . e-ISSN: 2279-0837, p-ISSN: 2279-0845. Available from: www.iosrjournals.org
10. WhatsApp buyout on social media Strategist Team. 2014 Mar 3. Available from: http://www.business-standard.com/article/management/impact-of-WhatsApp-buyout-on-social-media-114030200632_1.html
11. <https://telegram.org/faq>
12. <https://en.wikipedia.org/wiki/MD5>