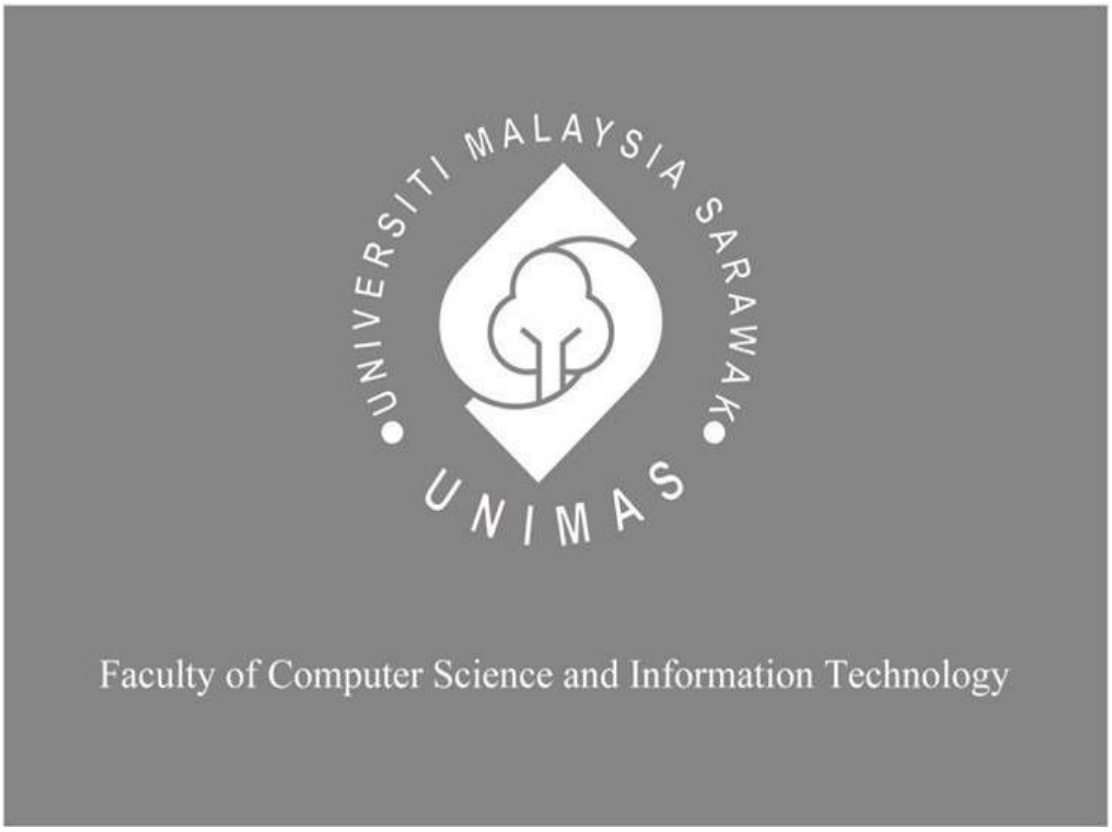

SCYChat: Privacy Enhanced Messaging App Using Face and Fingerprint Recognition

TEO YU CHUAN

Bachelor of Computer Science with Honors

(Software Engineering)

2020

SCYChat: Privacy Enhanced Messaging App Using Face and Fingerprint Recognition

TEO YU CHUAN

This project is submitted in partial fulfillment of

the requirements for the degree of Bachelor of

Computer Science with Honors

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK 2020

SCYChat: App Pemesejan Privasi yang Dipertingkat Menggunakan Pengenalan Wajah dan Cap jari

TEO YU CHUAN

Projek ini merupakan salah satu keperluan

untuk Ijazah Sarjana Muda Sains Komputer

dengan kepujian

Fakulti Sains Komputer dan Teknologi Maklumat

UNIVERSITI MALAYSIA SARAWAK 2020

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE SCYChat: Privacy Enhanced Messaging App Using Face and Fingerprint Recognition

ACADEMIC SESSION: 2019/2020

TEO YU CHUAN
(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

Teo
(AUTHOR'S SIGNATURE)

Permanent Address
A5, Taman Bersatu Maju
08100 Bedong,
Kedah

Date: 1/8/2020

Validated by

(SUPERVISOR'S SIGNATURE)
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak

Date: 12 August 2020

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

DECLARATION

I hereby declare that the project report entitled "SCYChat: Privacy Enhanced Messaging App with Face and Fingerprint Recognition" submitted to Dr. Lau Sei Ping which is my supervisor and Associate Professor Dr. Jane Labadin which is my examiner. I assure the project is my original work and did not copy from other people or sources except the cited sources.

Teo
……
TEO YU CHUAN

5 July 2020
……

ACKNOWLEDGMENT

First, I would like to express thanks to all those who have contributed towards the completion of my final year project. The first person I would like to thanks is my supervisor, Dr. Lau Sei Ping. He is always helping me in discussion and give me some comments about the project. The advice from my supervisor is very valuable and helpful for me. He is very patient to help me and give some ideas to the system. The project can be proceeding smoothly because of my supervisor's support.

Besides, I also would like to thanks the coordinator of FYP 2020, Professor Dr. Wang Yin Chai. He put his efforts and guidance to FYP students for the flow and requirements of the final year project. Another person that I want to thanks is my examiner, Associate Professor Dr. Jane Labadin. She gives some feedbacks about my project to improve my project weaknesses.

Finally, I also need to thanks, my family and my friends. With their support, I have the confidence to complete this project.

ABSTRACT

Messaging applications are very famous in this world. Most of the time, people will choose messaging applications to send a message or call because it will not charge your phone fee. It just used your data from the internet plan to work. In the messaging applications, there is much information that may contain privacy or confidential information during the conversation. To protect this information, the SCYChat application is developed. The development of the project will be based on the user requirement.

The user of the SCYChat application can use it as a normal messaging application such as send messages and files. The additional feature is the face and fingerprint recognition. The application can detect the current user are the owner itself or other. Besides, the application also can automatically lock the phone when the user did not look to the phone. The application will give the user high-level security of a messaging application.

ABSTRAK

Aplikasi pemesejan sangat terkenal dalam dunia ini. Kebanyakan orang akan pilih aplikasi pemesejan untuk menghantar mesej atau buat panggilan kerana aplikasi ini hanya guna data dari pelan internet dan tidak akan kena caj bagi bayaran telefon. Dalam aplikasi pemesejan, terdapat banyak maklumat yang mungkin mengandungi privasi atau maklumat rahsia semasa perbualan. Untuk melindungi maklumat ini, aplikasi SCYChat dibangunkan. Pembangunan projek akan berdasarkan keperluan pengguna.

Pengguna aplikasi SCYChat dapat digunakan sebagai aplikasi pesanan biasa seperti menghantar mesej dan fail. Ciri tambahan adalah pengenalan wajah dan cap jari. Aplikasi ini dapat mengesan pengguna semasa adalah pemilik itu sendiri atau yang lain. Selain itu, aplikasi juga boleh mengunci telefon secara automatik apabila pengguna tidak melihat ke telefon. Aplikasi ini akan memberi pengguna aplikasi keselamatan mesej tahap tinggi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF GRAPHS

LIST OF FIGURES

Chapter 1: Introduction

1.1 Background

Messaging application is very popular to use in our daily life. A lot of people using messaging applications such as WhatsApp or WeChat to communicate with their friends or family. It can help people communicate with each other even they are not in the same location or country. Almost all communication applications have similar designs and interface to make the user easier to use. There is some similar functionality for communication applications. The first function can text messaging with each other without limit any distance and share files, photos, or video to another. This function will help us to save time when transmitting a message or share file, photo, or video to another. The second function can make a video or voice call to another person. It can help us reduce travel time and cost because we do not need to pay the traveling fee to the person's place. The third function is provided security to information. Most messaging applications apply the end-to-end encryption method to prevent the hacker get the information from the database. The communication applications also have their risk because all the information that store in your phone and web may be hacked or lost data. Nowadays, more and more people using the communication application to discuss their work and also share the confidential document. Some of the messaging application does not have a feature to protect these kinds of document. So, the messaging application still needs to improve based on their security.

1.2 Problem Statement

Even though messaging applications help us to communicate with each other. But some people also want to make private chat or protect their information. If the people forgot to lock or turn off their phones after running the application, the message may be seen by other people. Besides, some of the private and confidential information which is intended or exclusively for the group only maybe accidentally shared by members of the communication group. The user who used the device that did not implement the lock application function is not completely safe. Since the user may forget to close the application that being used and the screen still active. In this case, the content of the application will be read or even illegally used by others. Moreover, the device exposed to other people may cause a leak of information likes the information about the owner, the information of conversation, or the account for social media may be hacked.

1.3 Objectives

i. To detect if a user is using the application.

ii. To lock down the application automatically if the user is not using the application.

iii. To authenticate the user before executing the application.

1.4 Scope

i. This application will only support the mobile device with Android OS.

ii. The targeted users of this application are for people who have a smartphone.

iii. This application is for demonstration and not as complete chat application.

iv. The targeted device must have an embedded fingerprint feature.

1.5 Methodology

A suitable methodology can ensure efficiency and achieve success for a project. Rapid Application Development (RAD) model is not suitable for this project because require resources with high business knowledge are available and there is a need to produce the system in a short period (2-3 months). Agile software development is aimed at faster implementation of any project. It provides a cycle between phases so it was available to make changes for the previous phase. So, it not suitable for this project because this project needs to step by step to process each phase. In this project, the waterfall model is used because of no ambiguous requirements. Besides, the waterfall model can record processes and result in a project. It can be easy to make documentation for this project. The benefit of this methodology is easy to understand and functional saves a significant amount of time and allows for easy testing and analysis (Korkishko, 2017). This model contains several phases in the development and these phases need to ensure the previous phase is completed then the phase-only can continue. Figure 1 shows the waterfall model with several phases.

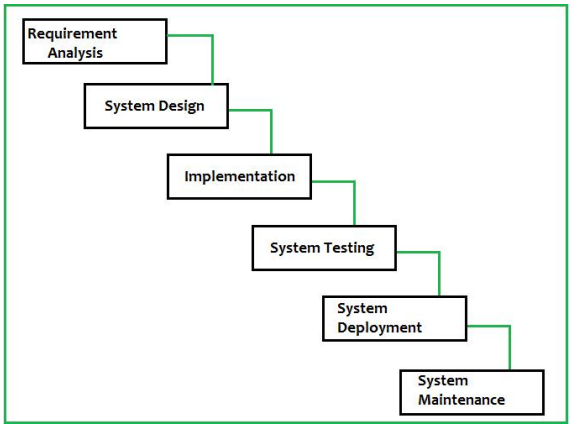

Figure 1.1: Waterfall Model (ADMIN, 2015)

In the requirement analysis phase, the system analysis and functional analysis of the system will be discussed. The system analysis includes hardware, software, and user requirements while functional analysis will be referring to user requirements. This project is to improve the current messaging application security to the highest level. The problem for the messaging applications is mostly applied end-to-end encryption to secure the information for the back end side but how about the front end side to secure our information is our main purpose to solve it. The front end side can be defined as the interface of the applications. The interface will make the user easier to understand, using it, and also convenient. For the interface of messaging applications, it will always show the message straight to the user when the user is accessing it. If the user is not the user itself, the information may be seen by others and used for illegal things. The user of confidential files, indecent photos, or the message contains any password for social media account is exposed to others. It may make people involve in cyberbully, social media account being stolen, and even blackmailed. Besides, the existing application will be reviewed to understand the functionality and design. This existing application will be enhanced by doing this project and make the people can highly protect the information in messaging applications.

In the system design phase, the design of the system will be determined. There are five different views of design will be shown which are system architecture design, use case diagram, activity diagram, class diagram, and user interface design. Since the messaging application already exists so this project will refer to the existing application design and make some changes. Because many people are using a messaging application at this time so to make people more convenient and easier to

use it. That means the user interface (UI) design of the system will slightly different from the existing system design.

In the implementation phase, the android studio will be used to create an app. The Cloud Firebase will be used to temporarily store the data from the user and transfer it to another user. Implement all the functions during the requirement analysis phase to the application.

After the implementation phase, the system testing phase will proceed. In the system testing phase, the proposed application will be tested by using test cases and make sure all the functions can work as usual. The next phase is system deployment, the application will be present for my supervisor and examiner. The final phase is system maintenance, this project is done for final year project so there will be not available for maintenance.

1.6 Significance of project

The purpose of creating a SCYChat application is to protect the user information when the user is neglected. The application will be locked when the user is not facing its device. It means the information between conversations will never be exposed and safe even the device still active.

1.7 Expected Outcome

A prototype system is created which is the SCYChat application. Users can relieve to use this application to communicate with each other without scare the information exposed.

1.8 Project Report Outline

Chapter 2 reviews the existing messaging application to compare its functionality and security level. Several existing messaging applications such as WhatsApp, WeChat, and Telegram are being chosen for this project. Besides, the history of WhatsApp, WeChat, and Telegram will be explained.

In chapter 3, the type of software development for SCYChat will be explained. The design for the SCYChat application will refer to other applications to make another user easier to use. Besides, the functional, and software requirements also will be discussing in this chapter.

In chapter 4, the application will start to develop and record the details for each phase. The functionality of the application will be tested. If not fulfill the requirement, then we need to fix it before the system deployment phase.

The last chapter summarizes all the process that implements for this project and provide evidence for this project work on the future. Even the failures that occur in this project also can be referred to and improve it in the future.

Chapter 2: Literature Review

2.1 Introduction

This chapter will discuss the literature that will be review during our final year project. In the project, fingerprint, face recognition, and the android studio will be used to develop the application. Then, the background of fingerprint, face recognition, and the android studio is being determined. Besides, several similar applications will be making a comparison between them.

2.2 Review of similar applications

There are several existing applications will be reviewed during this project. The several applications are SMS, Skype, WhatsApp, and Telegram. These four applications are famous to use as communication applications.

2.2.1 SMS

Figure 2.1: Interface when received SMS

SMS also is known as a short message service. It is a method of communication between a cellular phone. This text messaging application will be a charge to your phone when sending a message to another user. “On December 3, 1992, engineer Neil Papworth sent the first SMS message to Richard Jarvis of Vodafone. It

simply read "Merry Christmas," and Jarvis had no way of replying" (O'Mahony, J, 2012). After this idea was born, some companies started to implement this function in their device. In 1993, Nokia was the first handset manufacturer whose total GSM phone line supported the user-sending of SMS text messages (Erickson, C, 2012). Even though people can use SMS text messages but it still has a critical problem. The problem is people must use the same network to send text messages to each other. This problem was solved in 1999, it increases the usefulness of SMS.

Before the instant messaging (IM) technology rise, SMS is very famous to use for text messages between friends or family. Some commerce did not want to use SMS because SMS is insecure. Message from SMS can be easily intercepted and read for malicious purposes. To overcome this problem, secure SMS technology is created which provided end-to-end encryption within commerce and their mobile application. Nowadays, SMS already become a permanent application for all android based mobile devices.

2.2.2 Skype

Figure 2.2: Skype

Skype is the one famous for telecommunication applications. It supports desktop, mobile, tablet, Xbox, and Amazon Echo Devices. Skype founded in 2003 and headquartered in Luxembourg, Skype is a division of Microsoft Corporation. Skype is for connecting with people either one-to-one or group conversation. It can be messaging, HD voice, and video call with another user or group. All information

between skype itself is encrypted to avoid malicious users. Skype also has a new feature which is screen sharing and private conversation. Screen Sharing is available in Skype version 4.1 which launched in 2009. While the private conversation is only available in the latest version of Skype for Windows, Mac, Linux, Web, Windows 10 (version 14), iOS, and Android (6.0+).

2.2.3 WhatsApp

Figure 2.3: WhatsApp

WhatsApp was launched in 2009 and the developers are Jan Koum and Brian Acton who had previously spent 20 years combined at Yahoo. They also found the iOS developer, Igor Solomennikov to help in the development. WhatsApp using a phone number to logging in, it will be more convenient to register and use it. In 2013, WhatsApp already has 200 million users and the staff also increased to 50. After WhatsApp become popular, Facebook uses $19 billion to buy it in February 2014. WhatsApp applies end-to-end encryption to protect the user's information.

2.2.4 Telegram

Figure 2.4: Telegram

Telegram is a cloud-based instant messaging and voice over IP service. Telegram founded on August 14, 2013, and support for Android, iOS, Windows Phone, Windows NT, macOS, and Linux. Users can send a message, photo, audio, video, stickers, and file to another by using the internet. In March 2018, Telegram achieved 200 million users per month. In August 2019, 365 million lifetime downloads of Telegram. Telegram is targeting 1 billion users by 2022. All Telegram message is encrypted. Telegram uses two layers of secure encryption for cloud chats and secret chats. Cloud chats also known as private or group chats are used Server-Client encryption while secret chats use client-client encryption. All types of information are encrypted in the same way. Telegram also open their source code, protocol, and API for everyone.

2.3 Comparisons Table

Table 2.1: Comparison between SMS, Skype, WhatsApp, and Telegram.

Function	SMS	Skype	WhatsApp	Telegram
Sending message	Yes	Yes	Yes	Yes
Sending audio	No	Yes	Yes	Yes
Sending video	No	Yes	Yes	Yes
Sending file	No	Yes	Yes	Yes
Information encrypted	No	Yes	Yes	Yes

Private chat	Yes	Yes	Yes	Yes
Group chat	No	Yes	Yes	Yes
Secret chat	No	Yes	No	Yes
Secret Group chat	No	No	No	No
Sticker	No	Yes	Yes	Yes
Two layers of encryption	No	No	No	Yes
Fingerprint recognition	No	No	Yes	No
Face recognition	No	No	No	No

In table 2.1, the SMS application can only provide sending a message and create private chat functions. It is because the SMS application is the first generation of the text messaging application. SMS only can send text between handphones. So, there is no way to use SMS to send videos, files, etc. Skype and WhatsApp are almost similar to all the functions provided. Skype has a secret chat function but WhatsApp does not have while WhatsApp has fingerprint recognition but Skype does not have. The Telegram is the highest number of functions provided according to the table above. Telegram does not have secret group chat and face recognition functions but it provided two layers of encryption. Telegram applies two layers of encryption to make their data more secure. The functions on the table above only refer based on Android-based mobile devices. After compared between these applications, I found that Telegram is more functionality than SMS, Skype, and WhatsApp. Besides, Telegram is a higher security level compare to SMS, Skype, and WhatsApp. The proposed system will focus on the functions of face and fingerprint recognition shown in the table above.

2.4 Fingerprint Recognition

Figure 2.5: Fingerprint

Fingerprints defined as a mark made on a surface by human fingertips and it can use for identifying individuals. The pattern of a fingerprint is different for a different person. "There's a one in 64 billion chance that your fingerprint will match up exactly with someone else's. Fingerprints are even more unique than DNA, the genetic material in each of our cells. Although identical twins can share the same DNA -- or at least most of it -- they can't have the same fingerprints." (Watson, S, 2008). Fingerprint become famous in 1892 because Inspector Eduardo Alvarez used fingerprint identification to criminal case and success to identify Francisca Rojas, a woman who murdered her two sons and cut her own throat in an attempt to place blame on another. Besides, Sir Francis Galton published his book, "Finger Prints" and the book includes the first published classification system for fingerprints.

In 1924, the Federal Bureau of Investigation (FBI) was established to provide one central repository of fingerprints. The purpose was to provide a central repository of criminal identification data for law enforcement agencies throughout the Nation. A