ChatHit Mobile Application Achieving End-to-End Encryption

Author: Hasna M R N

Supervisor: Dr. Lakmal Rupasinghe

Reg-no.: MS19801100

Assignment 2 of IT 5090 Research Methodology on Research Proposal,
is submitted as a partial requirement of the module

M.Sc. in IT specializing in Cyber Security

Sri Lanka Institute of Information Technology

20 April 2020

Contents

1. Summary

Working title: ChatHit Mobile Application Achieving End to End Encryption
*T*he main goal of this project is to develop a secure communication mobile application/ chat application which is compatible with Android smart mobile phones as it will help to engage in chat between groups or individual calls or messages and helps to manage communication system among friends, employees, family and customers in a secure method which can prevent from information theft while transferring the messages or before the message was read.

2. Introduction

escalation of mobile chat application is due to the fascination for mobile technology which plays several roles such as intensified engagement, continual possession of the user and adaptation for mobile devices have innovated many chat applications as 70 percent of the total visits on top digital news websites in this digital era [6]. Chat applications are being transformed into vital merchandising and buying channels along with artificial intelligence as these applications have become the current trend of communication which helps to communicate in a reliable and cost effective manner [6].

2.1 Background

The modern era of communication technology demands instant, fast and reliable communication methods as mobile phones and other smart devices play a major role in human life. The increase use of mobile applications is the reason behind the expanding needs of mobile systems. The online instant message applications helps the users transfer messages over the web which mandates an internet connection in order to exchange messages from one device to another device [2]. Applications such as WhatsApp, Viber, and Messenger etc. have overtaken the traditional SMS services as these platforms provide instant messaging services for a cheaper cost to the users.

2.2 Significance of the study

A secure chatting application - ChatHit Mobile Application achieving an End-to-End encryption for smart phones which has Android platforms is expected to be implemented which could provide the ultimate security of data transfer via communication channels as a secure network channel with proper encryption mechanisms for exchange of messages have become vital during communication due to the increase in hacking and information theft every day by malicious intruders who are eagerly waiting to access personal information and transferred messages [3].

3. Problem definition and research questions

The evolution of devices have made day to day work convenient and smart, these devices have become vulnerable and exposed to weaknesses as they are connected through networks and inter connectivity for communication [3]. Due to the increase use of different instant messaging platforms, security and privacy have become a major concern [2]. Even though the introduced chat applications provide a certain level of security and privacy, these applications doesn't focus on End-to-End (E2E) security and privacy to the users [3].

3.1 Problem definition

Privacy and security concerns while developing or using a mobile application has become vital due to the escalation of online information theft and phishing attacks by malicious intruders. The major service available in mobile chat on platform such as Android is pondered as initially, WhatsApp messaging service is its primary focus than privacy and the server doesn't store any messages from WhatsApp, where the client device stores its chat history [5]. SSL is used as a connector between the server and client application. SSL is in secured as WhatsApp has the access to attack. The client messages between the sender and receiver has no end to end for securement which causes the server to access the message exchanged. By 2016, "WhatsApp" succeeded in implementing the end to end security which protects the messages from hacking while transferring or reading [5].

3.2 Research problems

- What encryption mechanisms could be used to secure the entire chat application?
- What kind of encryption could be used to achieve the end to end security feature?
- By which method can the database containing with messages be encrypted?
- How could the messages be secured while transferring from one device to another?

4. Theoretical framework

4.1 Requirement Analysis

The scope of the project and the initial guidelines required for the project are understood and doubts on the project planning and technical aspects are clarified. Technical and user interface along with the software requirements specification documents are finalized.

4.2 User Interface Analysis and Design

The application design will be finalized and the necessary changes if needed will be adjusted before the development of the application.

4.3 User Roles

User roles can be divided into two categories.

- Users, those who are registered with the application and access the features of the application
- Administrator, who controls the entire application, security settings and customers.

4.4 Process Flow Details

This phase mentions the business logic of the application on how it works between different modules Users.

- Sign up
- API
- Administration
- Analytics and Report
- Settings

Further, a content management system which provides administration access for the administrator of this application and the mobile application using Android studio where the user can download in their android mobile phones in order to access the features such as chat, group chat, message, etc. will be developed along with the end to end security feature for secure communication.

4.5 End to End Security Implementation

The application will use XSalsa20 encryption algorithm to encrypt the typed message while exchanged and Poly1305 will be used to read a Message Authentication Code (MAC) [1]. After the encryption of the raw message, a double encryption is done by encrypting again using the recipient session key before sending to the server. Further, message storage will be carried out using the AES-256+SHA2 algorithm [1].

5. Research Design

The project will be following the standard of software development life cycle which is normally followed by all the software development projects worldwide in order to achieve the consistency and proper development of this application. Further, the project will be following the waterfall model during the development phase.

- Requirement Analysis
- Project Design
- Development
- Testing
- Feedback

5.1 Type of study

This project is a theory building research which aims in establishing and formulating a theory to achieve end to end security for a chat application.

5.2 Data collection method and research instruments

The data regarding the research on end to end encryption methods will be done by referring to many published books, journal articles and verified official websites. And a group of selected individuals will be used to collect data regarding the application security awareness.

5.3 Sampling technique

To collect statistical data on user interest of using a chat application, a group of individuals will be selected and feedback will be retrieved by providing them a questionnaire and by interviewing the selected group of people in order to find out the interest of using a secure application and to find the rate of application security awareness among people.

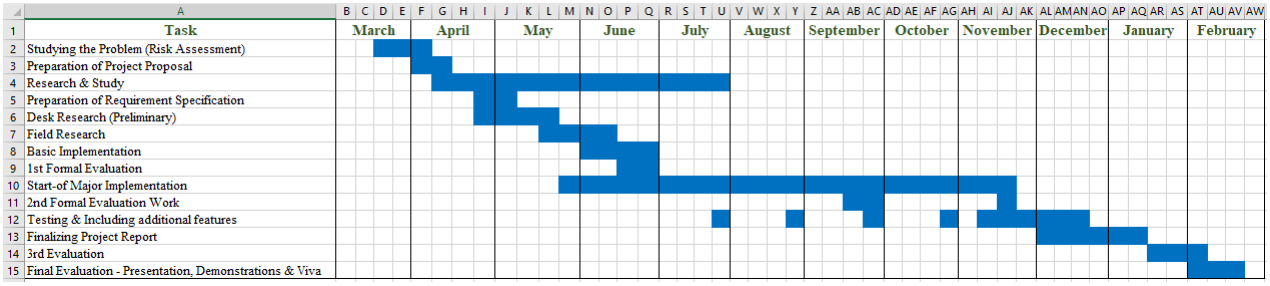
5.4 Intended data analysis techniques

A qualitative approach on data analysis technique will be used to carry out this project. The collected data will be analyzed using the Power Bi software in order to get a precise analysis on the sample.

6. Resource requirement

Required Resource	Justification	Acquiring Method
Android Studio	Build the chat application	Downloadable Application
MongoDB	Creation of database to store messages	Downloadable Application
Power Bi Software	Data analysis	Downloadable Application

7. Research Plan



Bibliography

1 N. Sabah, J. Kadhim and B. Dhannoon, "Developing an End-to-End Secure Chat Application", IJCSNS International Journal of Computer Science and Network Security, vol. 17, no. 11, 2017. [Accessed 10 March 2020].

2 A. Ali and A. Sagheer, "Design of Secure Chatting Application with End to End Encryption for Android Platform", Iraqi Journal for Computers and Informatics, vol. 43, no. 1, pp. 22-27, 2017. Available: 10.25195/ijci.v43i1.73 [Accessed 14 March 2020].

3 A. Ali and A. Sagheer, "Design and Implementation of Secure Chatting Application with End to End Encryption", Journal of Engineering and Applied Sciences, vol. 12, no. 1, 2017. [Accessed 15 March 2020].

4 J. Penttinen, The telecommunications handbook.2014.

5 R. Akram and R. Ko, "End-to-End Secure and Privacy Preserving Mobile Chat Application", 2016. [Accessed 1 April 2020].

6 "Purpose of Chat Applications | Redbytes Software", Redbytes: Custom Mobile Application Development Company [iOS, Android, Windows], 2020. [Online]. Available: https://www.redbytes.in/purpose-of-chat-applications/. [Accessed: 16- Apr- 2020].

7 WhatsApp, "WhatsApp Encryption Overview", WhatsApp, 2016

8 "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema", IEEE European Symposium on Security and Privacy, 2018. [Accessed 5 April 2020].

9 C. Idwenagu, Fundamentals of Research Methodology and Data Collection. ResearchGate, 2016.