**CHAPTER ONE**

**INTRODUCTION**

* 1. **Preamble**

Mobile chat applications are very popular among Internet users and smartphones’ owners. Hundred millions of smartphone owners use chat applications on monthly basis (Fang, 2009). These chat applications offer the communication free of charge and majority of them are free to install which makes it very appealing for the potential customers. These chat applications offer different services and built-in features to their users while in majority of the cases, they neglect security aspects of their usages and messages. According to a report provided by Electronic Frontier Foundation (EFF) majority of these chat applications do not provide enough security for their users.

Smartphones have become indispensable tools in today's workforce. There are hundred millions of smartphones in the market with different operating systems and capabilities. These smartphones have the capability of installing applications on them in order to do many tasks, such as sending text messages.

Wi-Fi networks have grown dramatically for the last decade and they are almost ubiquitous in daily life. According to a report by quarter 3 of year 2014, there are 2.5 billion mobile broadband subscriptions worldwide and it is predicted that it will be 8.4 billion mobile broadband subscriptions by the year 2020 (Wilson, 2002). This growth and accessibility to an Internet connection has brought opportunities for many Instant Messaging applications to enter a new area of communication and to penetrate traditional telephony communication.

Instant messaging applications are one of the most popular category of applications among the users. The IMs have the capability of sending messages or initiating voice calls via Internet, what makes it almost free for the users to communicate with each other and to share different type of files.

* 1. **Statement of the Problem**

Malicious users are always interested to hack servers and reveal information about users in a certain system including celebrities and this happens almost every day in the internet world. Unfortunately Mobile instant messaging applications are not an exception. There are many mobile chat applications available for users. Many of these applications claim that they are providing confidentiality, integrity and availability of user’s information, especially government agencies and organizations dealing with very sensitive information. However, daily hacking news prove that many developers do not consider security as the primary goal of their applications.

This final year project seeks to introduce a methodology that provides instant Messaging Service over the intranet which is addressed to android based smartphone and tablet users connected over intranet via Wi-Fi. Intranet based instant messenger is the key solution to provide a secure platform for agencies dealing with sensitive information to avoid the limitations of the internet based chat applications.

* 1. **Aim and Objectives**

This final year project is aimed at the design and implementation of an intranet based instant messenger (IM) app for android devices. The objectives are to:

1. Design the intranet based IM system;
2. Implement the designed mobile android based application;
3. Evaluate the implemented application for effective performance

**1.4** **Significance of Study**

Traditional instant messaging applications present a lot of problems and challenges to users due to pay services and internet security threats. These problems restrict user’s access to cheap and secure means of disseminating information with their colleagues, friends, and relations via a short distance. Thus the insight to propose an Android based IM system that will completely eliminate these problems users do experience so that they will have unrestricted access to free and secure means of communicating within a home, business or organizational set up, especially when privacy and security is of highest importance..

**1.5 Research Methodology**

This project is based on mobile application design and development science research methodology which makes it convenient to develop an artifact (an installable fully working mobile app and its server system). In such a methodology a problem is defined and the goals of the research is defined. A research was conducted to investigate current popular mobile chat applications, their features and threats that they might enforce to their users based on internet security flaws or IM app bugs. As the next step, the requirements for intranet based chat application are defined and architecture of a secure chat application is proposed in this project work. The final result of the research is a secure intranet based mobile chat application system. The methodology can be described as follows.

* Literature Review: A review of previous literatures that have relevance with the current thesis work was conducted. From the literature, different concepts and methodologies were adopted as deemed to be necessary.
* Resource Gathering: Here, the gathering of software tools and other necessary materials that are relevant to bringing the security countermeasure into picture were done. The materials are Android Studio IDE, Java 2 Mobile Edition (J2ME), different mobile simulators, etc.
* Developing the Prototype: Java programming language was used to develop the mobile application capability of android enabled mobiles and PHP (Laravel framework) for the server system.
* Experimenting: Android enabled phones of different capacities are to be selected to widen the depth of the application. The developed application will be installed on real android enabled mobile phones (not just emulators) and configure the application for compatibility with the selected phones.
* Testing the Performance: The degradation of performance would be investigated and Quality of Service due to the added security.
  1. **Scope of Study**

The scope of this research is developing a prototype of intranet IM mobile application design and development techniques for android enabled mobile phones and tablets. Also, the proposed system is based on the design and development of the secure intranet based instant messaging application using the client/server model.

* 1. **Limitations of Study**

This application is to be restricted to android platform alone. That means it can only be used on android-enabled phones and tablets. Also, it does not support sending and receiving of multimedia messages like picture, video and .gif messages, only text instant messages are allowed on the platform. This might be a good area for future researchers to look into.

**1.8 Organization of Project Report**

The remainder of this project work is divided into five chapters as follows:

• In chapter two, relevant literatures on past works on Chat system were intensively reviewed. This done in order to perfectly understand the full concepts behind the IM system in general as well as the technologies behind mobile application development, and the inclusion of various functionalities. The chapter also contained a brief overview of the tools used in the implementation of the system.

• Chapter Three: This chapter carefully explains the procedure followed in the implementation (the design and development) of the application software. Entity relational diagrams, flowchart and analysis of the mobile application development methodologies and tools used presented in this chapter. The relationships between the programming languages and tools used were properly given. The source code written in this chapter are to be attached as an appendix at the back of the project report when done.

• Chapter four: Here, the result of the implementation in chapter three is to be presented. The tools used in the development and presentation of the finished mobile application and its local server systems to be showcased and explain the way the system works. Snapshots of the working mobile android app were captured and shown in this chapter as well.

• Chapter Five: This is the chapter where a brief summary of the whole project work was given. Some conclusions drawn and further study recommendations were given as well.