CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, there has been quite a lot of improvement in technology sector. There have been much advancement in telecommunication, computing, research and other important fields out there. As a proof, we can take the mobile phones produced these days which is full packed with high end technologies to make its user to have a much better user experience and make it easy for them to carry out their daily tasks from anywhere and whenever they want to. But along with all those advancements, there have been also some serious issues that have emerged. An example of the issue would be the breach of confidentiality of data being transferred from one individual to another. Recently, there are some major mobile operating systems being embedded in mobile phones nowadays especially the smartphones and some of the example would be Android operating system (OS), IOS, Symbian OS, and Windows OS as well (Guru, 2015). Taking Android OS into consideration as for today’s trend because there are more of Android based smart phones users and their number is more compared to IOS based phone users as said in an article posted in the BusinessInsider website. (Edwards, 2014). The Android OS could have some vulnerability due to its open source architecture and also because of the actions of certain of its users who roots their android smartphones to gain root access. Hence, when an Android smartphone user sends data from their phone to another, the network could be compromised especially if they use a public wireless making their device to be more prone to hackers’ attacks. When the confidentiality of data being
transmitted is breached, the content is no more private and it could spread to anywhere.

So in order to prevent that from occurring, an application has been designed to encrypt and decrypt files especially text files using a really secure encryption algorithm which is the AES encryption algorithm. According to a journal titled as “Evaluating The Performance of Symmetric Encryption Algorithms” (Elminaam, 2010), the authors have made a research on three main criteria and they are the encryption time, CPU process time and CPU clock cycles and battery power. As a conclusion from their research, it has been concluded that AES has better performance compared to other encryption algorithm tested which are the RC2, DES, and 3DES encryption algorithm. Besides that, AES has been also said to be quite suitable to encrypt messages sent from one device to another (Ramesh, 2013). Hence, it has been also decided to use the AES algorithm to encrypt and decrypt files using an Android platform based application. As a conclusion, this application is believed to be able to help Android users to secure as well as protect the integrity and confidentiality of their data being transferred from one device to another.

1.2 Problem Statement

Security of data being transferred from one place to another is a big concern for everyone nowadays. The confidentiality of data being sent could be compromised if it is not properly secured with encryption algorithm while being transferred from one device to other. This becomes a bigger problem when a user uses public wireless internet connection at public places which is not properly enhanced with security such as password and hiding of Service Set Identifier (SSID) of the wireless internet connection. Being connected to an unsecured public network
which is also used by a lot of other users, their devices could be prone to network breach issues (Markelj, 2012). Besides that, the Android OS based devices being as an open source operating system, could experience a lot of threats in terms of data confidentiality and integrity when it’s being sent over from one device to other as anyone could breach into the device if they know how to do so. It could be worse if the device has been rooted in order to gain super user access to the root files of the device. In other words, these will the device more vulnerable to attacks of hackers and other malicious individuals.

1.3 Objective

i. To investigate the AES encryption algorithm to encrypt and decrypt text files being sent from one Android based device to another.

ii. To design the architecture of Android mobile application using the AES encryption algorithm.

iii. To develop an Android based mobile application which have the function to encrypt and decrypt files being sent from one device to another.

1.4 Scope

i. Target user would be Android OS based smartphone users.

ii. Focuses more on file encryption using the AES encryption algorithm to encrypt the files.

iii. Application developed will be an Android based mobile application.

iv. Apply proper programming techniques and use Java as well as web programming languages to develop the application.