SECURE MOBILE AES ENCRYPTOR (SMAE)

SATIA A/L ANBALAGAN

A thesis submitted in fulfilment of the requirements for the award of the degree of Bachelor of Computer Science (Computer Systems & Networking) with Honours

Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang

JUNE 2016

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's full name : Satia S/O Anbalagan

Date of birth : 3rd of September 1993

Title : Secure Mobile Aes Encryptor (SMAE)

Academic Session : SEMESTER 2 2015/2016

I declare that this thesis is classified as :

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1972)*

☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*

☐ OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserve the right as follows :

1. The Thesis is the Property of Universiti Malaysia Pahang.
2. The Library of Universiti Malaysia Pahang has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

_____ _____

_____ _____

930903-10-5235 Dr. Mohammed Falah Mohammed

Date: Date:

DECLARATION

I hereby declare that the work in this thesis entitled "**Secure Mobile Aes Encryptor (SMAE)**" is my own work except for quotations and summaries which have been duly acknowledged.

6/6/2016

Satia S/O Anbalagan

CA13107

SUPERVISOR DECLARATION

I hereby declare that I have read this thesis and in my opinion this thesis/report is sufficient in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Computer Systems & Networking)

Signature : ……...

Supervisor Name : Dr. Mohammed Falah Mohammed

Date : ……

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS/ACRONYMS

ABBREVIATION	TITLE	PAGE
OS	Operating System	1
AES	Advanced Encryption Standard	2
SSID	Service Set Identifier	2
ER	Entity Relationship	4
EER	Extended Entity Relationship	4
DES	Data Encryption Standard	5
SD	Secure Digital	11
PDF	Portable Document Format	13
PC	Personal Computer	16
GUI	Graphical User Interface	16
RAM	Random Access Memory	17
SDLC	Software Development Life Cycle	20
DFD	Data Flow Diagram	27
UAT	User Acceptance Test	54

SECURE MOBILE AES ENCRYPTOR (SMAE)

SATIA A/L ANBALAGAN

A thesis submitted in fulfilment of the requirements for the award of the degree of Bachelor of Computer Science (Computer Systems & Networking) with Honours

Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang

JUNE 2016

ABSTRACT

The purpose of this project is to identify a way to develop a mobile web application for the encryption and decryption of files using the 256 –bit Advanced Encryption Standard (AES) encryption algorithm. This is to ensure the data or files being shared between users are secure from and breach. When a user wants to send a file which contains confidential and important information, the user can protect the data inside the file by encrypting the data using the application developed using their mobile phones and send it to the person they intended to send the data. The reason the AES encryption algorithm selected is because it is considered as one of the most secure encryption algorithm. This can be proved where the National Security Agency (NSA) in the United States to encrypt confidential data and information. This application will focus more on the user of the Android operating systems based mobile phone users. Besides that, the application is developed as a web based application to ensure the application can be accessed using both mobile application as well as web browser. On the other hand, the proper testing of the application is done to ensure that there is a proper user satisfaction level of the users of the application. This is done using the User Acceptance Test to evaluate the user experience while using the application as the objective of the application development is also to improve the interface as well as the functionality of the application compared to the similarly available applications in the Google Play Store.

ABSTRAK

Tujuan projek ini adalah untuk mengenal pasti satu cara untuk membangunkan aplikasi web mudah alih untuk penyulitan dan penyahsulitan fail menggunakan algoritma penyulitan “256-bit Advanced Encryption Standard (AES)”. Ini adalah untuk memastikan data atau fail yang dikongsi di antara pengguna telah selamat dari penggodam yang ingin mencuri data. Apabila pengguna ingin menghantar fail yang mengandungi maklumat sulit dan penting, pengguna boleh melindungi data di dalam fail dengan menyulitkan data menggunakan aplikasi yang dibangunkan menggunakan telefon bimbit mereka dan menghantar kepada orang yang mereka bertujuan untuk menghantar data. Sebab algoritma penyulitan AES dipilih adalah kerana ia dianggap sebagai salah satu algoritma penyulitan yang paling selamat. Ini dapat dibuktikan di mana Agensi Keselamatan Negara (NSA) di Amerika Syarikat mengunakan algoritma tersebut untuk menyulitkan data sulit dan maklumat. Aplikasi ini akan memberi tumpuan lebih kepada pengguna telefon bimbit yang berasaskan sistem operasi Android. Di samping itu, permohonan itu dibangunkan sebagai aplikasi berasaskan web untuk memastikan permohonan boleh diakses dengan menggunakan kedua-dua aplikasi mudah alih dan pelayar web. Tambahan pula, beberapa analisis serta kaji selidik telah dilakukan untuk memastikan tahap kepuasan pengguna berada dalam tahap yang memuaskan. Ini dilakukan dengan menggunakan Borang Kaji Selidik Kepuasan Pengguna untuk menilai pengalaman pengguna semasa menggunakan aplikasi.Hal ini kerana salah satu objektif pembangunan aplikasi ini adalah untuk menambah baik paparan serta fungsi permohonan itu berbanding dengan aplikasi-aplikasi yang boleh didapati di Google Play Store.

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.