SECURE COMMUNICATION IN LOCATION BASED SERVICES (LBS) USING ADVANCED ENCRYPTION STANDARD 256(AES 256)

This thesis is presented in partial fulfilment for the award of the Bachelor of Engineering Electronic (Communication) with honours.

UNIVERSITI TEKNOLOGI MARA (UITM)

NUR AFIQAH BINTI MOHD NOOR
FACULTY OF ELECTRICAL ENGINEERING
UNIVERSITI TEKNOLOGI MARA,
40450 SHAH ALAM,
SELANGOR, MALAYSIA

18 JULY 2014

ACKNOWLEDGEMENT

First of all, I would like to thank ALLAH SWT because for HIS blessing, finally I able to complete my final year project with this thesis as well within the allocated time.

This research work would not have been completed without help and support of many individuals. I would like to thank everyone who has helped me along the way. I would like also to thank my supervisor Puan Hanunah Othman for giving me the opportunity to conduct my final year project under her and for her guidance and support over the course of it. I am also grateful to Encik Mohd Anuar Mat Isa for his invaluable help to understand cryptography and for serving on valuable suggestions. I am specially thanked for their attention, guidance, insight and support during this final year project.

My appreciation also to my beloved family for their support and understanding, without which, I could never ever walk the first step. Lastly, my thanks to other colleagues and the persons who directly or indirectly involved and distributed in completing this project and not forget to all my friends who give their full commitment and their best effort. Thank you very much.

ABSTRACT

Location based services are any services or software applications that requires the geographic location (longitude and latitude) of an entity. Nowadays, with the aid of smartphones, location based services have improved tremendously in the market with wide range of users. Many mobile applications implement location based services in their applications to gain the user's information for applications service purpose. Location based services are used in a variety of scopes such as health, indoor object search, entertainment, work and personal life. However, in many existing location based services, the user's information were not private where the service provider is aware with the user's location and may leak this information to any unauthorized entities. This may lead to misuse of information by the third party which could endanger the user. As an instance, thieves may use the geo-location to determine whether victim is at home or not, and they able to use the data to plan a burglary.

Based on the issues, to encounter this problem a symmetric encryption can be used as a solution to encrypt the data sent within client and location based services. Symmetric encryption is used to protect user's information by convert the information to private text. Symmetric encryption performed the process of encryption and decryption by using same shared key between client and server. Symmetric encryption has some types such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

An experiment of symmetric encryption using TCP/IP client-server for protecting user's privacy in the communication had been conduct to prove the user's information is encrypted. Advanced Symmetric Encryption 256 (AES256) has been chosen among the symmetric encryption variations due to it benefits. This project demonstrates the process of creating the application which responsible for communication over TCP protocol between two computers and the user interface.

TABLE OF CONTENTS

DECLARATION	i
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
TABLE OF CONTENTS	vi
LIST OF FIGURES	vii
LIST OF TABLES	ix
LIST OF SYMBOLS AND ABBREVIATIONS	x
CHAPTER 1	
INTRODUCTION	1
1.1 BACKGROUND OF STUDY	1
1.2 PROBLEM STATEMENTS	2
1.3 OBJECTIVES	2
1.4 SCOPE OF PROJECT	3
1.5 THESIS ORGANIZATION	4
CHAPTER 2	
LITERATURE REVIEW	4
2.1 INTRODUCTION OF LITERATURE REVIEW	6
2.2 CRYPTOGRAPHY	6
2.3 ENCRYPTION	7
2.4 SYMMETRIC ENCRYPTION	8
2.5 ADVANCED ENCRYPTION SYSTEM (AES)	9

2.6 CLIENT-SERVER 10

2.7 LOCATION BASED SERVICES AND PRIVACY ISSUES 12

CHAPTER 3

METHODOLOGY **15**

3.1 OVERVIEW 15

3.2 FLOWCHARTS 15

3.3 WIRESHARK 19

3.4 LINUX 19

3.5 RASPBERRY-PI 21

3.6 WiPi 22

3.7 MACHINE SETUP 23

3.8 EXPERIMENTAL SETUP 24

CHAPTER 4

RESULTS AND DISCUSSIONS **29**

4.1 OVERVIEW 29

4.2 EXPERIMENT PERFORMANCE 30

4.3 RESULTS 31

4.4 RESULTS AND PERFORMANCE 33

CHAPTER 5

CONCLUSIONS **39**

5.1 CONCLUSIONS 39

5.2 RECOMMENDATIONS 39

REFERENCES **41**

APPENDICES **43**