

**SECURING FILE SHARING IN MOBILE APPLICATION USING  
STEGANOGRAPHY APPROACH**



MUHAMMAD HAFIZUDDIN BIN SHARUL LAZI



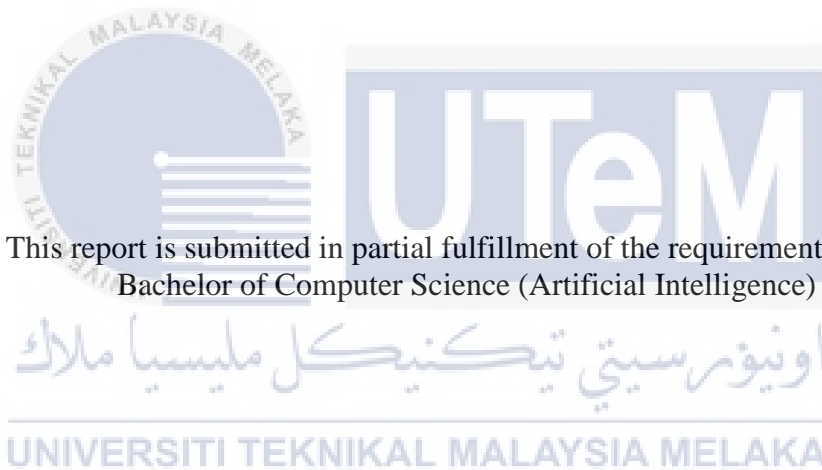
اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

# SECURING FILE SHARING IN MOBILE APPLICATION USING STEGANOGRAPHY APPROACH

MUHAMMAD HAFIZUDDIN BIN SHARUL LAZI



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

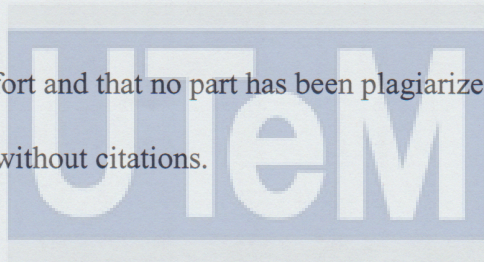
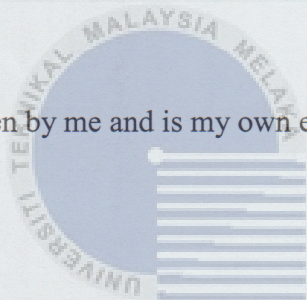
2017

## DECLARATION

I hereby declare that this project report entitled

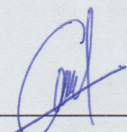
### SECURING FILE SHARING IN MOBILE APPLICATION USING STEGANOGRAPHY APPROACH

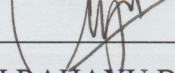
is written by me and is my own effort and that no part has been plagiarized  
without citations.



اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

STUDENT :  DATE: 17/08/2017  
(MUHAMMAD HAFIZUDDIN BIN SHARUL LAZI)

SUPERVISOR :  DATE: 23/8/2017  
(DR SITI RAHA YU BINTI SELAMAT)

## DEDICATION

Securing File Sharing In Mobile Application Using Steganography Approach are dedicated to my parent Mr. Sharul Lazi Bin Nik and Madam Roslina Binti Ariffin. My deepest dedication also goes to my final year project supervisor, DR Siti Rahayu binti Selamat. Last but not least, I would like to dedicate this system to the entire lecturer of Faculty Information and Communication Technology whose teach me from zero to what I am capable of and to my classmate that support me and give some idea in developing the project.



## ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful.

Alhamdulillah, all praises to Allah Almighty for the strengths and His blessing in completing this final year project. A special gratitude I give to my final year project supervisor, Dr Siti Rahayu binti Selamat whose contribute in stimulating suggestions and encouragement and also helped me to coordinate my project especially in developing the system specifically features and documentation.

Bearing in mind, I am using this opportunity to express my deepest gratitude and special thanks to my parent and family members because always give me a word of encouragement and taking part arranged all facilities to make my work easier.

Last but not least, I would like to give a special thanks to my classmates for their cooperation and always helping me in order to develop the system and writing this report. I will strive to use gained skills and knowledge in developing this final year project in the best possible way.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## ABSTRACT

File sharing application is the software application that providing access or distributing of digital media from devices to another such as electronic document, multimedia items and computer program. Nowadays, people are currently use mobile phone as their sharing medium as it more convenience and faster. This situation has led to data breach incident which mean the data are easily being stolen, accessed and manipulated by unauthorized party. Therefore, the aim of this project to hide the sensitive information from being known its existence by cyber-attacker. To achieve the aim, Steganography technology will be integrated within file sharing application as solution to the problem faced as this technology allow the file being transferred hidden inside other data. This project will used LSB (Least Significant Bit) algorithm technique as the steganography technology in which image is used as transfer medium to carry the sensitive data. This technique have two basic processes which are Embedding Process and Extracting Process. Embedding process is to hide the data while Extracting process is to recover back the data. The result of this project will be determined by the percentage of difference between the original image and the stego image in term of image pixel and size. In conclusion, the integration of steganography technology with the file sharing application will increase the security level of the sensitive data that being transferred.

## ABSTRAK

Aplikasi perkongsian fail merupakan aplikasi perisian yang menyediakan akses atau mengedar media digital dari peranti ke peranti yang lain seperti dokumen elektronik, barangan multimedia dan program komputer. Masa kini, orang ramai menggunakan telefon bimbit sebagai medium perkongsian mereka kerana ia lebih mudah dan pantas. Keadaan ini telah membawa kepada kejadian *Data Breaches* yang bererti data mudah dicuri, diambil dan dimanipulasikan oleh pihak yang tidak dibenarkan. Oleh itu, tujuan projek ini untuk menyembunyikan kewujudan maklumat sensitif daripada diketahui oleh penjenayah siber. Untuk mencapai matlamat ini, teknologi *Steganography* akan digunapakai dalam fail perkongsian sebagai jalan penyelesaian kepada masalah yang dihadapi. Penggunaan teknologi ini membolehkan fail dipindahkan tersembunyi di dalam data yang lain. Projek ini menggunakan teknik algoritma LSB (*Least Significant Bit*) sebagai teknologi steganography di mana imej digunakan sebagai medium pemindahan untuk membawa data yang sensitif. Teknik ini mempunyai dua proses asas iaitu proses *Embedding* dan proses *Extracting*. Proses *Embedding* adalah untuk menyembunyikan data manakala proses *Extracting* adalah untuk mendapatkan kembali data. Hasil akhir projek ini akan dapat ditentukan dengan kadar peratusan perbezaan dari segi piksel imej dan saiz di antara gambar asli dan gambar stego. Kesimpulannya, integrasi teknologi steganography dengan aplikasi perkongsian fail akan meningkatkan tahap keselamatan bagi data yang sensitif semasa data dipindahkan.

## TABLE OF CONTENTS

<b>DECLARATION</b> .....	<b>I</b>
<b>DEDICATION</b> .....	<b>II</b>
<b>ACKNOWLEDGEMENT</b> .....	<b>III</b>
<b>ABSTRACT</b> .....	<b>IV</b>
<b>ABSTRAK</b> .....	<b>V</b>
<b>TABLE OF CONTENTS</b> .....	<b>VI</b>
<b>LIST OF TABLES</b> .....	<b>XI</b>
<b>LIST OF FIGURES</b> .....	<b>XII</b>
<b>CHAPTER 1: INTRODUCTION</b>	
1.1 Introduction .....	1
1.2 Background Study .....	1
1.3 Problem Statement .....	4
1.4 Project Questions.....	5
1.5 Project Objective .....	5
1.6 Project Scope.....	6
1.7 Expected Output.....	6
1.8 Report Organization .....	6
1.9 Summary .....	8
<b>CHAPTER 2: LITERATURE REVIEW</b>	
2.1 Introduction .....	9
2.2 Mobile Application .....	10
2.2.1 Revolution of Mobile Application .....	10
2.2.2 Development Platform of Mobile Application.....	11
2.2.3 Mobile Client-Server Application.....	13
2.2.4 Analysis on Mobile Application .....	14
2.3 File Sharing Application .....	17
2.3.1 Definition of File Sharing Application .....	18
2.3.2 Method of File Sharing Application.....	18



2.3.3 File Sharing Application Available on Market .....	19
2.3.4 Analysis on File Sharing Application .....	20
2.4 Authentication Mechanism .....	22
2.4.1 Revolution of Authentication Mechanism .....	22
2.4.2 Types of Authentication Mechanism .....	24
2.4.3 Analysis on Authentication Mechanism .....	26
2.5 Encryption Technique .....	28
2.5.1 Definition of Encryption Technique .....	29
2.5.2 Types of Encryption Technique .....	30
2.5.3 Analysis on Encryption Technique .....	43
2.6 Steganography .....	46
2.6.1 Definition of Steganography .....	46
2.6.2 Types of Steganography Technique .....	48
2.6.3 Taxonomy of Image Steganography Technique .....	50
2.6.4 Analysis on Steganography Technique .....	56
2.7 Propose Project.....	62
2.8 Summary .....	64

### **CHAPTER 3: METHODOLOGY**

3.1 Introduction.....	66
3.2 Object-Oriented Approach Overview .....	66
3.2.1 Inception phase.....	67
3.2.2 Elaboration phase .....	68
3.2.3 Construction phase .....	69
3.2.4 Transaction phase.....	70
3.3 Project Schedule and Milestones.....	71
3.3.1 Flow Chart of Project .....	71
3.3.2 Gant Chart of Project.....	72
3.3.3 Milestone of Project .....	73
3.4 Summary .....	74

### **CHAPTER 4: ANALYSIS AND DESIGN**

4.1 Introduction .....	75
4.2 Problem Analysis .....	76
4.3 Cryptographic Technique Algorithm .....	78

4.3.1 Elliptic Curve Cryptography (ECC).....	78
4.3.2 Blowfish .....	82
4.4 Steganographic Technique Algorithm .....	85
4.4.1 Least Significant Bit (LSB).....	85
4.5 Message Digest Algorithm.....	93
4.5.1 Generation of Hash Data .....	93
4.5.2 Validation of Hash Data.....	94
4.6 Requirement Analysis .....	96
4.6.1 Software Requirement.....	96
4.6.2 Hardware Requirement .....	97
4.6.3 Data Requirement.....	99
4.7 High-Level Design .....	101
4.7.1 System Architecture .....	101
4.7.2 User Interface .....	101
4.8 Low-Level Design.....	103
4.9 Summary .....	103
<b>CHAPTER 5: IMPLEMENTATION</b>	
5.1 Introduction .....	104
5.2 Application Development Environment Setup .....	104
5.3 Configuration Management.....	106
5.3.1 Authenticate user validity process.....	108
5.3.1.1 Authentication using Fingerprint mechanism .....	109
5.3.1.2 Authenticate using Password mechanism process .....	111
5.3.2 Encrypt the selected file process .....	113
5.3.2.1 Encrypt file using ECC process .....	114
5.3.2.1.1 Encrypt file process.....	115
5.3.2.1.2 Decrypt file process.....	117
5.3.2.2 Encrypt file using Blowfish process .....	120
5.3.2.2.1 Encrypt file process.....	121
5.3.2.2.2 Decrypt file process.....	123
5.3.3 Generate hash value by message digest process .....	125
5.3.3.1 Get hash data process .....	126
5.3.3.2 Validate hash data process .....	128

5.3.4 Hiding data into image using LSB algorithm process .....	130
5.3.4.1 Embedding the secret message process.....	131
5.3.4.2 Extracting secret message from Stego-Image process .....	134
5.4 Summary .....	137

## **CHAPTER 6: TESTING**

6.1 Introduction .....	138
6.2 Testing Management .....	138
6.2.1 Testing Authentication .....	140
6.2.1.1 Testing Fingerprint authentication procedure .....	141
6.2.1.2 Testing Password authentication procedures. ....	142
6.2.2 Testing encryption procedure.....	143
6.2.2.1 Testing ECC encryption procedure .....	145
6.2.2.2 Testing Blowfish encryption procedure .....	146
6.2.3 Testing hash value procedure.....	148
6.2.4 Testing steganography using LSB algorithm .....	149
6.3 Testing Result and Analysis .....	150
6.3.1 Result and analysis of testing authentication .....	150
6.3.1.1 Result and analysis of testing Fingerprint authentication. ....	151
6.3.1.2 Result and analysis of testing Password authentication. ....	154
6.3.2 Result and analysis of testing encryption.....	156
6.3.2.1 Result and analysis of testing ECC encryption .....	157
6.3.2.2 Result and analysis of testing Blowfish encryption .....	160
6.3.3 Result and analysis of testing hash value .....	164
6.3.4 Result and analysis of testing Steganography using LSB algorithm .....	166
6.4 Summary .....	173

## **CHAPTER 7: CONCLUSION**

7.1 Introduction .....	174
7.2 Observation on Weaknesses and Strengths .....	174
7.3 Proposition for Improvement .....	177
7.4 Project Contribution .....	177
7.5 Project Summarization .....	178
7.6 Conclusion.....	178

<b>REFERENCES</b> .....	<b>179</b>
<b>APPENDIX</b> .....	<b>183</b>



## LIST OF TABLES

TABLE TITLE	PAGE
Table 1.1 Project Problem.....	4
Table 1.2 Project Question.....	5
Table 1.3 Project Objective.....	5
Table 2.1 Mobile Application Development Approach Comparison .....	16
Table 2.2 Comparison between 5 File Sharing applications.....	21
Table 2.3 Usability of Authentication Mechanism .....	27
Table 2.4 Analysis of Encryption Techniques .....	44
Table 2.5 Problem regarding Steganography Technique.....	57
Table 2.6 Overview problem faced by Steganography Technique .....	58
Table 2.7 Comparison of Image Steganography Techniques .....	61
Table 3.1 Milestone of Project Activities .....	74
Table 4.1 Procedure of Elliptic Curve encryption technique.....	80
Table 4.2 Procedure of Elliptic Curve decryption technique.....	81
Table 4.3 Procedure of Blowfish encryption technique.....	83
Table 4.4 Procedure of Blowfish decryption technique.....	84
Table 4.5 Conversion of Binary to Decimal .....	86
Table 4.6 Algorithm of LSB embedding technique .....	89
Table 4.7 Algorithm of LSB extracting technique.....	92
Table 4.8 Generation of Hash Data.....	94
Table 4.9 Validation of Hash Data.....	95
Table 4.10 Software Requirement.....	96
Table 4.11 Smartphone Specification .....	98
Table 4.12 Laptop Specification .....	99
Table 4.13 SFS Functional Requirements.....	100
Table 4.14 User Interface in Secure File Sharing application.....	102
Table 6.1 Difference in image pixels between stego image and original image.....	169
Table 6.2 Increment of Stego Image size based on two different algorithm .....	171

## LIST OF FIGURES

FIGURE TITLE	PAGE
Figure 1.1 Statistic Report for Number of Breach Incidents by Source over Time to First Half of 2016 (Gemalto NV, 2016).....	3
Figure 2.1 Framework of Literature Review.....	9
Figure 2.2 Client-Server system architecture.....	13
Figure 2.3 Cryptography Process (Bhanot & Hans, 2015) .....	29
Figure 2.4 Function F of DES .....	31
Figure 2.5 3DES Structure .....	33
Figure 2.6 Blowfish Function F (Christina & S, 2014).....	37
Figure 2.7 Round Function of Twofish (Уайтинг et al., 2004).....	38
Figure 2.9 Threefish-1024 Block cipher round.....	40
Figure 2.10 RC5 Encryption Procedure .....	41
Figure 2.11 IDEA Encryption Process.....	42
Figure 2.12 Graphical Version of the Steganography System ( <i>Kumar &amp; Pooja, 2010</i> ) .....	48
Figure 3.1 RUP Phase Process .....	67
Figure 3.2 Flow Chart of Project Activities .....	72
Figure 3.3 Gant Chart of Project Activities.....	73
Figure 4.1 Flow chart of Proposed System .....	77
Figure 4.2 Flow chart of ECC encryption process .....	80
Figure 4.3 Flow chart of ECC decryption process .....	81
Figure 4.4 Flow chart of Blowfish encryption process .....	83
Figure 4.5 Flow chart of Blowfish decryption process .....	84
Figure 4.6 Flow of LSB embedding process of application.....	87
Figure 4.7 Flow chart of LSB embedding algorithm .....	88
Figure 4.8 Flow of LSB extracting process of application .....	90
Figure 4.9 Flow chart of LSB extracting algorithm .....	91
Figure 4.10 Generation of Hash Data.....	93
Figure 4.11 Validation of Hash Data .....	95
Figure 4.12 Huawei P9 Lite smartphone.....	97
Figure 4.13 Overview System Interface.....	102
Figure 5.1 Overview of the Secure File Sharing application .....	105

Figure 5.2 Overview of process based on the modules.....	107
Figure 5.3 Overview of authenticate user validity .....	108
Figure 5.4 Authenticate using Fingerprint mechanism process flow .....	110
Figure 5.5 Pseudo code of authenticate using Fingerprint mechanism.....	111
Figure 5.6 Authentication using Password mechanism process flow .....	112
Figure 5.7 Pseudo Code of authenticate using Password mechanism process.....	113
Figure 5.8 Overview of Encrypt selected file process .....	114
Figure 5.9 Overview of encrypt selected file using ECC process.....	115
Figure 5.10 Encrypt file process flow .....	116
Figure 5.11 Pseudo code of encrypt file process.....	117
Figure 5.12 Decrypt file process flow .....	118
Figure 5.13 Pseudo code of decrypt file process.....	119
Figure 5.14 Overview of Encrypt selected file using Blowfish process .....	120
Figure 5.15 Encrypt selected file process.....	121
Figure 5.16 Pseudo code of encrypt file process.....	122
Figure 5.17 Decrypt file process flow .....	123
Figure 5.18 Pseudo code of decrypt file process.....	125
Figure 5.19 Generate hash value by message digest process flow.....	126
Figure 5.20 Flow of Get hash data process .....	127
Figure 5.21 Pseudo Code of Get Hash data process .....	128
Figure 5.22 Validate hash data process flow.....	129
Figure 5.23 Pseudo Code of Validate Hash data process.....	130
Figure 5.24 Overview of hiding data into image using LSB algorithm process.....	131
Figure 5.25 Embedding the secret message process flow .....	132
Figure 5.26 Pseudo code of Embedding secret message process.....	134
Figure 5.27 Extracting secret message from Stego-Image process.....	135
Figure 5.28 Pseudo code of Extracting secret message from Stego-Image .....	136
Figure 6.1 Overview of testing based on the modules .....	139
Figure 6.2 Overview of testing authentication procedure .....	140
Figure 6.3 Testing Fingerprint authentication procedures .....	141
Figure 6.4 Testing Password authentication procedures .....	143
Figure 6.5 Overview of testing encryption procedures .....	144
Figure 6.6 Testing ECC encryption procedures .....	145
Figure 6.7 Testing Blowfish encryption procedures .....	147

Figure 6.8 Overview of testing hash value procedures .....	148
Figure 6.9 Testing steganography using LSB algorithm procedures .....	149
Figure 6.10 Result of setup fingertips in Android Fingerprint Manager .....	151
Figure 6.11 Result of succeed Fingerprint authentication.....	152
Figure 6.12 Result of failed Fingerprint authentication .....	153
Figure 6.13 Result of succeed encrypted password .....	154
Figure 6.14 Result of succeed encrypted password in authentication process.....	154
Figure 6.15 Result of succeed Password authentication .....	155
Figure 6.16 Result of failed Password authentication.....	156
Figure 6.17 The Hexadecimal String value of private key and public key .....	157
Figure 6.18 The encrypted file create by encryption process .....	157
Figure 6.19 The confidentiality status of encrypted file .....	158
Figure 6.20 The original file create by decryption process.....	159
Figure 6.21 The readable decrypted file.....	160
Figure 6.22 The Hexadecimal String value of secret key .....	161
Figure 6.23 The encrypted file create by encryption process .....	161
Figure 6.24 The confidentiality status of encrypted file .....	162
Figure 6.25 The original file create by decryption process.....	163
Figure 6.26 The readable decrypted file.....	164
Figure 6.27 Comparison of two hash value for same file .....	165
Figure 6.28 Comparison of two hash value for two slightly difference file .....	166
Figure 6.29 Output of Embedding Process .....	167
Figure 6.30 Output of Extracting Process .....	168
Figure 6.31 Comparison between original image and stego image .....	168
Figure 6.32 Graph of differences in pixel between original image and stego image	170
Figure 6.33 Graph of increment in stego image size using two different LSB algorithm .....	172





## INTRODUCTION

### 1.1 Introduction

In this chapter, the background study is explained that led to discovery of problem statements. Based on identified problem statements, project question and project objective being develop. The study go on to indicate the project scope which identified the covered scope of the project and the limitation of the project. Next, expected output is being explained. Lastly, this chapter briefly explain the report organization.

### 1.2 Background Study

William Gibson was the first person who using the cyberspace term in his book which is Neuromancer. According to this book that was written in 1984, Gibson defines cyberspace as “a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concept. A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, Lines of light ranged in the non-space of the mind, cluster and constellation of data” (Christensson, 2006). However, cyberspace have no static definition as many people keep giving different definition for this term.

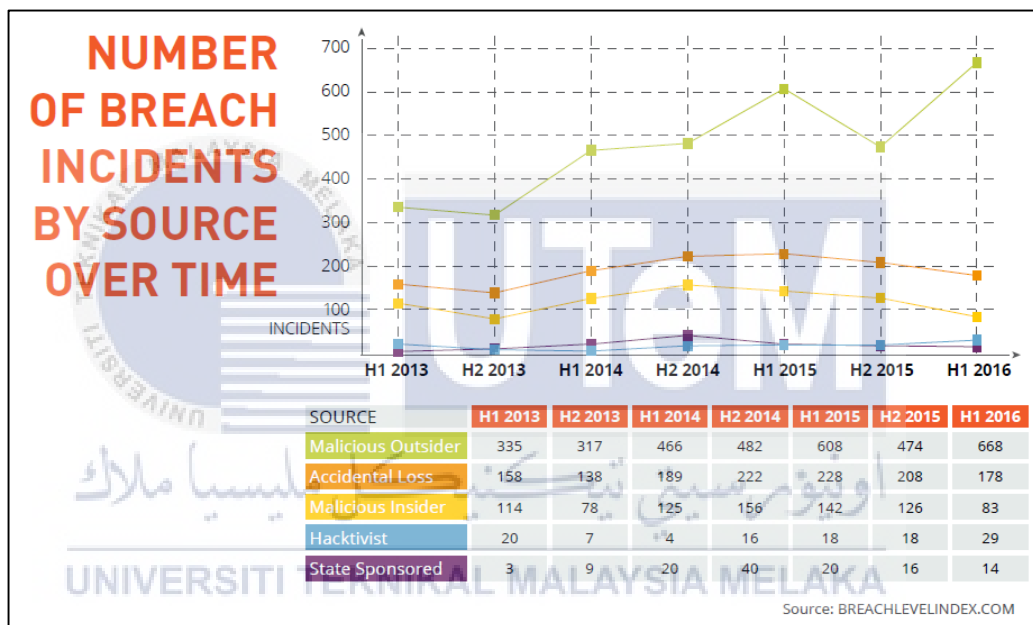
Instead of described as virtual world of computers, cyberspace also define as block of data that moving around network or computer system. The rapidly advancing of the internet has led cyberspace now extends to the network of computer globally.

Nowadays, as the technology emerged, most people no longer used manual method of send data to other persons. Instead, they will use cyberspace to share any information to the others without any hesitation. This behavior has led to the rising of data breaches activity. Data breach is an incident in which sensitive, protected or confidential data has potentially been view, stolen or used by an unauthorized individu. Even though 2016 not have as many headline-grabbing data breaches, it certainly has witness a continuation of assault in large-scale that have trigger senior business executives and boards of directors at many company to make cyber security as a top priority.

In the first half of 2016, approximately 553 million data record has been successfully breaches. There are 5 most popular source of data breaches incident namely Malicious Outsider, Malicious Insider, Accidental Loss, Hacktivists and State Sponsored. Data breaches caused by Malicious Outsider has result in theft or loss of 261 million data records or 47% of the total breached data record. That shown the increasing of 23% from the previous six months which only had 96.5 million breached data records. In addition, Accidental Loss involved the loss of 257 million data records or 46% of the total and increasing from 231 million in the previous six months. Moreover, Malicious Insider has accounted for 13.5 million data records that loss or theft. Apart from the rising of data record breached from other source of data breaches incident, this record shown the decreasing of 79% from the previous six months which accounted for 62.8 million breached data record. Furthermore, Hacktivists activity has involved 11.4 million records that also shown a significant drop from the previous six months which involved of 30 million. Meanwhile, State-sponsored attack led to 10 million of loss data record which indicate the increasing of 4 million in the prior six months (Gemalto NV, 2016) as shown in Figure 1.1.

Figure 1.1 shows the analytical report of data breaches incident that acquired for the first half of the 2016 compared to the previous six years. It shows that malicious outsiders were the biggest source of data breaches in the first half of 2016 which is 668 breaches, or 69% of the total. Compared to 474 attacks during the previous six

months, a rise of 41%. Next on the list of most common sources was accidental loss which encountered for 178 data breaches or 18% of the total. This was a 14% decline from the 208 breaches during the previous six months. Besides that, Malicious Insider were the next most common source of breaches, accounting for 83 or 8.5% of the total. That's down decrease from 126 during the previous six months. Furthermore, Hacktivists were responsible for 29 data breaches or 3% of the total from 18 during the previous six months which indicate the increase of 61%. Finally, state-sponsored attacks accounted for 14 of the data breaches or 1.4% of the total, down from 16 over the previous six months.



**Figure 1.1** Statistic Report for Number of Breach Incidents by Source over Time to First Half of 2016 (Gemalto NV, 2016)

From these statistic, it state that only two source of the breaches incident that increasing over the past six months which is Malicious Outsider and Hactivists. There are a lot of vulnerability of the network configuration in any organization that can lead to this cyber-attack. However one most common method of the data breaches is intercept the data when it was sent across the open network. Hence, the most common way to prevent this attack is by develop a secure platform for user to transmit any information to other people.

By developing a secure platform for information transmitting, data breaches from Malicious Outsider, Malicious Insider and Hacktivists can be reduced. Secure platform can be explained by implementing a few security techniques such as Cryptography and Steganography. Cryptography is defines as a technique to disguise information in such way that its meaning is unintelligible to an unauthorized person. However, it is very difficult to really secure the information from being breach by cyber criminals as the unintelligible information still can be withholding by attacker and might be successfully decrypted as the information is well known as encrypted data. Hence, the steganography technique should be used simultaneously with Cryptography as the unintelligible information will be embedded into other insensitive information that is allow to be breaches by unauthorized person.

### 1.3 Problem Statement

Nowadays, data breaches attack has increasing rapidly over the year. Even though many file sharing application provide Cryptography technology, this does not stop cyber-attacker from disclosure the sensitive data which violated the data's confidentiality and integrity value indirectly resulting to millions dollar of losses.

**Table 1.1 Project Problem**

No	Project Problem
PP1	The sensitive information can be seen its existence even may not be understand.
PP2	The confidentiality and integrity of information transmitted across network is not protected.
PP3	No secure Platform in sharing file across network.

## 1.4 Project Questions

Based on the problem statements, three project questions (PQ) are constructed as shown in Table 1.2.

**Table 1.2 Project Question**

PP	PQ	Project Question (PQ)
PP1	PQ1	How can we hide the existence of the information that being transmitted across the network?
PP2	PQ2	How can we secure the information's confidentiality and integrity is maintain after it received by others?
PP3	PQ3	How can we provide a secure platform for information being transmitted across the network?

## 1.5 Project Objective

In order to solve the problem identified as in Section 1.2, three project objectives (PO) are derived as shown in Table 1.3;

**Table 1.3 Project Objective**

PP	PQ	PO	Project Objective (PO)
PP1	PQ1	PO1	To conceal the presence of sensitive information from being disclosure by cyber-attacker.
PP2	PQ2	PO2	To secure the confidentiality and integrity of the information while being transfer across network.
PP3	PQ3	PO3	To develop a platform for users to share/transfer information amongst each other in secured environment

## 1.6 Project Scope

The scope for this project are:

- I. Secure the information that being transferred across the network by hiding and change the information structure using Steganography and Encryption approaches.
- II. The functionality of the project is based on mobile phone environment.

## 1.7 Expected Output

The expectation by the end of this project is to contribute and provide a better platform for user to transmitting information to other person by using the Secure File Sharing application.

## 1.8 Report Organization

The report is consists of seven chapters namely Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Analysis and Design, Chapter 5: Implementation, Chapter 6: Testing and Chapter 7: Conclusion. The brief elaboration of each chapter is as follow;

### **Chapter 1: Introduction**

This chapter explained about the definition, background study, problem statement, objective, scope and expected output related to the Secure File Sharing application.

## **Chapter 2: Literature Review**

This chapter discussed and analyzed the topics that related to this project such as mobile application, file sharing application, authentication mechanism, encryption technique and steganography. The outcome of this chapter will guide the development of this project's structure.

## **Chapter 3: Methodology**

This chapter provide a decision of the method of development that will be carry out to develop this project. With certain method of development will help to develop the system in less time required and easy for system testing and correction.

## **Chapter 4: Analysis and Design**

This chapter will explained the design phase of this project such as specifies the preliminary design and the detailed design of the system modules stated in Chapter 2 and specifies the Graphical User Interface design.

## **Chapter 5: Implementation**

This chapter will explained in detail the implementation phase of this project such as the software code and logic process based on module designed in Chapter 4.

## **Chapter 6: Testing**

This chapter will discussed the testing plan for each of the system modules as elaborated and analyzed in Chapter 4 and Chapter 5. Next, the result of each of the testing plan will be analyzed to ensure each of the system module is implemented correctly in this project.

## **Chapter 7: Conclusion**

This chapter compile the entire chapter in a final documentation by elaborated the observation on the weaknesses and strengths of this project, proposition for improvement, project contribution, project summarization and conclusion.

## 1.9 Summary

This chapter is elaborated in details about the introduction of this project that includes background study, problem statement, project questions, project objective, project scope, expected output and report organization. The background study explain data breaches incident across the world in 2016 that lead to developing of this project as one way to reduce the threat. Problem statement explained the problems faced by individu or organization in securing their information from attacker while transferring the information across the open network. The project question and project objective is corresponding to each other which the project question state the arise question about the project and the project goal is the answer of each question. Project scope explain in details about the elements covered in this project and the limitation of this project. Expected output state the last outcome of the project which is the developing of the Secure File Sharing application and lastly report organization briefly explain all chapter covered in this report. Chapter 2 will elaborate in details about the literature review done to develop the project which covers topic on mobile application, file sharing application, authentication mechanism, encryption technique and steganography.