**BORANG PENGESAHAN STATUS TESIS***

JUDUL: **IMPLEMENTATION OF SECURE CONFIDENTIAL-DOCUMENT TRANSFER AND STORAGE**

SESI PENGAJIAN: **2012**

Saya **DANIE DANIAL BIN MOHAMED SALIM**
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknikal Malaysia Melaka
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

| | | |
|---|---|---|
| _____ | SULIT | (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972) |
| _____ | TERHAD | (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ badan di mana penyelidikan dijalankan) |
| __/__ | TIDAK TERHAD | |

(TANDATANGAN PENULIS)

Alamat tetap: No 2 Jalan MP 11,
Melaka Perdana Resort Homes,
75450 Ayer Keroh,
Melaka

Tarikh : 29/8/2012

(TANDATANGAN PENYELIA)

DR SHEKH FAISAL BIN ABDUL LATIP

Nama Penyelia

Tarikh : 29/8/2012

# IMPLEMENTATION OF SECURE CONFIDENTIAL-DOCUMENT TRANSFER AND STORAGE

DANIE DANIAL BIN MOHAMED SALIM

This report is submitted in partial fulfilment of the requirements for the Bachelor of Computer Science (Software Development)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2012

# DECLARATION

I hereby declare this project report entitled

**IMPLEMENTATION OF SECURE CONFIDENTIAL-DOCUMENT TRANSFER AND STORAGE**

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

STUDENT : _____ Date: 29/8/2012

(DANIE DANIAL BIN MOHAMED SALIM)

SUPERVISOR : _____ Date: 29/8/2012

(DR SHEKH FAISAL BIN ABDUL LATIP)

# DEDICATION

To my beloved parents, Mohamed Salim Abbas and Faziah Omar

To my supervisor, Dr.Shekh Faisal Bin Abdul Latip

To my sisters and brothers

To my cooperative friends

## ACKNOWLEDGEMENTS

Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project which is titled Implementation of Secure Confidential-Document Transfer and Storage. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), basically for student in final year to complete the undergraduate program that leads to the degree of Bachelor of Computer Science. This report is based on the methods given by the university.

Firstly, I would like to express my deepest thanks to my supervisor, Dr Shekh Faisal Bin Abdul Latip for the inspirational instruction and guidance to me during this project. His guidance helped me in all the time in my project. I could not have imagined having a better supervisor for my project.

Deepest thanks and appreciation to my parents, siblings, and friends for their cooperation, encouragement, constructive suggestion and full of support for the report completion, from the beginning till the end.

## ABSTRACT

This project describes the development of a system which main objectives are to enhance the security and efficiency of the current system of file sharing and message sharing process. This idea of implementing a system that employs a client-server architecture which involves a certificate authority (CA), which acts as a server to issue a digital certificate and monitor all the client activities, and a client that uses encryption technology in order to secure the content of the message and the files, came up after studying the outdated and unsecure method of UTEMs process of vetting exam question paper.

For this project, the development focused on the client side. The client side will use a face recognition, which will be authenticated by the server. The client will use AES algorithm and RSA algorithm in encryption the messages or files before sharing or distributing the messages/files to other client. Each user will have their own digital certificate, issued by the certification authority. User can use the client to search for other online or offline user, validate their digital certificate and even send an offline message. The client also features a separate decrypting tools to decrypt received files at any time.

The interfaces and buttons will attempt to replicate the design and styles of commercial system. The design also will be developed and focused primarily to promote user friendly. This project will be developed in such a way that I can be run even using low hardware and software specification, so that I can be run by most computer. The system will be developed using VB.net languages, luxandFace SDK, and developed for Windows environment.

# ABSTRAK

Projek ini menerangkan prose pembangunan sistem dimana objektif utamanya adalah untuk meningkatkan keselamatan dan kecekapan sistem semasa proses perkongsian fail dan perkongsian mesej. Idea untuk melaksanakan satu sistem yang menggunakan seni bina client-server yang melibatkan *certification authority* (CA), yang bertindak sebagai pelayan untuk mengeluarkan *digital certificate* dan memantau semua aktiviti *client*, dan *client* yang menggunakan teknologi *encryption* untuk menjamin kandungan mesej dan fail-fail tersebut, timbul selepas mengkaji kaedah yang ketinggalan zaman dan tidak selamat, yg digunakan oleh UTEMs dalam proses *vetting* kertas soalan peperiksaan.

Untuk projek ini, focus tertumpu lebih kepada *client*. Bahagian *client* akan menggunakan pengenalan muka, yang akan disahkan oleh pelayan. Pelanggan akan menggunakan algoritma AES dan algoritma RSA dalam penyulitan mesej atau fail sebelum berkongsi atau mengedar mesej / fail kepada pelanggan lain. Setiap pengguna akan mempunyai *digital certificate* mereka sendiri, yang dikeluarkan oleh *certification authority*. Pengguna boleh menggunakan klien untuk mencari pengguna lain secara online atau offline, mengesahkan *digital certificate* masing-masing dan juga menghantar mesej *offline*. *Client* juga mempunyai fungsi yang berasingan, iaitu alat decrypting untuk menyahsulitkannya yang fail diterima pada bila-bila masa.

*Interface* dan butang akan cuba direka dengan meniru reka bentuk dan gaya sistem komersial. Reka bentuk juga akan dibangunkan dengan memberi tumpuan untuk mempromosikan mesra pengguna. Projek ini akan dibangunkan supaya boleh berfungsi walaupun menggunakan perkakasan yang rendah dan spesifikasi perisian, supaya ianya boleh dikendalikan oleh kebanyakkan komputer. Sistem ini akan dibangunkan dengan menggunakan VB.NET, luxandFace SDK, dan dibangunkan untuk persekitaran Windows.

# TABLE OF CONTENT

**CHAPTER II LITERITURE RIVIEW AND PROJECT METHODOLOGY**



**CHAPTER III ANALYSIS**

**CHAPTER VII PROJECT CONCLUSION**

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| ABBREVIATION | WORD/DESCRIPTION |
|---|---|
| DFD | Data Flow Diagram |
| DDL | Data Definition Language |
| ERD | Entity Relationship Diagram |
| UTeM | Universiti Teknikal Malaysia Melaka |

# LIST OF ATTACHMENTS

# CHAPTER I

# INTRODUCTION

## 1.1 Project Background

Everybody needs a sense of security and privacy in their life. This is the basic needs of human. This basic need also apply in the IT and cyber world. As an individual, we need to secure anything that is private and personal to us. As an organization, it is essential that sensitive data being protected. A breach of such security and privacy could result in safety concern, and loss in terms of profit for organization. That is why we need to secure anything that is important and private to us.

Encryption is one of the most effective methods to secure a files or application. This process of encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a difference form.

Key-based algorithms use an Encryption key to encrypt the message. There are two general categories for key-based Encryption: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys – a public key to encrypt the message, and a private key to decrypt it. Currently, there are several types of key based Encryption

algorithms such as: HASH, RSA, AES, BLOWFISH, RC6, and others but all of these algorithms depend on high mathematical manipulations.

In this project, a secure classified-document transfer and storage application will be developed, to address the problem of security attack and security flaw, and provide a secure method of sharing and storing classified documents.

## 1.2 Problem Statements

Security and privacy has been considered a basic need for human. It is crucial to protect individual or organization privacy and sensitive as failure to do so might cause trouble, problem and even crimes involving theft, fraudulence, and industrial spying. However, the current culture and society still take security issue for granted. Most individual and organization only employed and implemented minimum security measure at most, and the rest are still ignorance on issue related to security and privacy. The majority of business and educational institution are still using paper based submission, which is very unsecure way of circulating or transmitting sensitive and private information. To address this problem, most has already adopted a system that can send the soft-copy of the private files or messages, over the network, such as LAN or WAN. But still this method are not considered as a safer alternative as the files and messages can still be intercepted or sniffed. Message wrote in a plain-text format can easily be sniffed and read using Wireshark, a network monitoring tools that are available on the internet, free for download. File that was intercepted can readily be run or opened. Without applying an encryption on these messages or files, there is no use in migrating from paper-based system to computerized network based system.

Furthermore, with the current method or system, there is no way to be sure that there is no impersonation occur, which means that the person we are communication with are no an impersonator. There is also no effective way to ensure the integrity of the message, and proof of origin (non-repudiation). If there is a dispute, a complication will arise because the sender can deny the content of the message or even deny having sent it.

In short, the current method of sharing and sending classified information or files have no:

- Confidentiality to prevent unauthorized disclosure or information.
- Integrity to prevent unauthorized modification or substitution of information.
- Availability which prevent unauthorized withholding of information or resources (denial of service)
- Non repudiation, to avoid sender from deny the content of the message or even deny having sent it

## 1.3 Objectives

There are four main objective of the project. They are:

- To develop an application that is capable of sending and storing files/message securely by means of encryption technology.
- To provide the application with better security by implementing biometrics-face recognition login
- To ensure the developed software is user-friendly, practical and lightweight.

## 1.4 Scope

- Encryption Algorithm

- For this project, only block cipher encryption will be implemented. The encryption algorithm are Advanced Encryption Standard (AES) or rijndael algorithm and RSA algorithm.

- Stream cipher will not be use, as it is deemed unsuitable for this project

- This project will not explore or analyze these algorithm and its mathematical formulae in details.

- Environment

- This application is intended to be used on windows operating system environment, and this project will on limits its scope on window environment.

- Workstation

- This application is intended to be use on computer, laptops and netbook. Therefore this project will not cover on its usability, or guarantee its stability in other device such as mobile phone or tablet pc.

- Digital Certificate and Certification Authority

- Although this application rely on digital certificate to accomplish its objectives, this project do not cover on the subjects of generation of the asymmetric key (private/public key), creation of digital certificate, and its distribution.

## 1.5 Project Significance

The implementation of encryption method in securing messages and files, will surely increased the level of privacy and security of individual or organization. Files and messages can be send and distributed freely without worrying about the content being exposed or sniffed, as the content is encrypted and the cipher text is useless to those who did not know the private key. This will surely increase the productivity and stability of individual or organization.

## 1.6 Conclusion

Security and privacy remains as one of the basic needs of human being. It is also important for large organization and business. To an individual, protecting this means protecting their safety, and to a business organization protecting and security

means protecting their money. Therefore to ensure privacy and security, cryptography is one of the best and practical methods.

That is why protecting and securing files and messages by means of encryption is the main focus of this project, where the software is expected to be simple, user friendly and yet practical and full with features .

In the next chapter, the report will explain about literature review and project methodology used throughout the project. The literature review discusses the domain related to the project.

# CHAPTER II

# LITERATURE REVIEW AND PROJECT METHODOLOGY

## 2.1 Introduction

This chapter will discuss in details on literature review related to the project and also the methodology used in researching and completing the project. The purpose of this chapter is to conduct the research about the other systems or applications that are similar to the system that will be developed. All aspect is studied in order to develop a system that is more effective. Furthermore, the discussion is also including the methodologies, techniques, hardware and software that being used in other research. The comparison between them is analyzed to highlight the differences thus determine the better solutions for this project.

## 2.2 Facts and finding

Approach, passed research, reference and case study will be discussed under this topic. The approach will be supported from a publish materials or passed research.