

IMPLEMENTATION OF SECURE CRYPTOGRAPHIC ALGORITHM FOR
PRESERVING THE SECURE FILE TRANSFER AND CHATTIONG
APPLICATION

MUHAMAD BUDIE BIN BASRI



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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DECLARATION


I hereby declare that this project report entitled
PERFECT CRYPT

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

 **STUDENT** : _____ **Date:** _____
(MUHAMAD BUDIE BIN BASRI)

 **UTeM**

اونيورسيتي تيكنيكل مليسيا ملاك

 I hereby declare that I have read this project report and found
this project report is sufficient in term of the scope and quality for the award of
Bachelor of Computer Science (Software Development) With Honours.

SUPERVISOR : _____ **Date:** _____
(DR. SHEKH FAISAL BIN ABDUL LATIP)

DEDICATION

Dear Allah SWT

I can feel I am blessed with your love once I finished this project as a final year student. Syukur Alhamdulillah

Dear Beloved Family

Thank you because always supporting me in every part such giving me motivations ideas and accompany me while I am doing this project

Dear Supervisor and Lecturer

Thank you all your guidance, patience, encouragement, and supervision to enable me finish this project

Dear Friends

Thank you for all the knowledge, support and encouragement and share all the knowledges together.



ACKNOWLEDGEMENTS

I would like to thank Allah SWT for giving me ideas, strengths, knowledge and good health that help me finish this project

I would like to thank to my beloved supervisor DR. SHEKH FAISAL BIN ABDUL LATIP for her guidance, constant patience, excellent support, motivation and continuous understanding throughout this semester of my Final Year Project in Universiti Teknikal Malaysia Melaka (UTeM).

I would also like to dedicate my appreciation to my beloved mother, Sharizan binti Samah and also my entire family that always support me with their love and gives motivation to finish this project.

Lastly, I am thankful to all my colleagues and friends for their understanding, suggestions and comments throughout this project, which made my final year memorable.

ABSTRACT

This project is to provide the secure file transfer encryption Java Application. This project consists of two application which is one application for server and another one application is for client. Client can send file to desire sender by uploading the file to the server. The file can want to be sent is the encrypted file that been encrypted by various of encryption method that been choose by the user itself. RSA has been chosen for key exchange and encryption of secret key if the encryption method that user choose is the symmetric encryption techniques. Nowadays, the transaction of transferring file has become widely use in daily working life in the organisation such as government agencies, and non – government organisation. These organisations using the file transfer and chatting between their staff every day. The most concern is how best the protection of their confidentiality of the sensitive data that transfer across the network. The problem is the secrecy and confidentiality of the sensitive information in organisation not well preserve. In additional, the integrity of the data in organisation not protected. Finally, the authentication of the message and file transfer in organisation not well authentic. The objective of this to develop the secure platform for user to encrypt and decrypt their files and message. Furthermore, to preserve the integrity of the file that transmitted in organisation. Another objective of this project is to provide the authentication method for organisation to authenticate the user, file and message. This project methodology is the Object-oriented approach. The methodology can be used because it provides the conceptual structure that assist to deal with the modelling the information system including development of its sub-system. The significant contributions for this project is the highly secure file transfer encryption platform for user to transfer and communicate with another user.

ABSTRAK

Projek ini adalah untuk membangunkan aplikasi pemindahan fail yang selamat menggunakan Java. Projek ini terdiri daripada dua aplikasi iaitu satu aplikasi untuk pelayan dan lagi satu aplikasi kepada pelanggan. Pelanggan boleh menghantar fail untuk keinginan penghantar dengan memuat naik fail ke pelayan. Fail yang ingin dihantar adalah fail dienkripsikan yang telah dienkripsikan oleh pelbagai kaedah penyulitan yang telah dipilih oleh pengguna itu sendiri. RSA telah dipilih untuk pertukaran kunci dan penyulitan kunci rahsia jika pengguna memilih kaedah penyulitan adalah teknik penyulitan simetri. Pada masa kini, transaksi pemindahan fail telah menjadi meluas digunakan dalam setiap hari persekitaran kerja dalam organisasi seperti agensi kerajaan, dan bukan organisasi Kerajaan. Organisasi berkenaan menggunakan pemindahan fail dan berbual-bual antara kakitangan mereka setiap hari. Kebimbangan yang kebanyakan adalah cara terbaik melindungi kerahsiaan data sensitif yang dipindahkan di seluruh rangkaian mereka. Masalahnya ialah kerahsiaan dan kerahsiaan maklumat yang sensitif di organisasi tidak dirisaukan. Dalam tambahan, integriti data dalam organisasi tidak dilindungi. Akhirnya, pengesahan pemindahan mesej dan fail dalam organisasi tidak juga sah. Objektifnya untuk membangunkan satu platform yang selamat untuk pengguna untuk menyulitkan dan menyahsulitkan fail dan mesej mereka. Selain itu, untuk mengekalkan integriti fail yang dihantar dalam organisasi. Satu lagi Objektif projek ini adalah untuk menyediakan kaedah pengesahan bagi organisasi untuk mengesahkan pengguna, fail dan mesej. Metodologi projek ini ialah pendekatan yang berorientasikan objek. Kaedah yang boleh digunakan kerana ia memberikan struktur kepada konsep yang boleh membantu untuk berurusan dengan pemodelan sistem termasuk pembangunan sistem sub. Sumbangan ketara bagi projek ini adalah satu platform penyulitan pemindahan fail sangat selamat untuk pengguna untuk memindahkan dan berkomunikasi dengan pengguna lain.

TABLES OF CONTENT

CHAPTER I	12
INTRODUCTION	12
1.1 Background Study	12
1.2 Problem Statement	14
1.3 Project Question	15
1.4 Project Objective	16
1.5 Project Scope	16
1.6 Expected Output	17
1.7 Report Organisation	17
1.8 Summary	18
CHAPTER II	19
LITERATURE REVIEW	19
2.1 Introduction	19
2.2 Desktop Application	20
2.2.1 Revolution of Desktop Application	20
2.2.2 Development Technology of Desktop Application	21
2.2.3 Client Server	22
2.2 Cryptography	23
Definition of Cryptography	23
Security Services of Cryptography	25
Type of Cryptosystem	25
Type of the Cipher Method	28
Type of Encryption Program	44
Definition of the file sharing	45
Types of the File Sharing	45
File Sharing and Network Architecture	46
2.4 Chat Application	49
Definition of Chat Application	49
Architecture of the Chat Application	49
CHAPTER III	52
PROJECT METHODOLOGY	52

3.1 Introduction	52
3.2 Object Oriented Approach.....	53
Inception Phase	54
Elaboration Phase	54
Construction Phase	55
Transaction Phase	55
3.3 Project Schedule and Milestones.....	55
Flow Chart of Project.....	56
Gantt Chart of Project	57
Milestone of Project.....	57
3.4 Summary	58
CHAPTER IV	59
ANALYSIS AND DESIGN.....	59
4.1 Introduction	59
4.2 Problem Analysis	60
4.3 Requirement Analysis	62
4.3.1 Data Requirement	62
4.3.2 Functional Requirement.....	71
4.3.3 Other Requirement.....	72
4.4 High-level Design.....	74
4.4.1 System Architecture.....	74
4.4.2 User Interface Design.....	75
4.4.2.1 Navigation Design	76
4.4.2.2 Input Design.....	77
4.4.3 Database Design	88
4.5 Detailed Design	89
4.5.1 Software Design.....	89
4.6 Conclusion.....	95
CHAPTER V.....	96
IMPLEMENTATION	96
5.1 Introduction	96
5.2 Development Environment Setup	96
5.2.1 Environment Layout	97
5.2.2 Development Server Specification	97
5.3 Software Configuration Management	99

5.3.1 Configuration Environment Setup	99
5.3.2 Version Control Procedure	100
5.4 Implementation Status	100
5.5 Conclusion	103
CHAPTER VI	104
TESTING	104
6.1 Introduction	104
6.2 Test Plan	105
6.2.1 Test Organisation	105
6.2.1 Test Enviroment.....	105
6.2.2 Test Schedule	106
6.3 Test Strategy	107
6.2.1 Functionality Test	107
6.3.2 Alpha Testing	108
6.3.3 Integration Testing	108
6.4 Test Design	108
6.4.1 Test Description	109
6.4.2 Test Data	109
6.5 Test Result and Analysis	110
6.6 Conclusion	111
CHAPTER VII	112
CONCLUSION	112
7.1 Introduction	112
7.2 Project Summarization	113
7.3 Project Contribution	114
7.4 Project Limitation	114
7.5 Future Works	115
7.6 Conclusion	115
APPENDIX	116
REFERENCES	117

LIST OF FIGURES

Figure 1 : Number of Breach	13
Figure 2 : Framework for Literature Review	19
Figure 3 : Inter-process among client and server	23
Figure 4 : Symmetric Encryption and Decryption Process	26
Figure 5 : Asymmetric Encryption and Decryption Process.....	26
Figure 6 : Hash Function Process	27
Figure 7 : Message Authentication Code	27
Figure 8 : Digital Signature Signs and Verification.....	28
Figure 9 : Function F of DES	30
Figure 10 : DES Encryption Procedure.....	31
Figure 11 : 3DES Encryption Process.....	32
Figure 12 : RSA Encryption and Decryption Process.....	33
Figure 13 : AES Encryption and Decryption Process.....	34
Figure 14 : Blowfish F-function.....	36
Figure 15 : First Round of the Two Fish.....	37
Figure 16 : Blowfish Encryption Process.....	38
Figure 17 : Threefish-1024 One Round of Encryption.....	39
Figure 18 : Diffie-Hellman Exchange Key Method.....	40
Figure 19 : Trivium Phase.....	41
Figure 20 : MD5 Process.....	43
Figure 21 : SHA Process	44
Figure 22 : The original Napster P2P architecture	47
Figure 23 : Gnutella / FastTrack Peer-to-Peer Architecture	48
Figure 24 : Client-Server Communication	50
Figure 25 : Peer - to - Peer Communication	51
Figure 26 : Phase of Rational Unified Process.....	53
Figure 27 : Flow Chart of the System	56
Figure 28 : Gantt Chart	57
Figure 29 : Flow chart of the proposed system	61
Figure 30 : Data Flow Diagram	71
Figure 31 : System Architecture	75

Figure 32 : Client User Interface Navigation.....	76
Figure 33 : Server User Interface Navigation	76
Figure 34 : Perfect Crypt Login Screen	77
Figure 35 : Client User Dashboard Screen.....	78
Figure 36 : Client Add Friend Screen	79
Figure 37 : Client Send Files Screen.....	80
Figure 38: Client Download File Screen.....	80
Figure 39 : Client Decrypt File Screen	81
Figure 40 : Send Message Screen	81
Figure 41 : Forgot Password Screen	82
Figure 42 : Server Administrator Login Screen.....	83
Figure 43 : Server Administrator Dashboard Screen	83
Figure 44 : Manage Branch Screen	84
Figure 45 : Add Branch Screen	84
Figure 46 : Edit Branch Detail	85
Figure 47 : Manage User.....	86
Figure 48 : User Registration Screen	87
Figure 49 : Start RMI Server.....	87
Figure 50 : Entity-Relational Diagram.....	88
Figure 51 : DFD Registration.....	89
Figure 52 : DFD Login.....	90
Figure 53 : DFD Encrypt File	91
Figure 54 : Decrypt File	92
Figure 55 : Sign Digital Signature	92
Figure 56 : Verified Digital Signature	93
Figure 57 : Message Transection	94
Figure 58 : Forgot Password	95
Figure 59 : Generate Master Key	95
Figure 60 : Environment Layout	97
Figure 61 : Testing Organisation	105
Figure 62 : Test Environment	106
Figure 63 : Test Design	109
Figure 64 : Test Result	110

LIST OF TABLES

Table 1 : Project Problem Statement.....	15
Table 2 : Project Question.....	15
Table 3 : Project Objective.....	16
Table 4 : Milestone Project	57
Table 5 : Registration Data Requirement.....	62
Table 6 : Data Requirement Login.....	63
Table 7 : Data Requirement Sending File	63
Table 8 : Data Requirement Sending Chat.....	64
Table 9 : Data Dictionary for pc_adm_user.....	65
Table 10 : Data Dictionary Data Information	68
Table 11 : Data Dictionary User Friends	69
Table 12 : Data Dictionary for pc_message.....	70
Table 13 : Software Requirement	72
Table 14 : PC Specification.....	73
Table 15 : Development Server Specification	98
Table 16 : Development Machine Specification.....	99
Table 17 : Implementation Status	101
Table 18 : Test Schedule	106

CHAPTER I



1.1 Background Study

Nowadays, technology evolve from communicate with telegram until now can communicate with computer and smartphone. As technology emerged, people nowadays no longer used the manual method to send data to another person. Instead, they will use the internet to share any information including the sensitive file and the confidential data without hesitation. From these act, it led to the rising of the data breaches activity. Data breach is an incident of the sensitive, protected or confidential data has stolen and view by the unauthorized person. From year 2004 until 2016 the data breaches activity rapidly increase and the highest method of the leak is by hacked. There are few the most popular and the highest loss record in history of the data breach attack. First is Adult FriendFinder with the loss record of 412,214,295 and the type of

breach is the Account access. The Internet-based, adult-oriented social network and online dating service was hit with an account access data breach by a malicious outsider that exposed over 400 million records. The breach scored the max of 10 on the risk assessment scale. The hacked database includes customers' e-mail addresses, IP addresses last used to log-in to the site, and passwords, according to Ars Technica. Second is in year 2014, Yahoo has reported been hacked and loss record about 500,000,0000. Type of the information is names, email addresses, telephone numbers, dates of birth, hashed passwords and encrypted and unencrypted secret answer and question.

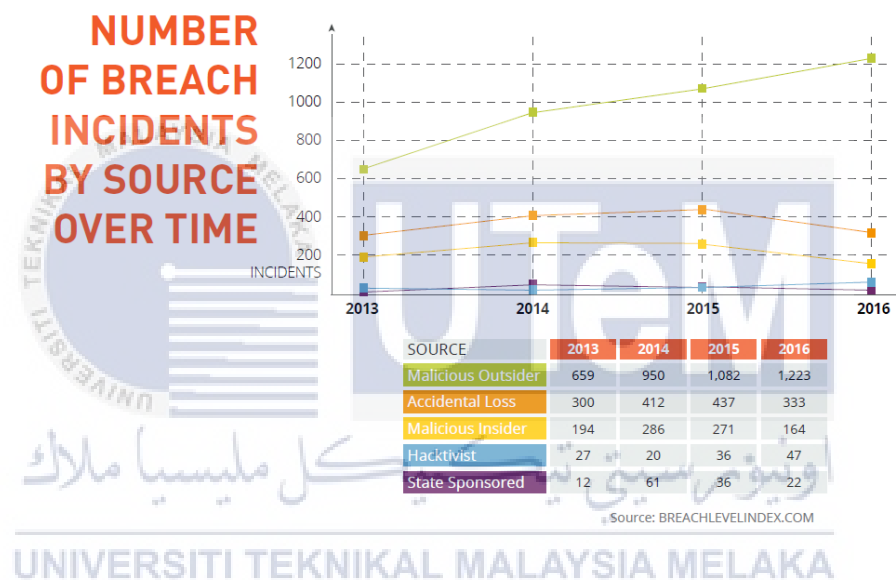


Figure 1 : Number of Breach

Based on Figure 1.1 the number of breach from the malicious outsider keep increasing each year. From 2013 only 659 incidents and increasing to 950 incidents in year 2014. In 2015, the number of the incidents is keep increasing to four number value, 1,082 incidents and for the 2016, the number of the incidents of the data breach that made by malicious outsider is 1,223 incidents. Other source also increasing from year 2013 to 2015 but decreasing the number of incidents in 2016.

In the age with consider advance technology, people tend to make their transaction via internet which is a lot easier compare to manual method. For example, one of the government agency worker want to give the confidential data to another worker through the internet. This behaviour is will led to the man-in-the-middle attack. Unauthorize person can retrieve the data and modifier before send back to the correct receiver. According news netcraft, only 5% of HTTPS server vulnerable to trivial Man-in-the-middle attack. Based on this statement, the man-in-the-middle attack can easily be done by attack via the HTTP server. HTTP is the protocols that people using all day from get the information to transferring the secretive and sensitive information. Attacker can easily intercept the user data transmission to server and get the data. Attacker also can made the fake of the web page to gather user information for their own intention.

By developing a secure transfer platform by implementing the cryptographic will help the reduce the number of attack for man-in-the-middle and decrease the number of the data breach. Cryptography is defining as a technique to disguise information in such way that its meaning is unintelligible to an unauthorized person. Cryptography will protect the sensitive data from fell down to unauthorize user by using the encryption but the encryption cannot protect the integrity and non-reputation of the information. Hence the Digital Signature and Message Authentication Header will be using in order to the information that transmitted are protected.

1.2 Problem Statement

The sensitive and confidential user information can be retrieve easily by the hacker. Thus many cases where the user information fell into wrong hand and using for the bad intention and being used to ransom, bring down a company and many more cybercrime activities.

Table 1 : Project Problem Statement

No	Problem Statement
PS1	The secrecy and confidentiality of the sensitive information in organisation not well preserve
PS2	The integrity of the data transfer in organisation are not protected
PS3	The authentication of the message and file transfer in organisation not well authentic

1.3 Project Question

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

Table 2 : Project Question

PS	PQ	Project Question
PS1	PQ1	How can we preserve the secrecy and confidentiality of the sensitive information in organisation?
PS2	PQ2	How can we protect the integrity of the transmitted data in organisation?
PS3	PQ3	How can we authenticate the message and file transfer in organisation

1.4 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 3 : Project Objective

PS	PQ	PO	Project Objective
PS1	PQ1	PO1	To develop the secure platform for user to encrypt and decrypt their files and message
PS2	PQ2	PO2	To preserve the integrity of the file that transmitted in organisation
PS3	PQ3	PO3	To provide the authentication method for organisation to authenticate the user, file and message

1.5 Project Scope

The scope for this project are:

- i. Secure the file and message that transmitted across the network by implementing the cryptography
- ii. The implementation is made in the File Transfer and Chat Application of Java application

1.6 Expected Output

The expected output by the end of this project us to provide the Secure Client and Server Encryption File Transfer Platform for user can transfer their files and message to other person by the publishing the Perfect Crypt (The Secure Encryption File Application)

1.7 Report Organisation

Chapter 1: Introduction

Introduction chapter described about the definition, background study, objective, problem statement, scope and expected output of the project in detail

Chapter 2: Literature Review

This chapter review, described about the literature review of the project that included the desktop application, cryptography, file transfer system and the chat application.

Chapter 3: Methodology

In this chapter, the decision of the method that want to use in project development will be explained.

Chapter 4: Analysis and Design

This chapter will explain about the problem analysis, requirement analysis that contain the data requirement, functional requirement and other requirement. High level design also will be explained in this chapter which is contain the system architecture, user interface design, navigation design ,input design and database design. Next the detail design of the project also will be explain in this chapter.

Chapter 5: Implementation

This chapter will be discussing about how the project implemented. This chapter consist of development environment setup which is included the environment layout and development server specification. Software configuration Management also will be stated in this chapter that consist of configuration environment setup and version control procedure. Next, the implementation status of the project also explained in this chapter.

Chapter 6: Testing

This chapter explained how the testing and the testing structure of the project. This chapter consist of test plan, test organisation that include test environment and test schedule, test strategy, test design and test result.

1.8 Summary

This section is elaborate about the introduction of the project that included background study, problem statement, project question, project objective, project scope, expected output and report organisation in details. Background study explain data breaches incidents across the world and the man-in-the-middle attack that happen now days which is triggering to develop this project as one way to reduce the dangerous threat. Problem statement explained the problem that faced by the user as the individual or the organisation about the securing the information that transmitted across the network from attacker. Next, the project question based on the problem statement and the project question also become the question for the project objective. Project objective is the answer from the project question and the objective of the project that must be achieve in the end of the project. Project scope are explained about what the element that been covered in this project and the limitation of the project. In additional, the expected output explained the last outcome of this project which publishing the Perfect crypt for organisational used. Last but not least is the report organisation briefly explain all the chapter covered in the report.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In previous chapter, the main point like problem statement, objective, and scope has been discussed. This chapter is about the literature review of the project. The literature review are based on the journal, book, and other reliably resources.

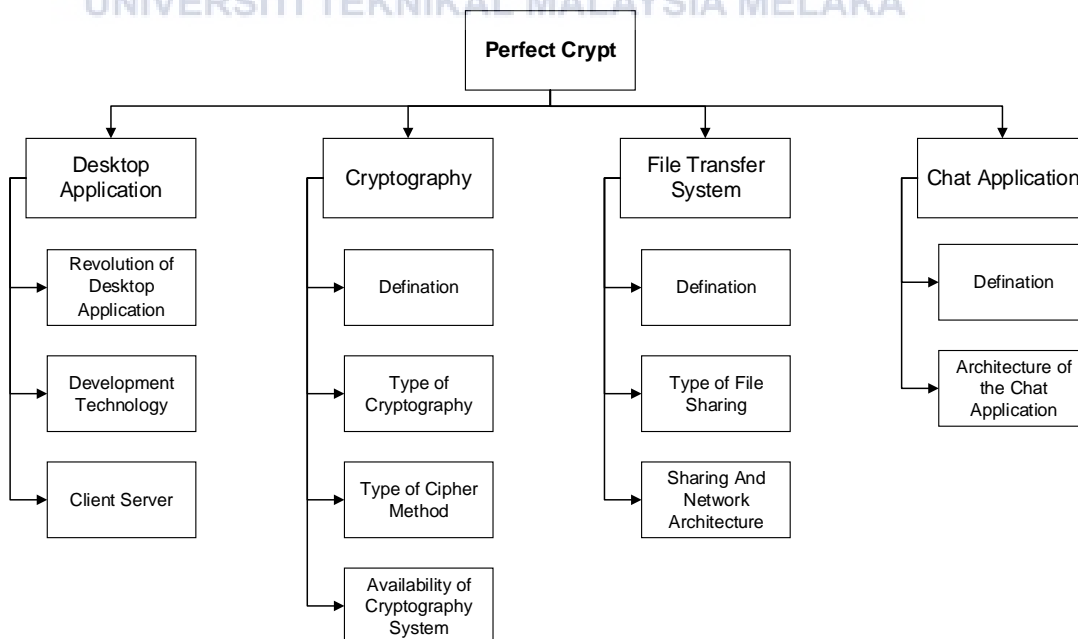


Figure 2 : Framework for Literature Review

2.2 Desktop Application

In this section contain the revolution, development platform, open technology and client server of the desktop application. By the end of the section, there are the analysis will be done.

2.2.1 Revolution of Desktop Application

From the past several decades, evolution of the computer is changing rapidly. From the computer only support for console to the astonishing graphical user interface of the computer. This evolution also lead the revolution of the desktop application. In early 1980, Microsoft are released the first Operating System that called MS-DOS and after several year later, Apple are launching the first commercial computer that support the graphical user interface are the starting point of the revolution of desktop application. The revolution of the desktop application radically fast because of the competition between various tech company like Apple and Microsoft to provide the best environment to the user from their Operation System Windows for Microsoft and Mac OS for Apple. Not to mention, the open source community also boost the revolution of the Desktop application via Linux Platform.

The definition of desktop application means any software that can be installed on a single computer and used to perform specific tasks. Some desktop applications can also be used by multiple user in a network environment. Desktop application has specific platform that can be run or written. Some of the desktop application are only be written on specific operating system only.

Even though, the rise of the web application technology and the rise of the smartphone application, the desktop application still the strong choice for development of application because of security. Desktop application are providing more security to the user because of the standalone characteristic of the application. With desktop application, the risk of the attack are breaches are much lower compare to web

application and mobile application. Desktop application also provide a provide a rich user interface and adapt depending on what the user types in.

2.2.2 Development Technology of Desktop Application

The platform of the Desktop Application is referred to the Operating System platform. The most popular platform is included Windows, Mac OS, Linux and UNIX..NET framework is a huge class library that provide language that can be operate, running and execute with several programming language such as C#, Virtual Basic. Everything that cooperation with .NET framework will have the .NET extension at their name such as ASP.NET for web application development. This framework is more focus on Windows Machine Application because of it developed and maintained by Microsoft. Programs that develop by .NET framework will executed in Common Language Runtime (CLR). CLR is the virtual machine that give the security, exception handling and memory management

The software environment called as Common Language Runtime is the .NET Framework programs. CLR is the application virtual machine that provides a ton of services for software running the machine. Most of the services is security of the program, memory management and last but not least is exception handling.

Another part of .NET framework is Framework Class Library(FCL). From user interface, network communications, web application development, cryptography, data access, numeric algorithms and database connectivity are provided by FCL. Usually, to develop the software by using .NET framework, programmer can merge their source codes with .NET Framework and other libraries. .NET Framework is used to develop the software that running on Windows Platform by using tools like Visual Studio. Visual Studio is the Microsoft Integrated Development Environment (IDE) for developing the Windows based software application.

Another platform that can be used to develop the desktop application is by using Java platform. Java application is can be run on any of operating system that Java supported. All the java language code will compile to the java virtual machine

that install in operating system. To develop the java application, the important tools that programmer need is the Java Development Kit (JDK) to compile and debugging the Java language code and Java Runtime Environment (JRE) to run the compiled program in any Operating System. JRE also known as Java Virtual Machine (JVM).

JVM has access to all the Operating System services. For example, the network access and disk Input/Output. With this architecture, java application not directly using the system services instead JVM that make it java application accessing the security services. This setup allow user with system services and access should be allow for Java application from access.

Right now, all Java desktop program can run on almost all operating system from Windows, MacOS, Linux and to UNIX based operating system. For mobile applications, browser plugins are used for Windows and Mac based devices, and Android has built-in support for Java. There are also subsets of Java, such as Java Card or Java Platform, Micro Edition, designed for resource-constrained devices. (“Advanced Desktop Application Development on the NetBeans Platform,” 2012)

2.2.3 Client Server

The famous and widely known the client-server become more popular and being using every day for different application. The protocols that being standardized by several authorities organisation and government will rapidly increasing the usage of this method. The protocols like File Transfer Protocols(FTP), Simple Mail Protocol (SMTP) and Hypertext Transfer Protocol (HTTP) is among the protocol that being standardized and support the client server application. The client-server modal are consist at least one server and one client. These two has to cooperate each other to serve the best performance to the user. Client usually only can request and retrieve the data from server. Client also provided the friendly graphical user interface. Server can listen the request, processes the request and give back the requested data from client to server. In additional, one server can listen from many client not only just one client at one time.

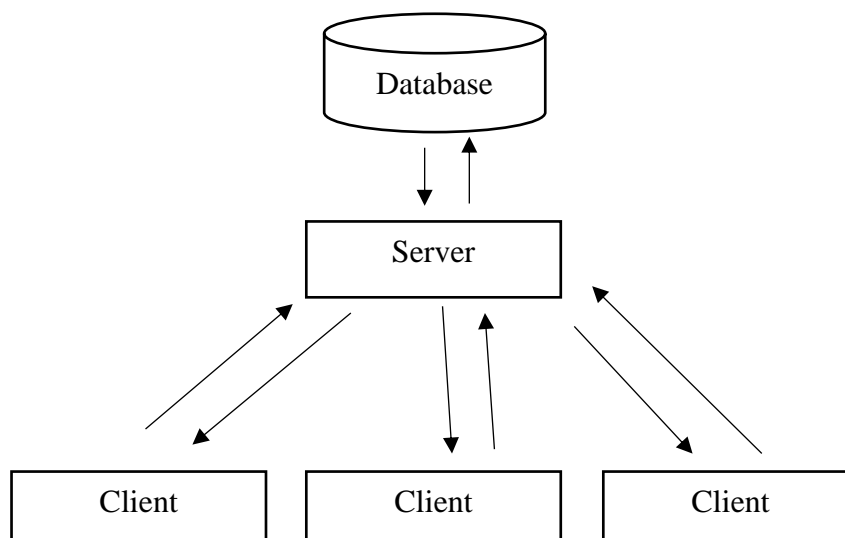


Figure 3 : Inter-process among client and server

Figure above has show the basic integration between client, server and database server. Client will send all the data to the server. Server responsible to process the data and insert into database server. When client request the data from database server, the client will sent request of the data to the server and server will retrieve the data from database server. Server will process the data and send back to requestor client.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
 اونیورسیتی تکنیکل ملیسیا ملاک

2.2 Cryptography

In this section, the definition, history, principle of modern cryptography and technique and algorithm of the cryptography are detailed describe and analysed.

Definition of Cryptography

The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.” (Katz, 2014). This definition might be generally exact, yet it does not catch the quintessence of the modern cryptography. First at all, the definition