Universiti Teknologi MARA

Securing Cloud Storage by Applying File Encryption Software using AES Encryption Technique

Mohd Shafrul Izzuddin Bin Mohd Saharuddin

Thesis submitted in fulfilment of the requirements for Bachelor of Computer Science (Hons.) Data Communication and Networking Faculty of Computer and Mathematical Sciences

July 2020

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thanks to my supervisor, Kamarul Ariffin Bin Abdul Basit who had guide of me and give me some tips on doing this project. I'm really grateful that he helped me with share all the information that he has and provide good guidance.

Special appreciation also goes to my beloved parents Mohd Saharuddin Bin Sis and who had given support to finish my project. Without them I will be lost and could not finish my project in time.

Last but not least, I would like to give my gratitude to my dearest friend for their support in finishing this project. My friend had given me guidance and tolerance to finish project.

ABSTRACT

This paper reviews vulnerabilities on cloud storage from the anonymous such as MITM or DDOS Attack and the solution on how to secure the data of the user when upload to cloud storage. To answer this question, encryption is the suitable method that relevant and can be use of by applying before uploading to cloud storage. The encryption will encrypt the file before upload to the cloud storage. The results revealed that file successfully encrypt and cannot be previewed before it is decrypted. From a safety perspective, this study emphasizes the need to consider the impact of these environmental changes along with the expert's adaptive capacities. The features also can be invented depends on the issue that happen.

TABLE OF CONTENTS

CONTENT

SUPERVISOR APPROVAL ..... **ii**

STUDENT DECLARATION ..... **iii**

ACKNOWLEDGEMENT ..... **iv**

ABSTRACT ..... **v**

TABLE OF CONTENTS ..... **vi**

LIST OF FIGURES ..... **ix**

LIST OF FIGURES ..... **x**

LIST OF TABLES ..... **xi**

LIST OF ABBRIVATIONS ..... **xii**

CHAPTER 1 ..... **1**

1.1 Introduction 1

1.2 Background of study 1

1.3 Problem Statement 1

1.4 Project Aim and Objectives 2

1.4.1 Project Aim 2

1.4.2 Objectives 2

1.5 Project Scope 2

1.6 Project Significance 2

1.7 Summary 3

CHAPTER 2 ..... **4**

2.1 Introduction 4

2.2 Overview of the Cloud Computing 4

2.2.1 Cloud Storage 4

2.2.2 Issues and Challenges 6

2.3 Techniques in the Cloud Storage 13

2.3.2 Encryption 14

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cloud storage is a new platform to store the data as the user will less use of physical storage. The cloud storage can be said to be secured but not the transmission of the data where they will be an attacker can steal the data. Using the encryption, it will mitigate any possibility come from the attacker to steal the data.

1.2 Background of study

The storage and the purpose are to store the data or any similar files. Usually, people want to keep the data as much as it can in the storage weather it is the confidential information or raw data. Leading to the modern age , people want to use something in virtual and do not need or reduce the use of hardware because it is cheaper

Cloud computing refers to an IT infrastructure pattern where all hardware and software resources are delivered to customers on request via the network in a self-service model, independent of location and application. Regardless of the nature of time and location restrictions, connecting to the cloud for resources can be easily reached through various networks without the use of any complicated hardware facilities.

The problem is that these data are likely to be exploited by the provider or other unauthorized persons. The method that has been used is encryption by applying the algorithm technique where it secured the data at the source user.

1.3 Problem Statement

Personal information can be classified as a sensitive issue when another person knows and use it for their own thus it will feel insecure about it. People prefer to use cloud storage as a medium or platform to store their personal or confidential information. The transmission of data from the cloud server to clients' computers can be stolen which is the Man-In-The-Middle Attack so basically there still a lack of security at the cloud storage. Clients need a guarantee that their data which is stored on the cloud will not be accessed by other clients (Kumari1, Pathak, & Madan, 2017)