COMPARATIVE STUDY ON ENCRYPTION ALGORITHMS IN CLOUD ENVIRONMENT

ASIAH MASTURA BINTI SUHAIMI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2017

ACKNOWLEDGEMENT

In preparing this project, I was in contact with many people, researchers, and academicians. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main supervisor, Assoc. Prof. Dr. Md Asri bin Ngadi for encouragement, guidance, critics and friendship. Without his support and interest, this project would not have been the same as presented here.

My fellow postgraduate students should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance on various occasions. Their views and tips are very useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members too.

ABSTRACT

Cloud computing is the Internet based development and used in computer technology where end users are provided with on demand shared resources, software and information. Security is being a major issue in the cloud computing, and it arise attention for Cloud Service Providers (CSP) and end users. Cloud computing security problem raises suspicions and makes many organizations refuse the idea of using the cloud in storing certain data within the cloud computing, especially data with high confidentiality. In addition, cloud users try to avoid being controlled by the CSPs. To avoid the data and data transmission from attackers, appropriate key management is necessary. Besides that, all the data is virtual and cloud is an open service and using a public network such as the Internet for application and services, which has security issues like authentication data loss. Encryption algorithm is a technique that is used to make data on the cloud secured. The aim of the study is to propose the authentication model using Kerberos technique for cloud environment to provides more security. This model can benefit by filtering the unauthorized access and also to reduce the memory usage of cloud provider against authentication checks for each user. It also acts as the third party between cloud server and users to allow authorized access to the cloud services. In this research, the performance of the algorithm is measured based on the computational and communication time. The performance is compared with three algorithms which are RSA, DSA and AES. Result experiment shows that RSA is performing much better than DSA and AES in terms of computational time.

ABSTRAK

Pengkomputeran awan adalah pembangunan berasaskan Internet dan digunakan dalam teknologi komputer di mana pengguna akhir berkongsi sumber, perisian dan maklumat. Keselamatan merupakan isu utama dalam pengkomputeran awan, dan ia menimbulkan perhatian kepada Pembekal Perkhidmatan Awan (CSP) dan pengguna akhir. Masalah keselamatan pengkomputeran awan menimbulkan syak wasangka dan membuatkan banyak organisasi menolak idea menggunakan pengkomputeran awan dalam menyimpan data tertentu dalam pengkomputeran awan, terutamanya data dengan kerahsiaan yang tinggi. Selain itu, pengguna pengkomputeran awan cuba untuk mengelak daripada dikawal oleh CSP. Untuk mengelakkan data dan data penghantaran daripada penyerang, pengurusan utama yang sesuai diperlukan. Di samping itu, semua data adalah maya dan pengkomputeran awan adalah perkhidmatan terbuka dan menggunakan rangkaian awam seperti Internet untuk aplikasi dan perkhidmatan, yang mempunyai isu-isu keselamatan seperti kehilangan data pengesahan. Algoritma penyulitan merupakan satu teknik yang digunakan untuk membuat data dalam pengkomputeran awan terjamin. Tujuan kajian ini adalah untuk mencadangkan model pengesahan menggunakan teknik Kerberos untuk persekitaran awan untuk menyediakan keselematan yang lebih. Model ini bermanfaat dengan menapis akses yang tidak dibenarkan dan juga untuk mengurangkan penggunaan memori bagi pembekal awan terhadap penyemakan pengesahan untuk setiap pengguna. Ia juga bertindak sebagai pihak ketiga di antara pelayan awan dan pengguna untuk membolehkan akses yang dibenarkan untuk perkhidmatan awan. Dalam kajian ini, prestasi algoritma diukur berdasarkan masa pengiraan dan komunikasi. Prestasi dibandingkan dengan tiga algoritma iaitu RSA, DSA dan AES. Keputusan eksperimen menunjukkan bahawa prestasi RSA lebih baik daripada DSA dan AES dari segi masa pengiraan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3DES	Triple DES
ABE	Attribute Based Encryption
ABP	Automatic blocker protocol
AES	Advanced Encryption Standard
AS	Authentication Server
CP-ABE	Ciphertext-Attribute Based Encryption
CRL	Certificate Revocation Lists
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
IT	Information Technology
KDC	Key Distribution Center
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
P2P	Peer-to-Peer Network
PKI	Public Key Infrastructure
RC4	Rivest Cipher 4
SaaS	Software as a Service
SHA-2	Secure Hash Algorithm 2
SLA	Service Level Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
TDEA	Triple Data Encryption Algorithm
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
TOTP	Time-based One-Time Password

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing is a model that provides shared processing data and resources to the computer and another devices on-demand. It is also for allowing the network to access configurable computing resources such as storage, server, networks, services and applications. There is also a disruptive technology that has a potential to enhance scaling, agility, availability, collaboration and provides the opportunities to reduce the cost through efficient computing and optimized. Furthermore, it also provides the best feature, but everything or all information through the Internet and there is a chance of attacker to hack the data.

Besides that, the security issues that inherent in the cloud such as data security and network. There are issues that involved in data security such as data confidentiality, data integrity, data authentication and access control. Data authentication is the most important issues in the cloud. An authentication process is to help verify the proof of identities. It is also to ensure that the originality of an electronic document or message is correct and valid. For the data authentication, password and login are compulsory or mandatory that provided by the cloud service provider and the authentication can be used in workgroup and domain.

Once the hacker hacking the password, the hacker gets access and it will affect to authentication where the authentication will be lost and the data or confidential information also can be modified or deleted by unauthorized users. Therefore, an authentication model is proposed based on Kerberos technique, so that it can solve the authentication problem and authorized user can access and get all the resources or services from the cloud provider.

Based on this study, the key management also used where it is the management of cryptographic keys. This key management includes dealing with the storage, exchange, generation, use and replacement of keys. In addition, it also includes key servers, user procedures, cryptographic protocol design, and other relevant protocols. This chapter is separated into a few sections to describe the problem background, problem statement, research questions, aim, scope, objectives and also the contribution of the study.

1.2 Problem Background

Cloud computing is a global issue. Nowadays, many researches are working on this concept so that the serious and private information should be protected from unauthorized access. Besides this issue, the information must be available to all users who are legitimate to use it at any time they want. Improving a secure method of accessing cloud is one of the highest concern issues. Furthermore, there is a large number of organizations use cloud storage for storing the private data, which is controlled by untrusted parties and have many issues regarding the privacy and security that will be occurring. One major issue regarding this is how to secure the confidentiality and privacy of user data, which is shared and used by multiple parties. For providing security the data stored in the cloud, encryption is needed so that only authorized parties having the decryption key can access. Besides that, authentication also one of the issues related which means verifying the truly person who claims to be.

In cloud, entities do not know each other to communicate, so entities need authentication to authenticate each other. In this case, public key infrastructure (PKI) is needed that enable entities to securely communicate on an insecure public network and reliably verify the identity of an entity via digital signatures. Furthermore, it can be said that an authentication is one of the most important issues where it allows only certain user to log in and use the services of a cloud. Authentication is a process to confirm the identity of the user or system before access to the cloud (Veeraragavan and Arockiam, 2016). This process is required to create the password and login. Furthermore, authentication is the part of sensitive issues in the cloud. In the cloud, security is the major issues where all the data coming from the cloud and there are chances for an attacker to hack the data in the cloud (Nashaat and Hossam, 2012).

Although many researches have done on the challenges and improving security issues in the cloud but the solution it is not fully proof. Some of the security concerns that are worthy to maintain are security capabilities discovery, data protection between users a cloud server, and authentication between users and cloud server. There exist many of authentication method that use encryption algorithms and hashing the password such as SSL/TLS, SSH and SHA-2. On the other hand, there are many attacks on the data that can destroy the data on the server. One of the solutions for scattered data on many servers rather than one server still cannot solve the problem because the data is stored in the encrypted mode using an encryption key (Lomte and Dudhani, 2015). Furthermore, the scattered data on the various server is possible to reconstruct the data again but there must be the problem. What will happen if the encryption key lost due to these attacks? So, there is no possibility to decrypt the data again.

Besides that, the security of the data stored is provided through the encryption mode, but what will happen if the encryption key is known by an unauthorized user or third party? Then the attackers will attack the keys and maybe can hack the data (Yaser and Khamitkar, 2013). In this case, access control service and identity should provide access control and identity management to cloud resources for registered process of entities. Such entities can be user or people, software processes or other systems. In order to give a proper level of access to a resource, the identity of an entity should be verified first where the authentication process is needed.

Among all the issues in the cloud, the most important issue is authentication that allowed certain users to log in and use the services of cloud. Many researchers have tried to implement different types of authentication to make the cloud more secure. There are several ways to implement authentication such as graphical, biometric, 3D password and third party authentication. In addition, implement authentication technique in multi-layer, which authenticates the password in multiple layers to access the cloud services (Dinesha and Agrawal, 2012). The other researcher proposed structure provides identity management, mutual authentication, session key creation between the cloud and users (Choudhury *et al.*, 2011). Moreover, another researcher implement SSL/TLS protocol to secure authentication and authorization to cloud at the same time.

1.3 Problem Statement

Cloud computing offers on-demand services to customers with the properties of distributed systems such as unlimited virtual resources, dynamic scalability, web hosting as well as cost advantages for business organizations. Security issues that arise within this cloud environment result in various obstacles from both business and technological perspectives. There is a continuous development of security solutions with lots of challenges for a cloud environment. Furthermore, there are many concerns about security of cloud the most critical issue nowadays is authentication. The problem for cloud providers is the way to manage all users in cloud by giving or register each user using different username and password for logging into the cloud servers and assigns privileges to them and determined what they can perform when they authenticate or login to resource server of cloud. Some authentication that can be implemented for the cloud are still under development stage and there is a big need of transparent and simplified cloud security infrastructure that can provide security authentication services to cloud.

As a solution to this problem, this master project will investigate how to manage authentication in the cloud and propose an authentication model using the Kerberos technique. At the same time, the project will focus on how to deliver those services in a secure manner.

1.4 Research Questions

This research question has been made to support this aim of the study. The following are the research questions of this study:

i. How to develop an authentication model using Kerberos in the cloud?
ii. How to develop key management that prone to the attack?
iii. How to evaluate the performance of the RSA and other algorithms?

1.5 Aim of study

The aim of the study is to compare the encryption algorithms using the Kerberos technique for cloud environments.

1.6 Objectives of study

The followings are the objectives proposed for this study:

i. To develop the key management based on public key infrastructure for cloud using Kerberos technique.
ii. To develop key management that prone to the attack such as replay attack or man in the middle attack.
iii. To evaluate the performance of the RSA with other algorithms in the cloud.

1.7 Scope of study

The scope of this study:

i. Focus on the key management based on the PKI for cloud environments.
ii. Authentication model using the Kerberos technique for cloud environments.
iii. The performance of the RSA with other algorithms in the cloud is evaluated using GridSim simulator.

1.8 Significance of Research

The contribution of this study is to develop and implement an authentication model using the Kerberos technique for cloud environment. In this authentication process, it provides a login and password for the consumers to access into the cloud. But there is the problem in this process where the password can be easily hacked by the attacker or hacker on a public network such as Internet to hijacking the system for bad reasons or without reasons. So to prevent this problem from occurring, the key infrastructure mechanism is used and it is also commonly used in the symmetric and asymmetric algorithm. In addition, Rivest Shamir Adleman (RSA) is the popular one algorithm in asymmetric cryptography and it also uses Kerberos technique.

Key management based on the PKI scheme that allows the storage of and access to encrypted data on different sites within the same cloud according to its importance and frequency of use. Managing the keys in the cloud environment is the important thing in order to provide synchronization for data flow in the network. This is because, the keys are needed for the encryption process in the cloud environment and encryption also is the main thing to ensure the security in the cloud for consumers.

1.9 Report Organization

This report consists of six chapters including Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5 and Chapter 6. In Chapter 1, it explains about the introduction of the proposed project, the introduction includes the overall explanation of the purpose of the project. In addition, it state the problem background of the study, research aim, objectives that is achieved at the end of the study, scope and the research contribution of this study.

Chapter 2 discusses literature review, where it is an introduction of case study and study of the domain from general to specific. In this chapter, it also explains related studies, description of the identified problem, a study of theory and method that can contribute towards solving the problem, justification of chosen theory and method and suggestion to solve the identified problems.

Chapter 3 discusses the methodology. In this chapter, it describes the method of implementing the project, which provide the guidelines to help to conduct the research. Besides that, choices of tools and technique is justified. The performance about this study regarding technique and method used is measured in this chapter.

Chapter 4 describes the design and implementation of authentication model using a Kerberos technique for cloud environments. All the design is explained in the form of figures and flow diagram.

Chapter 5, it is about testing and discussion session where all results is discussed in detail and the figures also provided to show that the output is successfully working or not.

Lastly which is Chapter 6 will summarize the whole project and also discusses the achievements of this project and future works.

REFERENCES

Abhiram V. and Murty S. A New Approach to Data Authentication in Cloud Storage. *International Journal of Science and Research,* 2015. 4 (12): 2319–7064

Baiju NT. Five Advantages and Disadvantages of Cloud Storage. Available online at http://bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloud-storage/. 2014

Bennani N., Damiani E. and Cimato S. Toward Cloud-Based Key Management for Outsourced Databases. *34th Annual IEEE Computer Software and Applications Conference Workshops*. IEEE. 2010

Brad C. Can Public Key Infrastructure Provide More Security Online. Available online at https://www.techopedia.com/2/28476/security/can-public-key-infrastructure-provide-more-security-online. April 2012

Buchade A. R. and Ingle R. Key Management for Cloud Data Storage: Methods and Comparison. *Fourth International Conference on Advanced Computing & Communication Technologies*. IEEE. 2014

Calheiros R. N., Ranjan R., Beloglazov A., De Rose C. A. F. and Buyya R. Cloudsim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms. *Software Practice and Experience*, 2011. 41: 23–50

Carlos C. Cloud Security: The Challenges with Key Management in the Cloud. Available online at https://www.joyent.com/blog/cloud-security-the-challenges-with-key-management-in-the-cloud-and-everywhere-else. September 2013

Chandramouli R., Iorga M., Chokhani S. Cryptographic Key Management Issues & Challenges in Cloud Services. *National Institute of Standards and Technology Interagency or Internal Report 7956*. September 2013

Choudhury A. J., Kumar P., Lim H. and Jae-Lee H. A Strong User Authentication Framework for Cloud Computing. *IEEE Asia -Pacific Services Computing Conference*. IEEE. 2011

Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Available online at https://cloudsecurityalliance.org/csaguide.pdf. December 2009

Cynthia H. What is Cloud Computing. Available online at http://www.datamation.com/cloud-computing/what-is-cloud-computing.html. March 2017

Dinesha H. and Agrawal V. Multi-Level Authentication Technique for Accessing Cloud Services. *Computing, Communication and Applications (ICCCA), 2012 International Conference.* IEEE. 2012. 4(12)

El-Booz S. A., Attiya G. and El-Fishawy N. A Secure Cloud Storage System Combining Time-Based One-Time Password and Automatic Blocker Protocol. *Computer Engineering Conference (ICENCO), 2015 11th International*. December 29–30, 2015. Cairo, Egypt: IEEE. 2015

Gary C. K. An Overview of Cryptography. Available online at http://www.garykessler.net/library/crypto.html. April 2017

Guo M. H., Liaw H. T., Hsiao L. L., Huang C. Y. and Yen C. T. Authentication Using Graphical Password in Cloud. *15th International Symposium on IEEE Wireless Personal Multimedia Communications (WPMC)*. September 24–27, 2012. Taipei, Taiwan: IEEE. 2012

Huang R. W., Gui X. L., Yu S. and Zhuang W. Research on Privacy-Preserving Cloud Storage Framework Supporting Ciphertext Retrieval. *International Conference on Network Computing and Information Security*. May 14–15, 2011. Guilin, China: IEEE. 2011

Jaidhar C. D. Enhanced Mutual Authentication Scheme for Cloud Architecture. *3rd International IEEE Advance Computing Conference (IACC)*. February 22–23, 2013. Ghaziabad, India: IEEE. 2013

Jeff Tyson. How Encryption Works. Available online at http://computer.howstuffworks.com/encryption2.htm. 2016

John R. V. Public Key Infrastructure: Building Trusted Applications and Web Services. *A CRC Press Company*. Available online at https://books.google.com.my/books?id=3kS8XDALWWYC&printsec=frontcover#v=onepage&q&f=false. 2004

Keijo Ruohonen. Mathematical Cryptology. Available online at http://math.tut.fi/~ruohonen/MC.pdf. 2014

Lakshmi R. S. and Nirmalan R. Survey on Imparting Data in Cloud Storage Using Key Revocation Process. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2014. 4(11)

Lei S., Zishan D. and Jindi G. Research on Key Management Infrastructure in Cloud Computing Environment. *Ninth International Conference on Grid and Cloud Computing*. November 1–5, 2010. Nanjing, China: IEEE. 2010

Lomte S. and Dudhani S. (2015). Secure Key for Authentication and Secret Sharing in Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2015. 5(6)

Maninder S. and Sarbjeet S. Design and Implementation of Multi-tier Authentication Scheme in Cloud. *International Journal of Computer Science Issues*, 2012. 9(2)

Margaret R. Cloud Storage. Available online at http://searchcloudstorage.techtarget.com/definition/cloud-storage. May 2016

Margaret R. PKI (Public Key Infrastructure). Available online at http://searchsecurity.techtarget.com/definition/PKI. November 2014

Martin L. Federated Key Management For Secure Cloud Computing. *Voltage Security Conference Presentation*. Available online at http://storageconference.us/2010/Presentations/KMS/17.Martin.pdf. 2010

Nashaat E. K. and Hossam A. R. A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems. *Journal of Emerging Trends in Computing and Information Sciences*, 2012. 3(6): 970–974

Parul C. A Survey of the Existing Security Issues in Cloud Computing. *International Journal of Computer Science and Information Technologies*, 2014. 5(2): 1066–1068

Passent M. E. K., Azza A. A., Amr F. S. Security Issues Over Some Cloud Models. *International Conference on Communication, Management and Information Technology*, 2015. 853–858

Pate S. and Tambay T. Securing the Cloud – Using Encryption and Key Management to Solve Today’s Cloud Security Challenges. *Storage*

Networking Industry Association. Available online at http://www.snia.org/sites/default/education/tutorials/2011/spring/security/PateTambay_Securing_the_Cloud_Key_Mgt.pdf. 2011

Rathod P. and Sapkal S. Audit Service for Data Integrity in Cloud. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2014. 4(4): 288–292

Reddy B. G. V. R. and Kavya A. Remote Access and Dual Authentication for Cloud Storage. *International Journal of Modern Engineering Research*, 2014. 4(5): 53–55

RF Wireless World. Cloud Storage Infrastructure, Storage Types and Requirements. Available online at http://www.rfwireless-world.com/Tutorials/cloud-storage-infrastructure.html. 2012

Sanka S., Hota C. and Rajarajan M. Secure Data Access in Cloud Computing. *IEEE 4th International Conference Internet Multimedia Services Architecture and Application (IMSAA)*. December 15-17, 2010. Bangalore, India: IEEE. 2010

Sekhar R. V., Nandini N., Bhanumathy D., Hemalatha M. Identity Based Authentication for Data Stored in Cloud. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2015. 5(3): 243–247

Selvaraj A. and Sundararajan S. Survey on Public Auditability to Ensure Data Integrity in Cloud Storage. *International Journal of Computers and Applications*, 2015. 37: 3–4 and 102–110

Shelton B. K. Introduction to Cryptography. *Auerbach Publications: The Final Word in Enterprise Computing and Networking*. Available online at http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm. 2015

Sulistio A., Yeo C. S. and Buyya R. GridSim: A Grid Simulation Toolkit for Resource Modelling and Application Scheduling for Parallel and Distributed Computing. Available online at http://www.buyya.com/gridsim/. 2010

Suparman S. and Kwang E. P. Key Management System Framework for Cloud Storage. Available online at http://docplayer.net/14081345-Key-management-system-framework-for-cloud-storage-singa-suparman-eng-pin-kwang-temasek-polytechnic-singas-engpk-tp-edu-sg.html. 2014

University of California. *Above the Clouds: A Berkeley View of Cloud Computing*. Berkeley, UCB/EECS–2009–28. 2009

Veeraragavan N. and Arockiam L. Enhanced Authentication Mechanism for Securing the Cloud Services using AaaS. *International Advanced Research Journal in Science, Engineering and Technology*, 2016. 3(3)

Wang, P., Ku, C. C. and Wang, T. C. A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security. *Institute of Computer and Communication Engineering*, July 27, 2011. Taiwan. 183–196

Yaser F. A. D. and Khamitkar S. D. A Proposed Model For Data Storage Security in Cloud Computing. *International Journal of Computer Engineering and Technology (IJCET)*, 2013. 4(6): 970–974

Yassin A. A., Jin H., Ibrahim A., Qiang W. and Zou D. A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing. *IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum.* May 21-25, 2012. Shanghai, China: IEEE. 2012. 1210–1217

Zhu H. H., Qian H. H., Hong T. and Cao W. H. (2011). Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security. *IEEE International Conference on Cloud and Service Computing.* December 12-14, 2011. Hong Kong, China: IEEE. 2011. 302–308