AUTHENTICATION AND AUTHORIZATION IN CLOUD COMPUTING USING KERBEROS

AHMAD M. SAEED HIDAR

A project 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

JANUARY 2014
“This Project is dedicated especially to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task could be accomplished if it is done one-step at a time. My brother and beloved my wife, daughter, family and supervisor”
ACKNOWLEDGEMENT

First and foremost, I would like to thank Allah because of his blessing; I would like to express heartfelt gratitude to my supervisor Prof Dr. MUHAMMAD SHAFIE BIN ABD LATIFF, and Co-supervisor Dr. YAHAYA COULIBALY for their constant support during my study at Universiti Teknologi Malaysia (UTM). They inspired me greatly to work on this project. Their willingness to motivate me contributed tremendously to our project. I have learned a lot from them and I am fortunate to have them as my mentor and supervisor. I am also would like to express my sincere appreciation to Associate Prof. Dr. Mazleena Salleh and Dr. Majid Bakhtiari as my examiner for their constructive suggestions to improve this project report and my understanding.

I would like to acknowledge and thanks all my close friends particularly Harith Ekal and Mohannad Ghazi for usual support and corporation that will never be forgotten. I would not have done it without the help and motivation from both of you.

To my family, no words can describe me gratefulness foe always being there despite of the distance. They showered me with love and compassion and enrich my life like no other. They are the source of comfort and kept me focus the priorities in life and therefore, this work are dedicated to them.
The emergence of cloud computing paradigm offers attractive and innovative computing services. Cloud providers deliver various types of computing services to customers according to a pay-per-use economic model. However, this technology introduces a new concern for enterprises and businesses regarding their privacy and security. Security as a Service is a new cloud service model for the security enhancement of a cloud environment. This is a way of centralizing security solutions under the control of professional security specialists. Authentication and authorization services are parts of cloud security services. This study focused on Authentication and authorization solutions for cloud environments. More specifically, architecture of a cloud security system is designed and proposed for providing two identity services for cloud-based systems: authentication and authorization. The main contribution of this study is to implement these services using Kerberos protocol, which will enable cloud-based application service providers to manage their users in an open, flexible, interoperable and secure environment. The methods of the proposed services are necessary for managing and providing those identity services. The implementation and specification of each service is described and explained, a prototype system of an authentication and authorization services are implemented and tested. The implementation is done using Web Service technology; it is shown that both services are at least computationally secure against potential security risks associated with different types of attacks. The security of Kerberos protocol that has been implemented for authentication ensures a secure and reliable environment for cloud-based application services, which is very easy to deploy and exploit on cloud-based platforms.
ABSTRAK

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td>ii</td>
<td></td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iii</td>
<td></td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
<td></td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>vi</td>
<td></td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
<td></td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xi</td>
<td></td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xiii</td>
<td></td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td>vii</td>
<td></td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 Introduction 1
1.2 Problem Background 2
1.3 Problem Statement 5
1.4 Project Objectives 6
1.5 Project Scope 7
1.6 Contribution 7
1.7 Organization of the Project 7
1.8 Summary 8

## 2 LITERATURE REVIEW

2.1 Introduction 9
2.2 Existing Problem in Cloud Computing 10
  2.2.1 Cloud Computing Security Threats 11
  2.2.2 Security Concerns in Cloud Computing 14
## 2.2.2.1 Data Leakage

2.2.2.2 Reputation Fate Sharing

2.2.2.3 Customer Identification

2.2.2.5 XML Signature

2.2.2.6 Browser Security

2.2.2.7 Loss of Control Over Data

2.2.2.8 Side Channels

2.2.3 Previous Studies and Contribution in Cloud Computing

## 2.3 Authentication and Authorization Review in Cloud Computing

2.3.1 Authentication Used by Cloud Providers

2.3.2 User Authentication in Cloud Computing

2.3.3 Previous Studies and Contributions on Security Issues in Cloud Computing

## 2.4 Features of Kerberos Protocol

## 2.5 Summary

## 3 RESEARCH METHODOLOGY

3.1 Introduction

3.2 Project Methodology

3.3 Usable of Kerberos Protocol

3.3.1 Study of Kerberos Capabilities and Features

3.4 Phase 1: Identify the problem and Propose an Authentication System

3.5 Phase 2: Role-Based Access Control as an Authorization Technique

3.6 Phase 3: Security Validation of Kerberos Protocol

3.7 Software Requirements

3.8 Summary

## 4 DESIGN AND IMPLEMENTATION

4.1 Introduction

4.2 Kerberos Authentication System Design

4.2.1 Flow of Packets in Kerberos Protocol
4.3 Cryptography for Secure Communication 48
4.4 Design of Web Interface, Authentication and Authorization 54
  4.4.1 Authentication Interface 55
  4.4.2 Authorization Technique 56
4.5 Publishing Steps of the Web Application 59
4.6 Summary 65

5  EVALUATION AND VALIDATION
  5.1 Introduction 66
  5.2 Evaluation of System Security 66
  5.3 Validation of Security of Kerberos Protocol 67
    5.3.1 Acunetix Web Vulnerability Scanner 69
    5.3.2 Burp Suite 70
      5.3.2.1 Web Browser Configuration 71
      5.3.2.2 Burp Suite Configuration 72
      5.3.2.3 Intercepting Web Request 74
    5.3.3 Wireshark to Intercept packet 78
  5.4 Summary 79

6  CONCLUSION AND RECOMMENDATION
  5.1 Introduction 80
  5.2 Summary of Project 80
  5.3 Future work 81

REFERENCES 83
APPENDICES 90
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Authentication Attacks</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>Contribution Of Security in Cloud Computing</td>
<td>29</td>
</tr>
<tr>
<td>5.1</td>
<td>Some example of security testing tools</td>
<td>69</td>
</tr>
</tbody>
</table>
# List of Figures

<table>
<thead>
<tr>
<th>Figure No.</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Top 20 passwords</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Packet capture in Wireshark</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Google Apps Two-step verification</td>
<td>24</td>
</tr>
<tr>
<td>2.4</td>
<td>Kerberos actions overview</td>
<td>30</td>
</tr>
<tr>
<td>3.1</td>
<td>Methodolgy Framework</td>
<td>35</td>
</tr>
<tr>
<td>3.2</td>
<td>Kerberos Authentication process</td>
<td>39</td>
</tr>
<tr>
<td>4.1</td>
<td>Kerberos authentication flowchart</td>
<td>44</td>
</tr>
<tr>
<td>4.2</td>
<td>JavaScript Object Notation (JSON)</td>
<td>45</td>
</tr>
<tr>
<td>4.3</td>
<td>Flow of Kerberos</td>
<td>45</td>
</tr>
<tr>
<td>4.4</td>
<td>Data flow from client to AS</td>
<td>46</td>
</tr>
<tr>
<td>4.5</td>
<td>Data flow from AS to client</td>
<td>46</td>
</tr>
<tr>
<td>4.6</td>
<td>Data flow from client to TGS</td>
<td>47</td>
</tr>
<tr>
<td>4.7</td>
<td>Data flow from TGS to client</td>
<td>47</td>
</tr>
<tr>
<td>4.8</td>
<td>Data flow from client to server</td>
<td>47</td>
</tr>
<tr>
<td>4.9</td>
<td>Data flow from server to client</td>
<td>48</td>
</tr>
<tr>
<td>4.10</td>
<td>Login page</td>
<td>55</td>
</tr>
<tr>
<td>4.11</td>
<td>User ticket page</td>
<td>56</td>
</tr>
<tr>
<td>4.12</td>
<td>Types and rights of users</td>
<td>57</td>
</tr>
<tr>
<td>4.13</td>
<td>Admin ticket page</td>
<td>57</td>
</tr>
<tr>
<td>4.14</td>
<td>User management page</td>
<td>58</td>
</tr>
<tr>
<td>4.15</td>
<td>User page</td>
<td>58</td>
</tr>
<tr>
<td>4.16</td>
<td>Service provided by cloud provider</td>
<td>59</td>
</tr>
<tr>
<td>4.17</td>
<td>Microsoft Azure welcome interface</td>
<td>60</td>
</tr>
<tr>
<td>4.18</td>
<td>Interface for creating new web site</td>
<td>60</td>
</tr>
</tbody>
</table>
4.19 Interface for assigning URL to a website
4.20 Interface for publishing Kerberos service webpage
4.21 Interface for publishing Kerberos authentication webpage
4.22 Dashboard of web site
4.23 Kerberos Login and KDC pages
5.1 Acunetix Scan of Web Application Server For Vulnerability
5.2 Configure Local proxy in Firefox
5.3 Burp proxy interacts
5.4 Burp proxy configuration
5.5 Username intercept packet
5.6 Intercept ticket
5.7 Intercept SessionID
5.8 Brute force attack of authentication
5.9 Wireshark packet stream intercept
# LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AS</td>
<td>Authentication service</td>
</tr>
<tr>
<td>ASP</td>
<td>Active Server Pages</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Service</td>
</tr>
<tr>
<td>DS</td>
<td>Distributed System</td>
</tr>
<tr>
<td>EC</td>
<td>Elastic Compute Cloud</td>
</tr>
<tr>
<td>IBA</td>
<td>Identity-Based Authentication</td>
</tr>
<tr>
<td>IDaaS</td>
<td>Identity as a Service</td>
</tr>
<tr>
<td>IDC</td>
<td>International Data Corporation</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>KDC</td>
<td>Kerberos Distribution Centre</td>
</tr>
<tr>
<td>MTM</td>
<td>Mobile Trusted Module</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OAuth</td>
<td>Open authorization</td>
</tr>
<tr>
<td>OS</td>
<td>Operating system</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
</tr>
<tr>
<td>PKI</td>
<td>Public-Key Infrastructure</td>
</tr>
<tr>
<td>RC4</td>
<td>Ron's Code 4</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>SecaaS</td>
<td>Security as a Service</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-oriented architecture</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>TCP</td>
<td>Trusted Computing Platform</td>
</tr>
<tr>
<td>TCPS</td>
<td>Transparent Cloud Protection System</td>
</tr>
<tr>
<td>TGS</td>
<td>Ticket Granting Service</td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket-Granting Ticket</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Authentication Server code</td>
<td>91</td>
</tr>
<tr>
<td>B</td>
<td>Login to Web Application Server code</td>
<td>96</td>
</tr>
<tr>
<td>C</td>
<td>Advance Encryption Standard (AES) code</td>
<td>100</td>
</tr>
<tr>
<td>D</td>
<td>Secure Hash Function Algorithm (SHA-2)</td>
<td>125</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

Cloud computing as a new paradigm of information technology that offers tremendous advantages in economic aspects such as reduced time to market, flexible computing capabilities and limitless computing power. To use the full potential of cloud computing, data are transferred, processed and stored by external cloud providers.

The NIST (National Institute of Standards and Technology: is the federal technology agency that works with industry to develop and apply technology, measurements, and standards) definition of cloud computing: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Authentication is the process of verifying the identity of particular users. To authenticate a user, the user is asked for information that would prove his identity. Once the server receives the information from the user who provides his identity, the server determines whether that information is correct. Furthermore, the server verifies whether the password entered by user matches the one listed in the password database. If so, then the user is authenticated. If not, then his request is denied or terminate.
Authorization refers to granting or denying access to specific resources based on the requesting user’s identity. This step is performed after authentication phase. Authorization is usually performed through access control list which associate user identities with specific rights. Authorization includes information such as a user’s group membership, user policies, and other information that determines what level of access that user has to computer or network resources.

As the model of cloud computing is quite new, there are various exposed issues which need to be fixed before cloud computing can be fully conventional to the broad community. Before we dive into the research methodology and the issues of security in cloud, a deeper clarification is needed of what cloud computing comprises.

This chapter will describe the problem background, problem statement, scope, and objectives of this study as well as contribution of 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 computing is one of the highest concern issues. Some of the important issues related is the authentication and authorization which means verifying the truly the person who claims to be.

Although many researchers have been done on improving the security of authentication and authorization in cloud computing, many issues have not yet been solved totally. 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 e.g. SSL/TLS, SSH, RC4 and SHA-2 and so on. On the other hand, users and companies are concerned about their data and where it is located,
is it encrypted to deny unauthorized users to read it, modify the data or attacker interception.

The obstacles that limit the spread of cloud computing is the mentality of those who work on IT department and impede the transition to this technology. That accelerate the adoption of cloud computing requires a change of mentality that control the IT departments. To complete the adoption of cloud computing as an alternative to traditional technical regulations require overcoming technical and regulatory obstacles. The researchers also claims that all the doubts and fears related to technical cloud computing may still exist. Even a few institutions find that performance and availability are the key requirements for the adoption of cloud computing, where some of the issues still raise concerns, however, they are important issues within the institution itself, may prevent it from moving to the use of cloud computing.

Both cloud service providers and customers are concerned about security issues associated with the cloud environment. Although different cloud domains have different security and policy characteristics corresponding to specific functionality and usage of the system, the important aspects of secure service provisioning are generic among them. All the potential security issues associated with Identity Management, Confidentiality, Authentication, Access Control and Authorization, None-Repudiation are fatal for a cloud environment (Hamdi, 2012). Cloud service providers try to overcome security and privacy related issues by offering security solutions to its customers. Security as a Service (SecaaS) is a new instance of cloud service model which delivers security solutions to enterprises by means of cloud-based services from the cloud. These services may be delivered in different forms, what may result in market confusion and complication of the selection process. That is why implementation of SecaaS is still limited, but usage of those cloud-based security services will more than triple in many aspects by 2013, based on the predictions made by Gartner IT research center (Subashini and Kavitha, 2011).

Identity and Access Control Service should provide identity management and access control to cloud resources for registered entities. Such entities can be 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, which is the authentication process that precedes the authorization process. Besides authentication and authorization processes,
audit logging mechanism should be used to keep track of all successful and failed operations regarding authentication and access attempts by the application (Subashini and Kavitha, 2011).

Confidentiality is achieved by different encryption mechanisms, which is the procedure of encoding data by means of cryptographic algorithms. Providing such a service will guarantee privacy of sensitive and private data and the intended entity can only decode it. Cryptographic algorithms, which are computationally hard to crack together with encryption and decryption procedures, digital signatures, hashing, certificates, key exchange and management form an encryption system which can be delivered as a service and assure confidentiality and non-repudiation in a cloud environment (Subashini and Kavitha, 2011).

As such, the centralization of security services and implementation of those services through standardized security frameworks under the model of SecaaS can be viewed as an innovative and beneficial utility for a cloud environment. This method promotes the delivery of security services to customers in a professional and standardized manner (Demchenko et al., 2011). Many motives can be pointed for such kind of solution for a cloud environment:

- Aggregation of security skills and security experts.
- Effective centralized solution.
- Standardization of security practices.
- Competitive advantage in the market over the competitors.

The effective management of security in cloud-based applications is one of the core factors for the successful cloud computing platform (Ramgovind et al., 2010).

Identity as a Service (IDaaS) is one area of SecaaS and it aims to provide security services within the scope of “identity eco-system” of a cloud environment (Ates et al., 2011). Existing cloud-based identity service mechanisms require constant improvements and enhancements as identity-associated security risks have become one of the most
significant issues for a cloud environment. Privacy protection for identity information is critical factor for a successful identity system (Lee et al., 2009).

The issues are highlighting that internal obstacles ranging from the constraints and psychological barriers to simply knowing that the data and applications exist somewhere else. The mixing of roles between managers applications and managers of infrastructure, leading to potential opposition within the IT department to move to the use of cloud computing, add to it pressure faced by technical department managers and employees to provide IT services to the maximum effectiveness and economic efficiency equivalent to that provided by external service providers.

Among all the issues in cloud computing, the most important issues are authentication and authorization 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 implemenent SSL/TLS protocol to secure authentication and authorization to cloud computing, 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, Platform as a Service, web hosting as well as cost advantages for business organizations. Security issues that arise within this computing 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. Security as a Service is a rather new approach to provide security solutions for a cloud environment in a professional and
centralized way. Furthermore, there are many concerns about security of cloud computing the most critical issue nowadays is authentication and authorization. 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. Because of Security as a Service delivery model is very broad and not a concrete implementation and currently still in its improvement stage, few cloud providers have a system that contains centralized security infrastructure, which can provide all the needs of customers from the security perspective. Some Authentication and authorization that can be implemented for cloud computing 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-based platform services.

As a solution to this problem, this master project will investigate how to manage authentication and authorization systems in cloud environments and propose an approach of cloud security system for providing authentication and authorization services to cloud-based software services through Kerberos protocol. At the same time, the project will focus on how to deliver those services in an interoperable and secure manner.

1.4 Project Objective

The objectives of this project are:

1. To study the features and capabilities of Kerberos and authentication mechanisms applied in cloud computing.
2. To develop and implement Kerberos based authentication and authorization technique for cloud computing.
3. To validate authentication by performing penetration testing in order to verify the security.
1.5 Project Scope

The scopes of this project are:

1. The project will focus on secure authentication based on the Kerberos authentication protocol.
2. The validation of authentication in cloud computing by using Kerberos based authentication, authorization and evaluate it on the certain Level of cloud computing services.
3. The validation of security by using some tools to break authentication.

1.6 Contribution

The contribution of this project is to implement a working authentication solution, that can be used in cloud services. The authentication method will be Kerberos protocol with an encryption algorithm that protects the user password and communication between clients and cloud server. This project also present a solution to securely logs in users over the Internet. Appropriate encryption methods to use with cloud service, which must be a fast and secure encryption algorithm, will be discussed and implemented. The results of the authentication solution is evaluated and compared to other providers’ current solution. Furthermore, the encryption method used for Internet transmissions is Advanced Encryption Standard (AES) and Hash function (SHA-2) had been used as well.

1.7 Organization of the Project

The report of this master project comprises six chapters, organized in the following way:
Chapter 1 presents the background of the research area and defines the motives of this investigation, the problem statement to be solved, the objectives, and scopes that required accomplishing this project. Contribution and summary.

Chapter 2 presents a literature review and analysis of the existing problems, solutions, and related standards and mechanism.

Chapter 3 describes the methodology of the proposed security system, including authentication phase, authorization phase, and penetration testing phase, their functionalities and security considerations.

Chapter 4 describes and explains design details and implementation of authentication and authorization services of the proposed protocols (Kerberos).

Chapter 5 provides the evaluation of the proposed security system. The evaluation is performed from two aspects: system integration and security.

Chapter 6 finalizes the report by presenting conclusions from this investigation and future work which may contribute to this research.

1.8 Summary

This chapter provided a complete definition and introduction to the research; including the research aim, scope of the research and its objectives. In addition, the chapter provided a comprehensive background of the problem, contribution and importance of the research.
REFERENCES


