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.

ABSTRACT

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

Kebangkitan paradigma komputeran awan menawarkan pelbagai perkhidamatan komputeran yang menarik dan inovatif. Pembekal-pembekal awan menyediakan pelbagai jenis perkhidmatan komputeran kepada para pelanggan yang mengikut kaedah model ekonomi membayar setiap penggunaan. Akan tetapi, teknologi ini memperkenalkan masalah-masalah kesulitan dan keselamatan. Keselamatan sebagai perkhidmatan adalah model perkhidmatan awan yang baru untuk meningkatkan alam awan. Kaedah ini adalah cara untuk memusatkan penyelesaian keselamatan dibawah kawalan para pakar keselamatan yang berprofesional. Perkhidmatan-perkhidmatan pengesahan dan kebenaran adalah sebahagian daripada perkhidmatan keselamatan awan. Kajian ini fokus dalam penyelesaian pengesahan dan kebenaran untuk alam awan. Lebih terperinci, mereka bentuk dan mencadangkan seni bina sistem keselamatan awan untuk menawarkan dua perkhidmatan identiti untuk sistem-sistem berasaskan awan: pengesahan dan kebenaran. Sumbangan utama kajian ini adalah untuk melaksanakan perkhidmatan-perkhidmatan ini dengan menggunakan protokol Kerberos, yang akan membolehkan pembekal-pembekal perkhidmatan aplikasi berasaskan awan untuk menguruskan pengguna-pengguna didalam suasana yang terbuka, fleksibel, saling beroperasi, dan terjamin. Kaedah-kaedah perkhidmatan yang dicadangkan diterangkan, semua entiti-entiti yang diperlukan untuk menguruskan dan menyediakan perkhidmatan-perkhidmatan identiti ditakrifkan. Setiap perlaksanaan dan spesifikasi perkhidmatan diterangkan dan dijelaskan, suatu sistem prototaip perkhidmatan pengesahan dan kebenaran dilaksanakan dan diuji. Kaedah perlaksanaan dibuat dengan menggunakan teknologi Perkhidmatan Web; telah ditunjuk bahawa kedua-dua perkhidmatan ini adalah terjamin secara komputer terhadap risiko-risiko keselamatan yang berpotensi yang berkait dengan jenis serangan yang berbeza. Keselamatan protokol Kerberos yang telah dilaksanakan untuk pengesahan menjamin suasana perkhidmatan-perkhidmatan aplikasi berasaskan awan yang senang untuk diguna dan dieksploitasi pada landasan-landasan yang berasaskan awan terjamin dan boleh dipercayai.

TABLE OF CONTENTS

CHAPTE	TITLE	PAGE
	DECLARATION	**ii**
	DEDICATION	**iii**
	ACKNOWLEDGEMENT	**iv**
	ABSTRACT	**v**
	ABSTRAK	**vi**
	TABLE OF CONTENTS	**vii**
	LIST OF TABLES	**x**
	LIST OF FIGURES	**xi**
	LIST OF ABBREVIATIONS	**xiii**
	LIST OF APPENDICES	**vii**
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 17
2.2.2.2 Reputation Fate Sharing 17
2.2.2.3 Customer Identification 17
2.2.2.5 XML Signature 18
2.2.2.6 Browser Security 18
2.2.2.7 Loss of Control Over Data 18
2.2.2.8 Side Channels 19
2.2.3 Previous Studies and Contribution in Cloud Computing 19
2.3 Authentication and Authorization Review in Cloud Computing 23
2.3.1 Authentication Used by Cloud Providers 23
2.3.2 User Authentication in Cloud Computing 25
2.3.3 Previous Studies and Contributions on Security Issues in Cloud Computing 27
2.4 Features of Kerberos Protocol 30
2.5 Summary 32

3 **RESEARCH METHODOLOGY**
3.1 Introduction 33
3.2 Project Methodology 24
3.3 Usable of Kerberos Protocol 36
3.3.1 Study of Kerberos Capabilities and Features 36
3.4 Phase 1: Identify the problem and Propose an Authentication System 37
3.5 Phase 2: Role-Based Access Control as an Authorization Technique 40
3.6 Phase 3: Security Validation of Kerberos Protocol 41
3.7 Software Requirements 41
3.8 Summary 42

4 **DESIGN AND IMPLEMENTATION**
4.1 Introduction 43
4.2 Kerberos Authentication System Design 43
4.2.1 Flow of Packets in Kerberos Protocol 45

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

53.2.3 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 NO	TITLE	PAGE
2.1	Authentication Attacks	13
2.2	Contribution Of Security in Cloud Computing	29
5.1	Some example of security testing tools	69

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Top 20 passwords	15
2.2	Packet capture in Wireshark	16
2.3	Google Apps Two-step verification	24
2.4	Kerberos actions overview	30
3.1	Methodolgy Framework	35
3.2	Kerberos Authentication process	39
4.1	Kerberos authentication flowchart	44
4.2	JavaScript Object Notation (JSON)	45
4.3	Flow of Kerberos	45
4.4	Data flow from client to AS	46
4.5	Data flow from AS to client	46
4.6	Data flow from client to TGS	47
4.7	Data flow from TGS to client	47
4.8	Data flow from client to server	47
4.9		48
	Data flow from server to client	
4.10	Login page	55
4.11	User ticket page	56
4.12	Types and rights of users	57
4.13	Admin ticket page	57
4.14	User management page	58
4.15	User page	58
4.16	Service provided by cloud provider	59
4.17	Microsoft Azure welcome interface	60
4.18	Interface for creating new web site	60

4.19 Interface foe assigning URL to a website 61

4.20 Interface for publishing Kerberos service webpage 62

4.21 Interface for publishing Kerberos authentication webpage 63

4.22 Dashboard of web site 64

4.23 Kerberos Login and KDC pages 64

5.1 Acunetix Scan of Web Application Server For Vulnerability 70

5.2 Configure Local proxy in Firefox 72

5.3 Burp proxy interacts 73

5.4 Burp proxy configuration 73

5.5 Username intercept packet 75

5.6 Intercept ticket 76

5.7 Intercept SessionID 77

5.8 Brute force attack of authentication 78

5.9 Wireshark packet stream intercept 79

LIST OF ABBREVIATION

AES	-	*Advanced Encryption Standard*
AS	-	Authentication service
ASP	-	*Active Server Pages*
AWS	-	Amazon Web Service
DS	-	Distributed System
EC	-	Elastic Compute Cloud
IBA	-	Identity-Based Authentication
IDaaS	-	Identity as a Service
IDC	-	International Data Corporation
JSON	-	JavaScript Object Notation
KDC	-	Kerberos Distribution Centre
MTM	-	Mobile Trusted Module
NIST	-	National Institute of Standards and Technology
OAuth	-	Open authorization
OS	-	Operating system
OTP	-	*One-Time Password*
PKI	-	*Public-Key Infrastructure*
RC4	-	*Ron's Code 4*
RFC	-	*Request for Comments*
SecaaS	-	Security as a Service
SHA	-	Secure Hash *Algorithm*
SMS	-	*Short Message Service*
SOA	-	*Service-oriented architecture*
SOAP	-	Simple Object Access Protocol
SSH	-	Secure Shell

SSL	-	Secure Sockets Layer
SSO	-	Single Sign On
TCP	-	Trusted Computing Platform
TCPS	-	Transparent Cloud Protection System
TGS	-	Ticket Granting Service
TGT	-	Ticket-Granting Ticket
TLS	-	Transport Layer Security
TPM	-	Trusted Platform Module
XML	-	Extensible Markup Language

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Authentication Server code	91
B	Login to Web Application Server code	96
C	Advance Encryption Standard (AES) code	100
D	Secure Hash Function Algorithm (SHA-2)	125

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 loud 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 impalement 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

Abu-Nimeh, S. 2011. Three-Factor Authentication. *Encyclopedia of Cryptography and Security*. Springer.

Almulla, S. A. & Yeun, C. Y. 2010 .Cloud computing security management. Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on, IEEE, 1-7.

Armando, A., Carbone, R., Compagna, L., Cuellar, J. & Tobarra, L. Formal 2008. Analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps. Proceedings of the 6th ACM workshop on Formal methods in security engineering, ACM, 1-10.

Ates, M., Ravet, S., Ahmat, A. M. & Fayolle, J. 2011. An identity-centric internet: identity in the cloud, identity as a service and other delights. Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, IEEE, 555-560.

Bella, G. & Paulson, L. C. 1998. Kerberos version IV: Inductive analysis of the secrecy goals. *Computer Security—ESORICS 98.* Springer.

Bella, G. & Riccobene, E. 1997. Formal analysis of the Kerberos authentication system. *Journal of Universal Computer Science,* 3**,** 1337-1381.

Bellovin, S. M. & Merritt, M. 1990. Limitations of the Kerberos authentication system. *ACM SIGCOMM Computer Communication Review,* 20**,** 119-132.

Bertino, E., Paci, F., Ferrini, R. & Shang, N. 2009. Privacy-preserving Digital Identity Management for Cloud Computing. *IEEE Data Eng. Bull.,* 32**,** 21-27.

Bleikertz, S., Schunter, M., Probst, C. W., Pendarakis, D. & Eriksson, K. 2010. Security audits of multi-tier virtual infrastructures in public infrastructure clouds. Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 93-102.

Brodkin, J. 2008. Gartner: Seven cloud-computing security risks.

Bryant, B. 1988. *Designing an authentication system: a dialogue in four scenes*, MIT, Project Athena.

Chang, H. & Choi, E. 2011. User Authentication in Cloud Computing. *Ubiquitous Computing and Multimedia Applications.* Springer.

Chen, Y., Paxson, V. & Katz, R. H. 2010. What’s new about cloud computing security. *University of California, Berkeley Report No. UCB/EECS-2010-5 January,* 20**,** 2010-5.

Choudhury, A. J., Kumar, P., Sain, M., Lim, H. & Jae-Lee, H. 2011. A strong user authentication framework for cloud computing. Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, IEEE, 110-115.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, 85-90.

Claburn, T. 2009. Twitter hack tars Google’s cloud. *Information Week,* 16.

Crampton, J., Lim, H. W. & Paterson, K. G. 2007. What can identity-based cryptography offer to web services? Proceedings of the 2007 ACM workshop on Secure web services, ACM, 26-36.

Dao, T.-B. & Shibayama, E. 2009. Idea: Automatic Security Testing for Web Applications. *Engineering Secure Software and Systems.* Springer.

Demchenko, Y., Ngo, C., De Laat, C., Wlodarczyk, T. W., Rong, C. & Ziegler, W. 2011. Security infrastructure for on-demand provisioned cloud infrastructure services. Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, IEEE, 255-263.

Di Pietro, R., Me, G. & Strangio, M. A. 2005. A two-factor mobile authentication scheme for secure financial transactions. Mobile Business, 2005. ICMB 2005. International Conference on, IEEE, 28-34.

Dinesha, H. & Agrawal, V. 2012. Multi-level authentication technique for accessing cloud services. Computing, Communication and Applications (ICCCA), 2012 International Conference on, IEEE, 1-4.

Griffin, D. 2008. Safer Authentication with a One-Time Password Solution. *published May*.

Gupta, A. 2010. Cloud computing growing interest and related concerns. Computer Technology and Development (ICCTD), 2010 2nd International Conference on, IEEE, 462-465.

Hamdi, M. 2012. Security of cloud computing, storage, and networking. Collaboration Technologies and Systems (CTS), 2012 International Conference on, IEEE, 1-5.

Hota, C., Sanka, S., Rajarajan, M. & Nair, S. K. 2011. Capability-based cryptographic data access control in cloud computing. *Int. J. Advanced Networking and Applications,* 3**,** 1152-1161.

Jansen, W. A. 2011. Cloud hooks: Security and privacy issues in cloud computing. System Sciences (HICSS), 2011 44th Hawaii International Conference on, IEEE, 1-10.

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L. 2009. On technical security issues in cloud computing. Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, IEEE, 109-116.

Kang, L. & Zhang, X. 2010. Identity-based authentication in cloud storage sharing. Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE, 851-855.

Kim, H. & Park, C. 2010. Cloud Computing and Personal Authentication Service. *KIISC,* 20**,** 11-19.

Kohl, J. & Neuman, C. 1993. RFC 1510–The Kerberos Network Authentication Service (V5). IETF.

Kohl, J. T. 1990. The use of encryption in Kerberos for network authentication. Advances in Cryptology—CRYPTO’89 Proceedings, Springer, 35-43.

Lee, H., Jeun, I. & Jung, H. 2009. Criteria for evaluating the privacy protection level of Identity Management Services. Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on, IEEE, 155-160.

Lim, H. W. & Paterson, K. G. 2005. Identity-based cryptography for grid security. e-Science and Grid Computing, 2005. First International Conference on, IEEE, 10 pp.-404.

Lim, H. W. & Robshaw, M. J. 2004. On identity-based cryptography and Grid computing. *Computational Science-ICCS 2004.* Springer.

Liu, P., Zong, R. & Liu, S. 2008. A new model for Authentication and Authorization across Heterogeneous Trust-Domain. Computer Science and Software Engineering, 2008 International Conference on, IEEE, 789-792.

Lombardi, F. & Di Pietro, R. 2010. Transparent security for cloud. Proceedings of the 2010 ACM symposium on applied computing, ACM, 414-415.

Lu, R., Lin, X., Liang, X. & Shen, X. S. 2010. Secure provenance: the essential of bread and butter of data forensics in cloud computing. Proceedings of the 5th ACM

Symposium on Information, Computer and Communications Security, ACM, 282-292.

Manral, V. 2011. Network Working Group D. Zhang Internet-Draft Huawei Intended status: Standards Track M. Bhatia Expires: April 11, 2012 Alcatel-Lucent.

Mao, W. 2004. An identity-based non-interactive authentication framework for computational grids. *Hewlett-Packard Laboratories, Technical Report HPL-2004-96*.

Mowbray, M. & Pearson, S. 2009. A client-based privacy manager for cloud computing. Proceedings of the fourth international ICST conference on COMmunication system softWAre and middlewaRE, ACM, 5.

Neuman, B. C. & Ts'o, T. 1994. Kerberos: An authentication service for computer networks. *Communications Magazine, IEEE,* 32**,** 33-38.

Neuman, C., Yu, T., Hartman, S. & Raeburn, K. 2005. RFC 4120: The Kerberos network authentication service (V5). *Request for Comments*.

Paar, C. & Pelzl, J. 2010. *Understanding cryptography: a textbook for students and practitioners,* Springer.

Pfleeger, C. P. & Pfleeger, S. L. 2006. *Security in computing*, Prentice Hall PTR.

Pippal, S. K., Kumari, A. & Kushwaha, D. S. 2011. CTES based Secure approach for Authentication and Authorization of Resource and Service in Clouds. Computer and Communication Technology (ICCCT), 2011 2nd International Conference on, IEEE, 444-449.

Popovic, K. & Hocenski, Z. 2010. Cloud computing security issues and challenges. MIPRO, 2010 proceedings of the 33rd international convention, IEEE, 344-349.

Ramgovind, S., Eloff, M. M. & Smith, E. 2010. The management of security in cloud computing. Information Security for South Africa (ISSA), 2010, IEEE, 1-7.

Rimal, B. P., Choi, E. & Lumb, I. 2009. A taxonomy and survey of cloud computing systems. INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on, Ieee, 44-51.

Roschke, S., Cheng, F. & Meinel, C. 2009. An extensible and virtualization-compatible IDS management architecture. Xian. 130-134.

Sabahi, F. Virtualization-level security in cloud computing. 2011 Xi'an. 250-254.

Saxena, A. 2008. Dynamic authentication: Need than a choice. Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, IEEE, 214-218.

Schneier, B. 2007. *Applied cryptography: protocols, algorithms, and source code in C*, john wiley & sons.

Shamir, A. 1985. Identity-based cryptosystems and signature schemes. Advances in cryptology, Springer, 47-53.

Shen, Z. & Tong, Q. 2010. The security of cloud computing system enabled by trusted computing technology. Signal Processing Systems (ICSPS), 2010 2nd International Conference on, IEEE, V2-11-V2-15.

Smith, R. E. 2001. *Authentication: from passwords to public keys*, Addison-Wesley Longman Publishing Co., Inc.

Soh, B. & Joy, A. 2003. A novel Web security evaluation model for a one-time-password system. Web Intelligence, WI 2003. Proceedings. IEEE/WIC International Conference on, 2003. IEEE, 413-416.

Sriramulu, B., Chandrasheker, T. & Suresh, T. 2012. A Secure Network Communication Based on Kerberos & MD5. *International Journal of Engineering,* 1.

Steiner, J. G., Neuman, B. C. & Schiller, J. I. 1988. Kerberos: An Authentication Service for Open Network Systems. USENIX Winter, 191-202.

Stinson, D. R. 2006. *Cryptography: theory and practice*, CRC press.

Stone, B. 2008. Twitter, Even More Open Than We Wanted. *Twitter. http://blog. twitter. com/2009/07/twitter-even-more-open-than-we-wanted.html. Retrieved***,** 05-07.

Stubblebine, S. G. & Gligor, V. D. 1992. On message integrity in cryptographic protocols. Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, IEEE, 85-104.

Subashini, S. & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,* 34**,** 1-11.

Sumter, R. L. Q. 2010. Computing, Cloud Security Risk Classification. Oxford, USA.

Tao, J., Marten, H., Kramer, D. & Karl, W. 2011. An intuitive framework for accessing computing clouds. *Procedia Computer Science,* 4**,** 2049-2057.

Tóth, G., Kőszegi, G. & Hornák, Z. 2008. Case study: automated security testing on the trusted computing platform. Proceedings of the 1st European Workshop on System Security, ACM, 35-39.

Un, S., Jho, N., Kim, Y. & Choi, D. 2009. Cloud computing security technology. *ETRI,* 24**,** 79-88.

Van Kesteren, A. 2010. Cross-origin resource sharing. *W3C Working Draft WD-cors-20100727.*

Vance, A. 2010. If your password is 123456, just make it hackme. *The New York Times,* 20.

Vouk, M. A. 2004. Cloud computing–issues, research and implementations. *Journal of Computing and Information Technology,* 16**,** 235-246.

Voyiatzis, A. G., Fidas, C. A., Serpanos, D. N. & Avouris, N. M. 2011. An Empirical Study on the Web Password Strength in Greece. Informatics (PCI), 2011 15th Panhellenic Conference on, IEEE, 212-216.

Wei, J., Zhang, X., Ammons, G., Bala, V. & Ning, P. 2009. Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, 91-96.

Wu, T. D. 1999. A Real-World Analysis of Kerberos Password Security. NDSS.

Yang, J. & Chen, Z. (2010). Cloud computing research and security issues. Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, IEEE, 1-3.

Yu, T., Hartman, S. & Raeburn, K. 2004. The Perils of Unauthenticated Encryption: Kerberos Version 4. NDSS, 4.4-4.7.

Zhang, S., Chen, X., Zhang, S. & Huo, X. 2010a. The comparison between cloud computing and grid computing. Computer Application and System Modeling (ICCASM), 2010 International Conference on, IEEE, V11-72-V11-75.

Zhang, S., Zhang, S., Chen, X. & Huo, X. 2010b. Cloud computing research and development trend. Future Networks, 2010. ICFN'10. Second International Conference on, IEEE, 93-97.

Zhang, S., Zhang, S., Chen, X. & Wu, S. 2010c. Analysis and research of cloud computing system instance. Future Networks, 2010. ICFN'10. Second International Conference on, IEEE, 88-92.

Zhang, X., Du, H.-T., Chen, J.-Q., Lin, Y. & Zeng, L.-J. 2011. Ensure Data Security in Cloud Storage. Network Computing and Information Security (NCIS), 2011 International Conference on, IEEE, 284-287.

Zhou, M., Zhang, R., Zeng, D. & Qian, W. 2010a. Services in the cloud computing era: A survey. Universal Communication Symposium (IUCS), 2010 4th International, IEEE, 40-46.

Zhou, W., Sherr, M., Marczak, W. R., Zhang, Z., Tao, T., Loo, B. T. & Lee, I. 2010b. Towards a data-centric view of cloud security. Proceedings of the second international workshop on Cloud data management, ACM, 25-32.