A NOVEL TRUSTED BASE MODEL FOR CLOUD COMPUTING USING FEDERATED IDENTITY ARCHITECTURE AGAINST IDENTITY THEFT

EGHBAL GHAZIZADEH

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name: EGHBAL GHAZIZADEH

Date of birth : 22 SEPTEMBER 1980

Title : A NOVEL TRUSTED BASE MODEL FOR CLOUD COMPUTING USING FEDERATED IDENTITY ARCHITECTURE AGAINST IDENTITY THEFT

Academic Session: 2012/2013

declare that this thesis is classified as :

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

■ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

SIGNATURE	**SIGNATURE OF SUPERVISOR**
L95236155	**Dr. Mazdak Zamani**
(NEW IC NO. / PASSPORT NO.)	**NAME OF SUPERVISOR**

"I declare that I have read this project, in my opinion this project report has satisfied the scope and quality for the award of the degree of Master of Computer Science (Information Security)."

Signature :

Name of Supervisor : DR. MAZDAK ZAMANI

Date : JANUARY 2013

A NOVEL TRUSTED BASE MODEL FOR CLOUD COMPUTING USING FEDERATED IDENTITY ARCHITECTURE AGAINST IDENTITY THEFT

EGHBAL GHAZIZADEH

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

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

January 2013

I declare that this project report entitled ‘‘A Novel Trusted Base Model for Cloud Computing Using Federated Identity Architecture against Identity Theft” is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

SIGNATURE:

Name : EGHBAL GHAZIZADEH

Date : JANUARY 2013

ACKNOWLEDGEMENT

First, thank you Allah for giving me strength to take up this challenge and with your blessing to complete this study. Second and foremost, I am deeply indebted to my supervisor, Dr. Mazdak Zamani for his patience in assisting, advising and guiding me throughout this project. Next, I am also deeply grateful to my co-supervisor professor Dr. Jamalul-Lail Ab Manan from Malaysian Institute Of Microelectronic Systems (MIMOS) for his precious advices, guidance, continuous and kind help during this project. To the admin staff of UTM AIS, thank you for your continuous help and kind assistance during my presence in UTM AIS.

To my family, a million thanks for your understanding and ardent support extended to me throughout my journey to accomplish this study. Last but not least I want to thank all of my friends especially all my dear classmate who helped and understood me during this project.

DECLARATION of PROJECT STATUS FORM

Student Name : **Eghbal Ghazizadeh**

Student ID : **MC101230**

Supervisor Name : **Dr. Mazdak Zamani**

Course code : **MCU1016**

Academic : **2012/2013**

Title of Project : **A TRUST-BASED NOVEL MODEL FOR CLOUD COMPUTING USING FEDERATED IDENTITY ARCHITECTURES AGAINST IDENTITY THEFT**

The above project work *has / has not**** fulfilled the necessary criteria towards the completion of the project, hence the mentioned student is *ready / not ready**** to submit the project report and orally present his/her project work.

*** **Additional Remarks**

_____

SUPERVISOR'S SIGNATURE

Date :

***Choose appropriately

This form MUST be submitted a week before the drop date in the UTM academic calendar.

ABSTRACT

Cloud computing with the many advantages and benefits has been emphasized by many enterprises. Easy access information, quick deployment, cost efficient, greater business agility are some of the cloud advantages. While ease and cost are two great benefits of cloud but Security and technical issue are significant problems of the cloud. This is a vital component of the cloud's critical infrastructure. Cloud users use this environment to enable numerous online transactions crossways a widespread range of sectors and to exchange information. Especially, identity theft, online fraud, misuse of information should be addressed in the cloud. Increase level of trust is the vital key to decrease identity theft and online fraud. Therefore, cloud vendors should utilize easy-to-use, secure, and efficient identity. Strong Cloud Identity Access Management (IAM) is the best way to deploy trust relationship between users and cloud vendors to guarantee that only authorized users can access to cloud applications. Cloud Identity with Trusted Computing and Trusted Platform Module (TPM) is a strong approach promotes and defines a cloud user's identity where Relying Parties, users, and Service Providers can trust each other. In this study, trusted Single-sign-On has been proposed to mitigate identity theft in the cloud environment. Security architecture, design, efficient identity and access management solution for cloud applications has been identified. Finally, security and efficiency of the proposed model have been evaluated and analyzed and also it has been compared with some of the existing cloud identity methods.

ABSTRAK

Cloud Computing, merupakan satu applikasi yang mempunyai banyak kelebihan dan manfaat, telah diberi penekanan oleh banyak syarikat. Kemudahan capaian maklumat cepat dan cekap, kos yang effektif, dan peluang perniagaan yang lebih besar adalah antara kelebihan Cloud Computing. Walaubagaimana pun, isu keselamatan dan teknikal adalah masalah utama di dalam Cloud Computing. Kedua-dua isu ini adalah komponen critical di dalam Cloud Computing. Pengguna menggunakan aplikasi ini untuk menjalankan pelbagai transaksi atas talian melangkaui pelbagai sektor dan bertukar-tukar maklumat. Kecurian identiti, penipuan atas talian dan salah guna maklumat merupakan isu yang patut ditangani dalam Cloud Computing. Peningkatan tahap kepercayaan merupakan kunci utama untuk mengurangkan masalah-masalah ini daripada berlaku. Oleh itu, penjual Cloud Computing perlu memanfaatkannya dengan mudah, selamat dan cekap identitinya di dalam Cloud Computing. Strong Cloud Identity Access Management (IAM) merupakan cara terbaik untuk menggunakan hubungan antara pengguna dan vendor dalam hanya menjamin kesahihan pengguna. Cloud Identity dengan Trusted Computing dan Trusted Platform Module (TPM) merupakan satu pendekatan yang bijak dalam mempromosi dan mendefinisikan idenditi pengguna Cloud Computing yang mana pihak-pihak berkaitan, pengguna dan penjual servis boleh mempercayai antara satu sama lain. Kajian ini mencadangkan penggunaan Single-Sign-On untuk mengurangkan kecurian identiti di dalam persekitaran Cloud Computing. Reka bentuk keselamatan, identiti yang cekap dan penyelesaian bagi pengurusan capaian telah dikenalpasti. Secara keseluruhan, keselamatan dan kecekapan model yang dicadangkan telah dianalisis dan dibandingkan dengan beberapa kaedah Cloud Identity yang sedia ada.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The new definition of cloud computing has been born by Amazon's EC2 in 2006 in the territory of information technology. Cloud computing has been revealed because of Commercial necessities and make a suitable application. According NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources." Resource pooling, on-demand self-service, rapid elasticity, measured serviced and broad network access is five vital features of cloud computing. Other definitions of cloud are executed, supplying material, organized, and infrastructure based that they should be rapidly provisioned and unrestricted automatically access or service provider interaction (Grance, 2009).

"The push for growth in 2011 is leading to changes in emphasis," said M. Chiu. Also he said that IT is now recognized by business transformation, or better said that digitalization is accelerating. Cloud computing and IT management according statistics is top ten business and technology priorities of Asian CIOs strongly. Cloud computing, IT management, mobile technology, Virtualization, business intelligence, infrastructure, business process management, data management, enterprise application, collaboration technologies, and network data communication are top ten technology priorities. Cloud will move to become the most popular business in the worldwide. It shows business and technology has been

dominated by cloud computing. Therefore, thousands of new business release every day about cloud computing technology (Gartner, 2011).

1.1.1 Security and Cloud Computing

While cost and ease are two top benefits of cloud, trust and security are two concerns of cloud computing users. Cloud computing has claimed insurance for sensitive data such as accounting, government, and healthcare and bring opportuneness for end users. Virtualization, multi tenancy, elasticity, and data owner which traditional security techniques cannot solve security problems for them are some new issues in the cloud computing. Trust is one of the most important issues in cloud computing security; indeed, two trust questions are in cloud computing. The first question is, are cloud users trust cloud computing and second question is, how could make a trusted base environment for cloud users? Besides these questions, cloud users and vendors when transfer their businesses to cloud also have these questions. Will cloud service providers trustworthy? Will the cloud enterprises could more attractive to hackers? All these concerns and questions encounter to cloud computing. These questions address these concerns when considering moving critical application, cloud must deliver a sufficient and powerful security level for the cloud user in term of new security issues in cloud computing (Rodriguez *et al.*, 2006).

Abbadi and Martin (2011) illustrated that trust is not a novel concept but users need to understand the subjects associated with cloud computing. Technology and business perspective are two sides of trust computing. The emerging technologies that best address these issues must be determined. They believed that trust means an act of confidence, faith and reliance. For example, if a system gives users insufficient information, they will give trust less to the system. In contrast, if the system gives users sufficient information, they will trust the system well. There are some important issues with trust. Control of our assets is the most important security issue in cloud computing because users trust a system fewer when users do not have much control of it. For example, bank customers use a confidentiality ATM

because when they withdraw money from an ATM machine, they trust it (Abbadi and Martin, 2011).

Cloud computing suppliers should prepare a secure territory for their consumers. A territory is a collection of computing environments connected by one or more networks that control the use of a common security policy. Regulation and standardization are another issue of trust that PGP, X509, and SAML are three examples for establishing trust by using standard. Access management, trust, identity management, single sign-on and single sign-off, audit and compliance and configuration management are six patterns that identify basic security in cloud computing . Computer researchers believe that trust is one of the most important parts of security in cloud computing. There are three distinct ways to prove trust. First, we trust someone because we know them. Second, we trust someone because the person puts trust on us. Third, sometimes we trust someone because an organization that we trust vouches for that person. In addition, there are three distinct definitions of trust. First, trust means that the capability for two special groups to define a trust connection with an authentication authority. Second, trust identifies that the authority can exchange credentials (X.509 Certificates). Third, it uses those credentials to secure messages and create signed security token (SAML). The main goal of trust is users can access a service even though that service does not have knowledge of the users (Carmignani, 2010).

Trusted computing growth with technology development and raised by the Trusted Computing Group. Figure 1.1 shows that it is a response to user's security concerns. Trusted Computing is the industry's response to growing security problems in the enterprise and is based on hardware root trust. From this, enterprise system, application and network can be made safer and secure. With trusted computing, the computer or system will reliably act in definite ways, and thus works in specific ways, and those performances will be obligated by hardware and software when the owner of those systems enabled these technologies. Therefore, using trust cause computer environments safer, less prone to viruses and malware, and thus more consistent.

In addition, Trusted Computing will permit computer systems to propose improved security and efficiency. The main aim of trusted computing has prepared a framework for data and network security that cover data protection, disaster recovery , encryption, authentication, layered security, identity, and access control (TCG, 2011).

Figure 1.1: Trusted Computing (TCG 2011)

1.1.2 Cloud computing and Federated Identity

One of the problems with cloud computing is the management and maintenance of the user's account. Because of the many advantages of cloud such as cost and security, identity management should promises all the cloud advantages. Therefore, the new proposed model and standards should make use of all the cloud advantages and prepare an environment to ease use all of them

Private cloud, Public Cloud, Community cloud, and Hybrid cloud are four essential types of cloud computing that named by cloud users and venders. In the community cloud definition shares infrastructure for definite community between organizations with common concern and private or internal cloud shares cloud

services between a classified set of users. Attend to establish the best digital identity for users to use is the most important concern of cloud providers. Cloud prepares a large amount of various computing resources; consequently, diverse users in the same system can share their information and work together. Classified identity and common authentication are an essential part of cloud authentication and federated identity acts as a service based on a common authentication even though it is broadly used by most important companies like Amazon, Microsoft, Google, IBM, and Yahoo (Yan *et al.*, 2009).

Today's an internet user has about thirteen accounts that require user names and passwords, and enters about eight passwords per day. It becomes a problem and internet users face the load of managing this huge number of accounts and passwords, which leads to password tiredness; indeed the burden of human memory, password fatigue may cause users to use password management strategies that reduce the security of their secured information. Besides, the site centric Web makes online and each user account is created and managed in a distinct administrative domain, profile man arrangement and personal content sharing will be difficult. SSO or Web single sign-on systems are invited to address the mentioned problem with the site centric. Web users, identity provider and identity provider are three parts of SSO and they have a distinct role in identity scenario. An IDP collects user identity information and authenticates users, while an RP trusts on the authenticated identity to make authorization decisions. OpenID is a promising and open user centric Web SSO solution. More than one billion OpenID accounts have been permitted to use service providers according to the OpenID Foundation. Furthermore, the US Government has cooperated with the OpenID Foundation in the provision of the Open Government Initiative's pilot acceptance of OpenID technology (Sun *et al.*, 2011).

Single username and password is an essential part of single sign-on protocols in term of authenticate crossway numerous systems and applications, efforts to statement privacy and security issues for web users. There are three widespread Web SSO implementations that named OpenID, Passport/Live ID, and SAML will be enclosed along with details of common weaknesses and issues (Wang, 2011). Web

SSO solutions were initially advanced by numerous educational institutions in the mid-1990s. For examples, Cornell University's SideCar, Stanford University's WebAuth and Yale's Central Authentication System (CAS) were entirely early reformers in the field (Hodges, 2008).

SSO today has a critical role in cloud security and becomes essential to realize how secure the deployed SSO mechanisms truly are. Nevertheless, it is a new idea and no previous work includes a broad study on commercially deployed web SSO systems, a key to understanding to what extent these real systems are subject to security breaches (Armando, 2008). In addition, Wang et al showed that Weaknesses that do not illustrate on the protocol level could be brought in by what the system essentially agree to each SSO party to do (Wang *et al.*, 2012b).

1.2 Background of the problem

Madsen et al (2005) defined some problems of federated identity and illustrated that FIM or Federated Identity Management established on standard permits and simplifies joining federated organizations in term of sharing user identity attributes, simplify authentication and allowance or deny using service access requirements. The definition of SSO is Using it facility user authenticates only one time to home identity provider and logged in to access successive service providing service providers within the federated. There are some active problem and concern in a federated identity environment like to misuse of user identity information through SSO capability in service providers and identity providers, user's identity theft, service providers and identity providers, and trustworthiness of the user. Federated identity has identified regardless of good architectures still has some security problems that should be considered in the real estate implementation (Madsen *et al.*, 2005).

In addition standard and facilities, speed and security are two user friendly issues of identity management. Users in federated identified must share their identities with numerous service providers. Consequently, personal information of

the user has been compromised during implementing a Federated Identity. Rodriguez et al (2006) discovered Federated identity Architecture (FIA) as a way for solving vulnerabilities. There are three architectures for implementing security issue in FIA which named Liberty Alliance, Shibboleth, and WS- Federation (Rodriguez *et al.*, 2006).

Archer et al (2011) argued that one of the most common attacks is identity theft because it is very problematic to identify until the harm is done. They believed that in the insecure channel is most of the identity theft attack have been occurred. Besides identity attack, legal compliance and privacy guaranty is another security problem with identity federated. For example, the current FIA has not a powerful way user's information. P3P has been released as a standard and a project for improving FIA that established by the W3C in term of creating a usefully integrated into the FIA. Moreover, PKI integration, AAA integration, and P2P application support are another attack that identity provider has to consider in trust security (Archer *et al.*, 2011).

There are five security issues of identity and attribute that computer scientific attend to improve security of them and implement a security transformation environment between users and vendors.

i. The connection to Human Resources is difficult as HR has been frequently only the master source for staff on systematic payroll.

ii. There are typically no authoritative information sources for partner information and their devices that it is most important for me.

iii. The capability to delivery other entities does not exist in most organizations that also it is important in my study.

iv. Self-asserted Identity public has been provided by identity service and it does not cover to the other Entity types.

Most organizations do not have the ability to off-board another organization or on the other hand De-provisioning needs to extend to all entities. Hence, the vendors should agree to finish and revoke the code from operating on systems when it is found to be faulty or obsolete. These issues and the lack of provisioning standards stress the necessity for good planning and a complete approach to how Identity Attributes, accounts, and Lifecycle management of all Entity-types will operate in the cloud eco-system being settled (Archer *et al.*, 2011).

Identified by Suriadi et al (2009), "one of the main problems with the model is user privacy. In an SSO environment, relying parties (RP) or service providers (SP). "It can also be gathering information about a user of the information that they get from the identity providers (IDP). They also analyzed that sharing of user's information by malicious IDPs and SPs can disclose a complete user's identity and activities"(Suriadi *et al.*, 2009). In addition Suriadi et al (2009), Zarandioon et al shows that this issue has caused web users to be cautious of SSO implementations and is one of the main causes for the lack of widespread adoption (Zarandioon *et al.*, 2009).

Wang (2011) discovered another problem of federated identity that is switching authentication mechanisms to an SSO solution. It means further education of the users is required and possible loss of the user base if the transition is not smoothly executed. Also worsening the situation is the lack of demand from users for a Web SSO solution. Studies have shown users are already satisfied by their own password managers (Wang, 2011).

1.3 Problem Statements

Digital Identity information must be exchanged between different service provider in the by considering security and trust. Based on CIA, confidentiality and integrity are two top security issues for digital identity and by using these factors we can keep safe our information. There are many levels of trust by considering identity and attribute for users in the data transaction. Therefore, management of identities in a secure and fast way for access computer resources is important for users and vendors. Madsen et al (2005) studied that service providers have problem to get the share identities and attribute. Online identity theft is the most critical problem for implementing of architecture in federated identity. Strong authentication, preventing theft, and decreasing risk can be achieved with a of good establishing federated identity management (Madsen *et al.*, 2005).

OpenID is one of the common standards that uses for federated identity in term of security. I will focus on Phishing attack on OpenID protocol and it will be explained step by step. Based on Figure 1.2 every system involves tree party that named user or the user's browser, relying party or RP, and identity provider or id which is the most important part of security and there are the most significant challenges in this part of identity security. It has been shown Figure 1.2 that OpenID use step by step way for exchanging messages and it is as below.

- In step 1, the pattern is saying the user's URL to RP.
- In step2, RP defines the User's location.
- In step 3 and 4, RP ask the user by considering the IP to get an authentication token. In this step RP should determines that this IP is the user who asking the request for authentication that normally shows by asking user name and password.
- In step 5 and 6, the IDP deliver token to the user's browser to send to the RP that has been shown in step 5 and 6. At the end of authentication part IP and RP distinguish each other.

Finally, the registration back to IdP and the connection will be established.

According to OpenID standard Kim (2007) studied and argued that then it will be weak for Phishing attack. Therefore, based on Figure 1.3, the attackers try to do another way to Phishing and identity theft. The Kim proposed Phishing attack described as below:

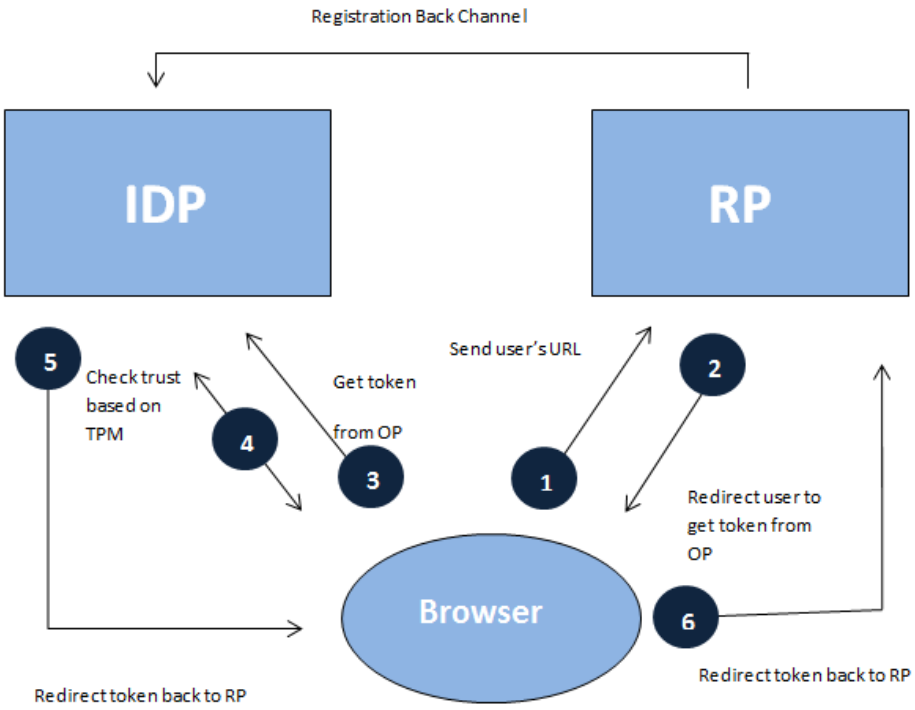

Figure 1.2: Authentication in OpenID (Kim, 2007)

- In step1, the web user by mistake goes to the evil site and the user sends to evil RP her/his URL and her/his location IDP.
- In step2, he or she redirects to the scooper contacts instead of legitimate IDP.
- In step 3 and 4, are the evil scooper contacts the legitimate IDP and pulls down an exact copy of its login experience. Convinced she or he is talking to her or his IDP; the user posts her or his credentials, which can now be used by the Evil Scooper to get tokens from the legitimate IDP.
- In step 5 and 6, token can then be used to gain access to any legitimate RP.

Redirection to the home site is under the control of the evil party is the problem here, and the user gives that party sufficient information to use by the evil. Further, the whole process can be fully automated (Kim, 2007).

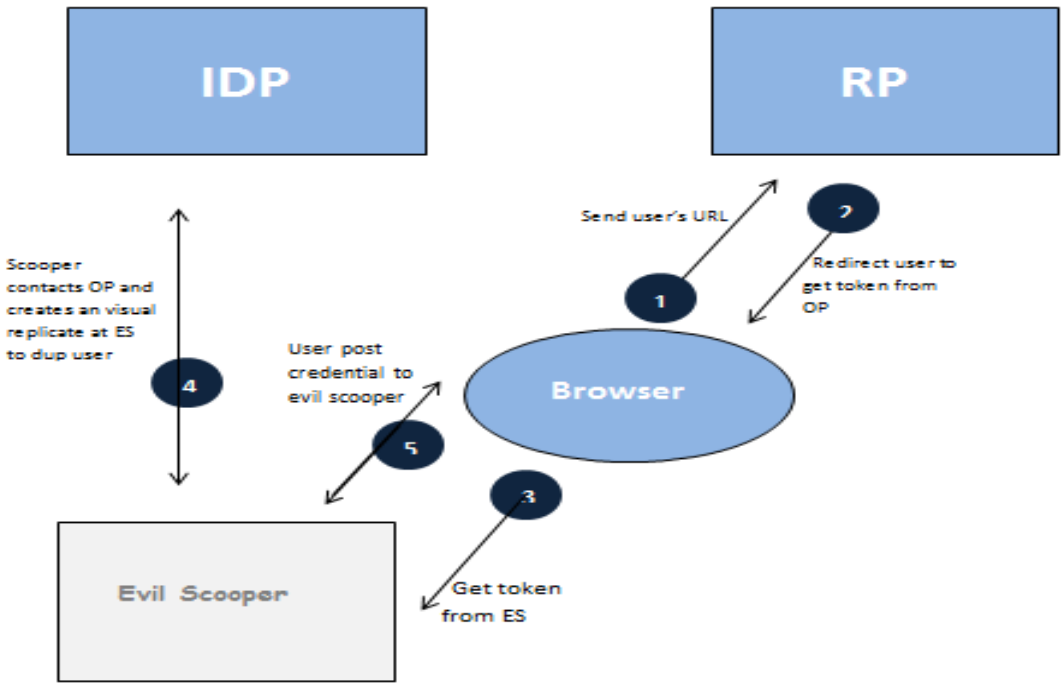

Figure 1.3: Identity theft in OpenID (Kim, 2007)

1.4 Project Objectives

The objectives of this study are as below:

i. To investigate existing cloud identity based models and their security architecture.
ii. To propose a model based on federated identify architecture for establishing trusted computing to mitigate identity theft.
iii. To analyze the propose model for establishing trust in cloud computing and comparison with other models.

1.5 Research Questions

The main questions this research motivates to answer are as follows:

1. What are the approaches that eliminate security issues by proposing a novel model for federated identify?
2. How to develop a new model regarding to the enhancement of security in cloud identity?
3. How to test and evaluate the performance of this model and comparison with other models?

1.6 Project Aim

Andre Durand, Ping Identity CEO said that “We live in an amazing time – the breadth of consumer services and transactions available online is endless and when it comes to securing these transactions, identity is the new perimeter,” The aim of this study is to enable secure and privacy, convenient online transactions for cloud users. This enhancement could be used to access cloud services such as health care service providers and various government agencies. The proposed model should be secure and simple through cloud identity management because users' identities hold excellent power and require excellent responsibility. Therefore, The aim of study is to investigate and evaluate some federated architecture to eliminate security faults and issues among authentication mechanism in order to provide a robust model and enhance the overall trusted with cloud security. Therefore, by having secure underlying, it can be more likely to achieve authentication secure and reliable identities and attributes in a cloud computing environment.

1.7 Scope of the Study

This research focuses on trust in cloud computing. Trust in the cloud is a critical part in cloud security. As it has been mentioned in the introduction, access management, trust, identity management, single sign-on and single sign-off, audit and compliance, and configuration management are six patterns that identify basic security in cloud computing. This study will focus on federated identity which is used for user identity management. In addition, there are several federated identity architectures for managing this problem. Hub and Spoke Model, Free Form Model, and Hybrid model are three models for implementing federated identify in trusted computing. Although, there are some remaining issues and challenges in these management trust models so this study will focuses on the hybrid model to enhance and propose architecture.

Stopping Phishing attacks completely is very difficult. Therefore, the aim of this study is to decrease the number of identity theft and Phishing attacks. Trusted computing that applies in this study try to decrease the success probability of Phishing attack and identity theft. However, as TPM in OpenID has been leveraged. Other attacks as Apart from Phishing, attempt to deal sensitive information as an asset of users. Furthermore, in this study attacks that compromise users' computers have been ignored. Also key loggers and rootkits, and cookie attacks look like cross site request forgery (CSRF) attacks and cross site script (XSS) attacks have been ignored. Finally, attacks which compromise the integrity of the web site will not discuss.

In conclusion, this study's scope is single sign on authentication by using some of the protocols look like SAML, OAuth, and OpenID. As it has been mentioned, today commonly in many APIs uses these authentication models. Visual Studio 2012 and SQL Server 2012 have been used for simulation of the proposed model.

1.8 Summary

As discussed in the previous sections, nowadays Phishing attack and identity theft are the most significant threats in the cloud authentication area. SAML, OpenID, and OAuth are some of the federated identity approaches which attend to mitigate these threats. There are insufficient studies that have been proposed within the journals, white paper, conference, and research paper but as mentioned in detail most of them have not considered trusted computing and worked in the network area. Thus, in this research based on Trusted Computing, Federated Identity Management, Single Sign On, and Cloud Computing has been tried to propose a trusted base model base on federated identity to mitigate identity theft and Phishing attack in the cloud computing environment.

REFERENCES

Abbadi, I. M., and Martin, A. (2011). Trust in the Cloud. *Information Security Technical Report*.

Ahmad, Z., Ab Manan, J. L., and Sulaiman, S. (2010). User Requirement Model for Federated Identities Threats.

Archer, D. C. J., Nils Puhlmann, Alan Boehme, Paul Kurtz, and Reavis, J. (2011). Security guidance for critical areas of focus in cloud computing v3.0. *Cloud Security Alliance*.

Armando, A. C., R. Compagna, L. Cuellar, J. Tobarra, L. (2008). Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps 1-10.

Badger, L., Grance, T., Patt-Corner, R., and Voas, J. (2011). Draft cloud computing synopsis and recommendations. *NIST Special Publication.* 800, 146.

Barrett, D., and Kipper, G. (2010). *1 - How Virtualization Happens*. In *Virtualization and Forensics* (pp. 3-24). Boston: Syngress.

Carmignani, A. (2010). Identity federation using SAML and WebSphere software.

Cooke, P. (2010). Black Hat TPM Hack and BitLocker. from http://blogs.windows.com/windows/b/windowssecurity/archive/2010/02/10/black-hat-tpm-hack-and-bitlocker.aspx

credentica.com. (2012). trusted computing. from http://www.credentica.com/trusted_computing.html

Dell. (2012). Red Flags. from http://www.secureworks.com/consulting/security_and_governance_program_development/red_flags/

Ding, X., and Wei, J. (2010). A Scheme for Confidentiality Protection of OpenID Authentication Mechanism 310-314.

Donovan, M., and Visnyak, E. (2011). Seeding the Cloud with Trust: Real World Trusted Multi-Tenancy Use Cases Emerge. from http://www.ittoday.info/Articles/Trust/Trust.htm

Fazli Bin Mat Nor, K. A. J., Jamalul-lail Ab Manan. (Nov - 2012). Mitigating man-in-the-browser attacks with hardware-based authentication scheme. *International Journal of Cyber-Security and Digital Forensics (IJCSDF).* Vol. 1, No. 3, 6.

Feng, Q., Tseng, K. K., Pan, J. S., Cheng, P., and Chen, C. (2011a). New Anti-phishing Method with Two Types of Passwords in OpenID System. *Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on*. 69-72.

Feng, Q., Tseng, K. K., Pan, J. S., Cheng, P., and Chen, C. (2011b). New Anti-phishing Method with Two Types of Passwords in OpenID System 69-72.

Ferg, B. (2007). OpenID Authentication 2.0—Final. *OpenID Community*.

Gartner. (2011). Gartner Survey of CIOs in Asia Shows Cloud Computing Tops the Technology Priority List as Businesses Focus on Growth in 2011. from http://www.gartner.com/it/page.jsp?id=1729814

Gawasane, V. (2012). All About Software Testing, Tools and Tutorials. from http://softwaretesting-qaqc.blogspot.com/2012/06/before-getting-into-world-of-software.html

Grance, P. M. a. T. (2009). The nist definition of cloud computing.

Hodges, H., Johansson,Morgan. (2008). Towards Kerberizing Web Identity and Services. *Kerberos consortium*.

Huang, C. Y., Ma, S. P., and Chen, K. T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications.* 34(4), 1292-1301.

Huang, H. Y., Wang, B., Liu, X. X., and Xu, J. M. (2010). Identity federation broker for service cloud. *2010 International Conference on Service Sciences, ICSS 2010, May 12, 2010 - May 14, 2010*. Hangzhou, China: 115-120.

Hwang, K., and Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *Internet Computing, IEEE.* 14(5), 14-22.

Jasti, A., Shah, P., Nagaraj, R., and Pendse, R. (2010). Security in multi-tenancy cloud. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology, ICCST 2010, October 5, 2010 - October 8, 2010*. San Jose, CA, United states: 35-41.

Jiang, J., Duan, H., Lin, T., Qin, F., and Zhang, H. (2011). A federated identity management system with centralized trust and unified Single Sign-On 785-789.

Khattak, Z., Sulaiman, S., and Manan, J. (2010). A study on threat model for federated identities in federated identity management system 618-623.

Khiabani, H., Manan, J. L. A., and Sidek, Z. M. (2009). A study of trust & privacy models in pervasive computing. *Technical Postgraduates (TECHPOS), 2009 International Conference for*. 1-5.

Kim, C. (2007). Integrating OpenID and Infocard from http://www.identityblog.com/?p=659

Latze, C., and Ultes-Nitsche, U. (2007). Stronger authentication in e-commerce: How to protect even naive user against phishing, pharming, and mitm attacks. *Proceedings of the IASTED International Conference on Communication Systems, Networks, and Applications*. 111-116.

Leandro, M. A. P., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., and Westphall, C. B. (2012). Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth 88-93.

Leicher, A., Schmidt, A., and Shah, Y. (2012). Smart OpenID: A Smart Card Based OpenID Protocol. *Information Security and Privacy Research*, 75-86.

Li, X. Y., Zhou, L. T., Shi, Y., and Guo, Y. (2010). A trusted computing environment model in cloud architecture 2843-2848.

Madsen, P., Koga, Y., and Takahashi, K. (2005). Federated identity management for protecting users from ID theft 77-83.

Mat Nor, F. B., Abd Jalil, K., and Ab Manan, J. (2011). Remote User Authentication Scheme with Hardware-Based Attestation. *Software Engineering and Computer Systems*, 437-447.

Ping-Identity. (2012). Internet-Scale Identity Systems: An Overview and Comparison.

Rodriguez, U. F., Laurent-Maknavicius, M., and Incera-Dieguez, J. (2006). Federated identity architectures.

Rouse, M. (2007). trusted computing. from http://searchsecurity.techtarget.com/definition/trusted-computing

Schäffer, B. (2011). Authentication and Authorization in Spatial Data Infrastructures.

Sha, S., Yan, W. Q., and Li, M. Z. (2010). A secure SSO protocol without clock synchronization V3-422-V423-424.

Spencer, T. (2012). Identity in the cloud. *Computer Fraud & Security.* 2012(7), 19-20.

Sun, S. T. (2012). Simple But Not Secure: An Empirical Security Analysis of OAuth 2.0-Based Single Sign-On Systems.

Sun, S. T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., and Beznosov, K. (2011). What makes users refuse web single sign-on?: an empirical investigation of OpenID 4.

Suriadi, S., Foo, E., and Jøsang, A. (2009). A user-centric federated single sign-on system. *Journal of Network and Computer Applications.* 32(2), 388-401.

Tan, X., and Ai, B. (2011). The issues of cloud computing security in high-speed railway. *2011 International Conference on Electronic and Mechanical*

Engineering and Information Technology, EMEIT 2011, August 12, 2011 - August 14, 2011. Harbin, China: 4358-4363.

TCG. (2011). Trusted Computing. from http://www.trustedcomputinggroup.org/trusted_computing

TCG. (2012). Trusted Computing. from http://www.trustedcomputinggroup.org/trusted_computing

Thibeau, D., and Drummond, R. (2009). Open trust frameworks for open government: Enabling citizen involvement through open identity technologies. *White paper, OpenID Foudation and Information Card Foudation*.

Urien, P. (2010). An OpenID provider based on SSL smart cards 1-2.

Wang. (2011). An Analysis of Web Single Sign-On.

Wang, R., Chen, S., and Wang, X. (2012a). Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided

Security Study of Commercially Deployed Single-Sign-On Web Services.

Wang, R., Chen, S., and Wang, X. F. (2012b). Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services.

Yan, L., Rong, C., and Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. *1st International Conference on Cloud Computing, CloudCom 2009, December 1, 2009 - December 4, 2009*. Beijing, China: 167-177.

You, J. H., and Jun, M. S. (2010a). A Mechanism to Prevent RP Phishing in OpenID System 876-880.

You, J. H., and Jun, M. S. (2010b). A Mechanism to Prevent RP Phishing in OpenID System. *Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference on*. 876-880.

Zarandioon, S., Yao, D., and Ganapathy, V. (2009). Privacy-aware identity management for client-side mashup applications 21-30.