AN EFFICIENT MIX AND MATCH ARCHITECTURE WITH SINGLE SIGNON FOR INFORMATION DISSEMINATION

[1]Palanisamy A M, [2]Premalatha K, [3]Parthiban K,
[1]PG Scholar, [2] Professor,Dept. of CSE,Bannari Amman Institute of Technology,Sathyamangalam
[3]Software Engineer,Dept. of IT,Bannari Amman Institute of Technology,Sathyamangalam
Email: [1]Palanisamy.cs13@bitsathy.ac.in, [2]premalathak@bitsathy.ac.in, [3]parthibank@bitsathy.ac.in

Abstract - The growth of Internet online services has been very quick in recent years. Each online service requires Internet users to create a new account to use the service. The problem can be seen when each user usually needs more than one service, and consequently, has numerous accounts. These numerous accounts have to be managed in a secure and simple way to be protected against identity theft. Single Sign On (SSO) and Open ID have been used to decrease the complexity of managing numerous accounts required in the Internet identity environment. This project proposes cloud-based single signon model for reliable accessing to cloud computing SaaS application. The proposed method has been analyzed by means of better efficiency and security comparing with existing methods.

IndexTerms: AES- Advanced Encryption Standard, SaaS- Software as a Service, PaaS- Platform as a Service, IaaS- Infrastructure as a Service, SSL- Secure Socket Layer, SSO- Single Sign On, PMA- Password Manager Agent, SSOCS- Single Sign On Cloud Server, SSOSA- Single Sign On SaaS Application

1.INTRODUCTION

The use of Internet and new technologies nowadays, for business and for the current users, is already part of everyday life. Any information is available anywhere in the world at any time. That was not possible few years ago. Nowadays it have arisen a lot of possibilities of access to public and private information like internet speed access or the deployment of mobile dispositive that allow the connection to Internet from almost everywhere.

Today a lot of people are consulting their mail online through webmail clients, writing collaborative documents using web browsers, creating virtual albums to upload their photos of the holidays. They are running applications and storing data in servers located in Internet and not in their own computers. Something as simple as enter in a web page is the only thing a user needs to begin to use services that reside on a remote server and lets him share private and confidential information, or using computing cycles of a pile of servers that he will ever see with his own eyes. And every day its being used more this services that are called cloud computer services. That name is given because of the metaphor about Internet, as something than the user see like a cloud and cannot see what’s inside.

This services can be offered by free or by paying by demand (pay for consume), can be simply like a function calling (like asking the temperature in some city in the world for include it in a web page) or complex (like the usage of a virtual machine with its own operating system, applications and storage space for running applications).

This means that many users and organizations can avoid install some applications in their computer or can have more computational power using cloud computer through internet, or they can make their own private cloud to manage it completely, or they can use both options for the moments of high demand of consume.

2.LITERATURE REVIEW

Security of federated identity has become an interesting research area in the last few years and been appealed by huge companies like IBM. Security concern in federated environment has been addressed by Huang and Wang in. They proposed an identity federation broker that introduced a trusted third party between SP and the IDP.

According to Freier et al study in [14], there are several different formations of identity management regarding ensuring access control in Cloud Computing environment which is named In-house, IDaaS. The users with In-house identity configuration are able to manage and issue their identity. If identity is configured and issued by outsource company, it is called Identity as a service or IDaaS. IDaaS is divided in to three categories which have been commercially offered in the market. Complete management, pseudonyms implementation, and independently IDaaS implementation are three configuration parts of IDaaS. Furthermore, the wide area of security via security guidance for critical areas of focus in cloud computing has been discussed by cloud security alliance.

Zhang et al in [13] presented the concept of trusted clouds and also discussed the challenges of cloud security and compliance. In this study, the necessities of rusted clouds are argued. Furthermore, four usage models are introduced in order to enable a trusted computing infrastructure.

Fengming in [12] explores the capabilities available to the mobile smartphone platforms to secure such participation, and describes architecture for adding trust management to the exchange of media to and from a smartphone user.

Ghazizadeh et al in [1] suggested a model in order to solve identity theft in the cloud.This model incorporates trusted computing, Federated Identity Management, and OpenID Web SSO. This proposed model is evaluated through BLP confidential model, security analysing and simulation.

OpenID in comparison with Security Assertion Mark-up Language (SAML) is authentication exchange protocol for identity management in the internet, but SAML is designed for limited or small scale Identity Management, and also OpenID is much easier to be deployed and implemented. SAML’s parties are based on trust while the parties in OpenID basically trust on DNS system to find the address of IDP and rely it in any case. Therefore, DNS cache poisoning and DNS hijack are common impersonation attacks in OpenID environment[11].

3.SINGLE SIGN ON

Authentication is the process by which a computer system confirms the identity of an individual, usually based on a name and password. Single sign-on (SSO) is a specialized form of authentication that allows a user to authenticate once in a particular system and thereafter gain access to multiple systems and services. Single sign-on relieves the burden on the user of having to enter authentication information multiple times (e.g., once for every service accessed). In addition, single sign-on facilitates the application of a consistent authentication policy across a domain based on centralized management of authentication.

Numerous single sign-on solutions have been developed by industry and academia. SSO solutions can be organized into two main categories: those that deal with a single set of credentials, and those that deal with multiple sets of credentials. The difference between the two categories is the number of user credentials handled by the SSO solution in a deployment environment. A SSO solution dealing with a single set of credentials only has to handle one type of authentication credential per user; for example, one common authentication mechanism is a username and password, so in SSO all the systems in the domain generally support the same authentication mechanism and accept the same password for an individual user.

4.INTRODUCTION TO PROPOSED MODEL TOOLS

The proposed model was designed by using concepts of agent, version 3.0 of Secure Socket Layer (SSL), Advanced Encryption Standard (AES) model, a middle cloud server, and a middle SaaS application to apply a secure and efficient SSO model for accessing to cloud computing environments.

4.1 Password Manager Agent (PMA)

Password Manager Agent is a client-based agent that is installed on browsers as an extension. The main obligation of PMA is to communicating with the single sign on cloud server for simultaneously sign on various SaaS applications.

4.2 Single Sign On Cloud Server (SSOCS)

Single sing on cloud server is a middle-based cloud server that has two main servers: Password Cloud Server (PCS) and Keys Cloud Server (KCS). Different usernames and passwords are encrypted and stored in PCS and the all keys are stored in KCS.

4.3 Single Sign On SaaS Application (SSOSA)

SSOSA is a cloud-based application that manages usernames and passwords, encrypts them and stores in PCS, stores keys in KCS, decrypts usernames and passwords, connects to various cloud computing environments and SaaS applications, and provides user requests from various applications to the client.

4.4 Secure Socket Layer (SSL)

SSL is used for transferring data from PMA and SSOSA. Moreover, it is used for the communications between SSOSA and various SaaS applications.

4.5 Advanced Encryption Standard (AES)

AES is a private key cryptography algorithm that is used for encryption data by SSOSA and storing them in PCS. In addition keys are stored in KCS. According to the nature of project, AES-192 or AES-256 has been chosen for cryptography processes.

5. PROPOSED ALGORITHM

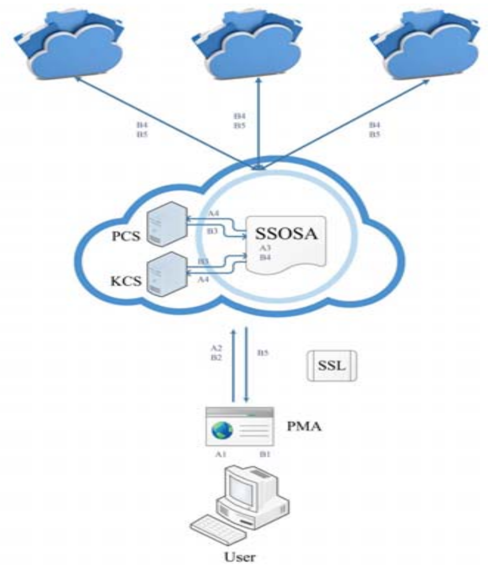

Figure 1: System Overview

The proposed algorithm has been presented in this section according to described tools. Furthermore, Figure. 1 Shows this algorithm in brief.

5.1 Storing Usernames and Passwords

- User installs PMA as an extension in his browser.
- By using PMA and singing on to this extension, user can access to SSOSA for storing his various usernames and passwords.
- SSOSA generates keys according to AES-256 and encrypts given usernames and passwords.
- After the encryption process, encrypted data are stored on PCS and keys are stored on KCS.

5.2 Accessing to Various SaaS Applications

- User accesses to SSOSA by signing on PMA.
- User requests to access on a specific cloud-based SaaS application from SSOSA.
- SSOSA gets encrypted username and password from PCS and related keys from KCS.
- Username and password are decrypted and sent to the requested SaaS application for signing on process.

- After confirmation process, data are transferred from the SaaS application to SSOCS and after that transferred to the user browser.

5.3 Specifications of the Proposed Model

5.3.1 Using a Cloud Server for Storing Passwords

In the proposed model, usernames and passwords are stored in a cloud-based server and accessible anytime and anywhere according to cloud computing concepts. Accordingly, the proposed model is more efficient and accessible in comparison with similar client-based password manager and single sign on systems. Furthermore, usernames and passwords are stored encrypted in PCS by one of the most powerful symmetric keys cryptography algorithms (AES-256 or AES-192) for increasing the security and reliability of the model.

5.3.2 Different Cloud Servers for Passwords and Keys

Usernames and passwords are encrypted and stored in PCS and all cryptography keys are stored in a different cloud server. This separation helps to increase the security of passwords according to the power of AES cryptography algorithm. This means, if the encrypted data are lost by possible attacks or unpredictable events, the attacker need 1.1 × 1017 possible combinations for decrypting each password and this amount of combinations needs 3.31 × 1056 years approximately [12]. This amount of time shows that passwords are stored quit safe and after a possible attack, users have enough time to change their passwords without any concerns.

5.3.3 Using SSL during Data Transmission

SSL is the most appropriate solution for providing security in data transmission process [13]. Accordingly, SSL was established in the proposed model in data transmissions between PMA and SSOSA for providing a secure and reliable transmission.

5.3.4 Accessing to SSOSA with Browser Extension

User can access to the single sign on cloud server by log in to an installed extension in his browser. This extension increases the dependency of the single sign on process to web browser and can use the security and error-handling tools of web browsers without establishing a new stand-alone application.

6. PERFORMANCE EVALUATION

The simulation process was done to compare the proposed model with a similar client-based single sign on system. Accordingly, a client-based single sign on prototype was implemented and run in a 2.40 GHz Intel® Core ™ i5 CPU and 4.00 GB RAM pc (Com-A). Moreover, a cloud-based SaaS application was simulated in a 3.06 GHz 6-Core Intel® Xeon CPU and 64.00 GB RAM (8×8GB) Mac Pro Server (Com-B) and was connected to Com-A (as PMA) via a wireless network. Furthermore, Microsoft Office 365, Google Docs, Microsoft Outlook, and Amazon have been chosen as target SaaS Applications. The following figure shows the simulation process in details:

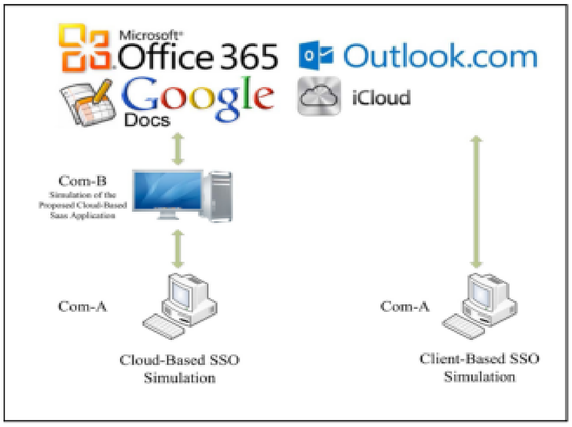
Microsoft Office 365
Outlook.com
Google Docs
iCloud
Com-B
Simulation of the Proposed Cloud-Based Saas Application
Com-A
Com-A
Cloud-Based SSO Simulation
Client-Based SSO Simulation

Figure. 2: Simulation of the Proposed Model

The process of storing usernames and passwords was simulated as follows:

- Cloud-Based SSO: Sending details from Com-A, encrypting and storing data in Com-B.
- Client-Based SSO: encrypting and storing details in Com-A.

The following table shows the time of storing process in both models according to AES-192 and AES-256 algorithms:

TABLE 1. PERFORMANCE OF THE ALGORITHM

Algorithm	Cloud-Based SSO (ms)	Client-Based SSO (ms)
AES-192	2754	7345
AES-256	3124	9247

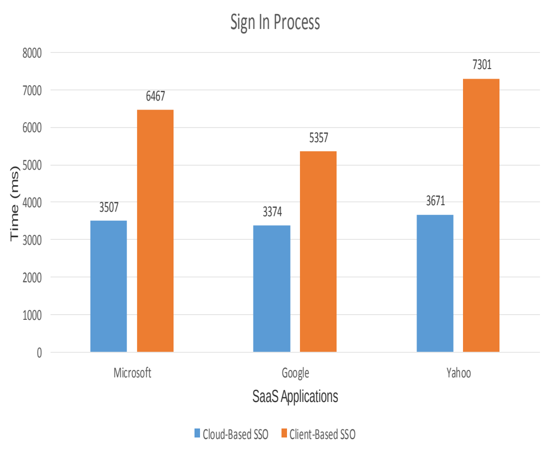

Figure. 3: Sign In Process in Various SaaS Applications

6.1 Security Evaluation of the Proposed Algorithm

The theoretical security analysis of the proposed method shows that the algorithm is enough reliable for establishing secure connections between SaaS application service providers and users. The most important advantage of this model is using a cloud-based SaaS application with two separate cloud servers. This separation and encrypting usernames and passwords with AES-256 cryptography algorithm increase the reliability and security of the proposed model for storing details of various user accounts in a cloud server without and concerns. Furthermore, using SSL between PMA and SSOSA establish security during data transmission processes. In addition, using browser extensions as PMA is led to an efficient dependency between PMA and web browsers and lets PMA to use strengths of web browsers in different ways especially in security parts. In overall, the proposed method provides a reliable cloud-based environment for storing important personal details without security concerns.

7. CONCLUSION

The proposed model is a cloud-based single-sign-on algorithm as an effective solution to increase the efficiency in cloud-based applications according to the limitations [15] and weaknesses of similar client-based models. The proposed model was designed and described by establishing two cloud servers for storing encrypted account details and cryptography keys. Moreover, a cloud-based SaaS application was designed to connect clients and SaaS service providers. Using AES-256 and SSL in the suggested model improves the security of cloud-based SSO algorithm. In conclusion, the reliability of the proposed model has been assured for storing user's important data according to specifications of the model.

The future work will involve the development of a prototype of the proposed system for cloud computing and testing it for diverse real-world scenarios. The goal is to prove effectiveness of the proposed privacy and identity management system, as well as its potential to become a standard for privacy and identity management in the Cloud Computing.

REFERENCES

[1] Alizadeh, M., Hassan, W.H., Zamani, M., Karamizadeh, S., and Ghazizadeh, E. (2013) "Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID", Journal of Next Generation Information Technology, Vol. 4.

[2] Ghazizadeh, E., Zamani, M., Ab Manan, J., and Alizadeh, M. (2014) "Trusted Computing Strengthens Cloud Authentication," The Scientific World Journal, Vol. 2014.

[3] Khalil, I.M., Khreishah, A., and Azeem, M. (2014) "Cloud computing security: a survey," Computers, vol. 3, pp. 1-35.

[4] Mackay, M., Baker, T., and Al-Yasiri, A. (2012) "Security-oriented cloud computing platform for critical infrastructures", Computer Law & Security Review, Vol. 28, pp. 679-686.

[5] Yin, S., Wang, G., and Yang, X. (2014), "Robust PLS approach for KPI-related prediction and diagnosis against outliers and

missing data", International Journal of Systems Science, pp. 1-8.

[6] Yin, S., Wang, G., and Karimi, H.R. (2014), "Data-driven design of robust fault detection system for wind turbines," Mechatronics, Vol. 24, pp. 298-306.

[7] Khalil, I., Khreishah, A., and Azeem, M. (2014), "Consolidated Identity Management System for secure mobile cloud computing", Computer Networks, Vol. 65, pp. 99-110.

[8] Uruena, M., Munoz, M., and Larrabeiti, D. (2014), "Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites", Multimedia Tools and Applications, Vol. 68, pp. 159-176.

[9] Zhang, Y., Hong, J.I., and Cranor, L.F. (2007), "Cantina: a content-based approach to detecting phishing web sites," Proceedings of the 16th international conference on World Wide Web, pp. 639-648.

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

[11] Xiuyi, W., Lingyan, W., Jihong, H., and Qingrong, C. (2007), “Security Research on a SAML-Based Single Sign-on Implement Mode," Microcomputer Information Journal,, Vol. 24, pp. 81-83.

[12] N. Fengming, X. Feng, and Q. Rongzhi,(2013) “SAML-Based Single Sign-On for Legacy System,” in Proc. IEEE International Conf. on Automation and Logistics (ICAL), Zhengzhou, pp. 470-473.

[13] F. Q. Zhang, and D. Y. Han, (2012), “Applying Agents to the Data Security in Cloud Computing,” in Proc International Conf. on Computer Science and Information Processing (CSIP), Shaanxi, China, pp. 1126-1128.

[14] A. Freier, P. Karlton, and P. Kocher, (2011), “The Secure Sockets Layer (SSL) Protocol Version 3.0,” Internet Engineering Task Force (IETF), RFC 6101, pp. 12-16.