International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 3 March 2015

A Survey: Single Sign On (SSO)

Garima Kumrawat[1], Prof. Amit Agrawal[2]
Dept. Of Computer Science and Engineering
Medi-Caps Institute Of Science and Technology, Indore, (M.P.)[1,2]
kumrawat.garima@gmail.com[1], amit@medicaps.ac.in[2]

Abstract: *At present, to access to email account or bank account, a network user has to remember the registered account number of the user and the corresponding password for every service with which they are registered. However, when multiple systems are involved, the user is then required to authenticate to each system individually and repeatedly. It results in inconvenience to each authentication. Recently, to overcome the problem, a single-sign-on (SSO) scheme was proposed to achieve user identification and authentication to multiple security-protected systems simultaneously through a single operation. We surveyed various papers to know the basic concept of SSO. In this paper we have to use cloud model, its key challenges and short intro of SSO.*

Keywords: *Cloud Computing; Single Sign- on; Key Challenges; Security and Privacy.*

1. Introduction

Cloud computing is an on demand service in which shared resources, information, software and other devices are provided according to the clients requirement at specific time. It's a term which is generally used in case of Internet. The whole Internet can be viewed as a cloud. Capital and operational costs can be cut using cloud computing [1].

The word "**cloud computing**" originated from the cloud symbol that is usually used to symbolize the internet on flow charts and diagrams. The cloud computing user doesn't need to deal with the physical hardware aspects of a computer or software maintenance tasks of having a physical computer in their home or office. Instead they use a share of an enormous network of computers, benefiting from economies of scale. The benefits of cloud computing includes the following in Figure 1:

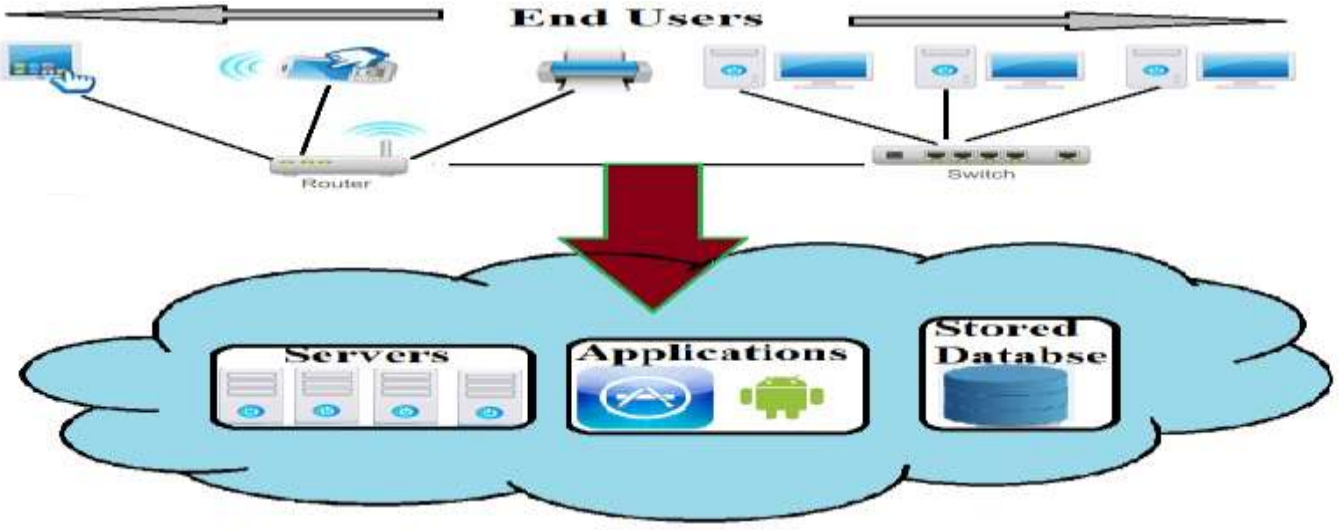

Figure 1: Cloud Computing Model

- Cloud computing minimize infrastructure costs.
- Save energy.
- Cloud computing reduce the necessity and frequency of upgrades.
- Lessen maintenance costs.
- Meet the overload temporal requirements.

Once an Internet Protocol connection is established among several computers, it is possible to share services within any one of the following layers.

End Users: Client consists of hardware and software that relies on cloud computing for application delivery, like tablets, some computers, smart phones, terminal devices, operating systems and browsers.

Application: Cloud computing application services or SaaS (software as a service) deliver application as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.

Server: The server's layer consists of computer hardware and software products that are specifically designed for the delivery of cloud computing services, including multi-core processors, cloud-specific operating systems and combined offerings.

A. Cloud Computing Challenges

Cloud computing [1, 2], an emergence technology, has placed many challenges in different aspects. Some of these are shown in the following diagram in Figure 2.

Security: Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications [2].

Interoperability: Application on one platform should be able to incorporate services from other platform. It is made possible via web services. But writing such web services is very complex.

Portability: This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There should not be vendor lock-in. However, it is not yet made possible because each of the cloud provider uses different standard languages for their platforms.

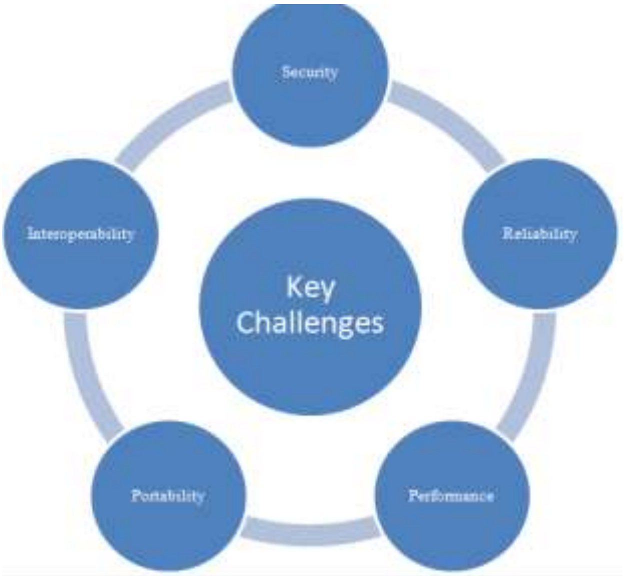

Figure 2: Cloud Computing Key Challenges

Performance: To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost. If done at low bandwidth, then it does not meet the required computing performance of cloud application [2].

Reliability: It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

B. Single Sign On

Single Sign On (SSO) is the ability for a user to enter the same id and password to logon to multiple applications within an enterprise. As passwords are the least secure authentication mechanism, single sign on has now become known as reduced sign on (RSO) since more than one type of authentication mechanism is used according to enterprise risk models.

For example, in an enterprise using SSO [9, 10] software, the user logs on with their id and password. This gains them access to low risk information and multiple applications such as the enterprise portal. However, when the user tries to access higher risk applications and information, like a payroll system, the single sign on software requires them to use a stronger form of authentication. This may include digital certificates, security tokens, smart cards, biometrics or combinations thereof.

2. Literature Review

Courtney Powell [3] we implemented a prototype of the proposed system and confirmed its efficacy. In the experiment conducted, we verified that SSO was operational between two locations, Kitami Institute of Technology and Hokkaido University. In addition, by using this authentication infrastructure and the adopted GSI technique, we plan to construct an SSO system for other computational resources. Quantitative measurements such as authentication delay and security threats are among other related aspects that will also be considered.

Faraz Fatemi Moghaddam [4] 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 users important data according to specifications of the model.

Yang Jian [5] The increased two data flows that are from AS (authentication server) to TGS (ticket-granting Server) and from TGS to app servers V (Ticket), which are used to transmit the ticket-granting ticket and the service-granting ticket, they are greatly reduced the client's security risks and it's workload, and enhanced the client's work efficiency through regulating the topological structure of the system and adjustment of the information flows. The new added authentication client database can dynamically register authenticated client information, and new added authorization client database can dynamically register authorized client information.

Jian Hu [6] Through the single sign-on project construction, a unified database of persons was established. We integrated the isolated system that is not only convenient for the customer but also convenient the manager. In the construction of the Digital Campus Enterprise Service Bus was also used to achieve synchronization of information between databases.

Sahana K. Bhosale [7] In this paper, we discussed the functional and technical requirements of an SSO application that would run on top of the existing bank application. Electronic Commerce can dramatically alter the structure of the banking industry if the primary concern of secured transactions and authentication is addressed through additional research for devising effective data and information security techniques.

Jianhong Zhang [8] Single-sign-on is a new technique thereby increases the usability of the network as a whole and at the same time centralizes the management of relevant system parameters. Unfortunately, we show that Ren's scheme is suffering unforgeable attack we proposed in this paper. Namely, any one without a legal ID can pass the verification. Finally, we give the corresponding revise. Ren's scheme was very efficient Single-sign-on formula for authentication in computer networks. Thus, it is an open problem to improve Ren's scheme and make it secure in the standard model.

David J. Boyd [9] The proposed method could improve the protection for the card, the cardholder and the service provider(s). No form of authentication is perfect because that authentication is only true at that point in time and its strength is also dependent on other external factors. Whether the authentication is sufficient for the business need; the user's privacy is enhanced, the user controls any release of personal information.

Spoorthi V.[10] The Solution explained in this paper can provide strong client side authentication in Single Sign-On domains. It has been proposed to be a Native app-friendly standard as it does not require a browser to authenticate. Also, multiple numbers of native apps can actually be managed using a single Mobile SSO Agent at the mobile device. It is a user friendly authentication mechanism as it does not involve multi-factor authentication or one time password, which decreases user acceptance of cloud. The access can be revoked to a particular user at any time just by revoking the corresponding certificate. The proposed system can also improve bandwidth efficiency of the communication protocol, as only the certificate address is sent over network.

3. Conclusion

In this paper, we discussed the functional and technical requirements of an SSO application that would run on Cloud based application. We have to survey on SSO with electronic device, web based, offline, cloud based etc. SSO work on Authentication and there is a two way to provide the authentication in single Sign on First is using one variable and second is using two variables. In this literature review most of the paper used one variable authentication. In the above review we have discussed various approaches based on SSO.

Reference

[1] Abhilasha Bhargav-Spantzel and Steve W. Deutsch,” Platform Capability Based Identity Management forScalable and Secure Cloud Service Access”, GC'12 Workshop: First International workshop on Management and Security technologies for Cloud Computing 2012.

[2] Ashish G. Revar, Madhuri D. Bhavsar,” Securing User Authentication using Single SignOn in Cloud Computing”, INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 08-10 DECEMBER, 2011.

[3] Courtney Powell, Takashi Aizawa, Masaharu Munetomo,” Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments”, 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet).

[4] Faraz Fatemi Moghaddam, Omidreza Karimi and Mostafa Hajivali,” Applying a Single Sign-On Algorithm Based on Cloud Computing Concepts for SaaS Applications”, 2013 IEEE 11th Malaysia International Conference on Communications, 26th - 28th November 2013, Kuala Lumpur, Malaysia.

[5] Yang Jian,” An Improved Scheme of Single Sign-on Protocol”, 2009 Fifth International Conference on Information Assurance and Security.

[6] Jian Hu, Qizhi Sun, Hongping Chen,” APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS”. 978-1-4244-6769-3/10/$26.00 ©2010 IEEE.

[7] Sahana K. Bhosale,"Architecture of a Single Sign on (SSO) for Internet Banking", IET International Conference on Wireless, Mobile and Multimedia Networks, 2008.

[8] Jianhong Zhang and Xue Liu,"On the Security of An Identity-based Single-sign-on Scheme",978-1-4244-5540-9/10/$26.00 ©2010 IEEE.

[9] David J. Boyd,"Single Sign-On to the Web with an EMV Card",978-1-4244-2249-4/08/$25.00 ©2008 IEEE.

[10] Spoorthi V and K. Chandra Sekaran, " Mobile Single Sign-On Solution for Enterprise Cloud Applications", 978-1-4799-3486-7/14/$31.00 c2014 IEEE.