Communications and Network, 2014, 6, 186-190
Published Online August 2014 in SciRes. http://www.scirp.org/journal/cn
http://dx.doi.org/10.4236/cn.2014.63020

Scientific Research

Implications of SSO Solutions on Cloud Applications

Mohamed Watfa*, Shakir Khan, Ali Radmehr

Faculty of Engineering and Information Sciences, University of Wollongong, Dubai, UAE
Email: *MohamedWatfa@uowdubai.ac.ae, ShakirKhan@uowdubai.ac.ae, ARadmehr@uowdubai.ac.ae

Received 18 June 2014; revised 18 July 2014; accepted 30 July 2014

Abstract

The trend in businesses is moving towards a single browser tool on portable devices to access cloud applications which would increase portability but at the same time would introduce security vulnerabilities. This resulted in the need for several layers of password authentications for cloud applications access. Single Sign-On (SSO) is a tool of access control of multiple software systems. This research explores the effects and implications of SSO solutions on cloud applications. We utilize a new framework of different attributes developed by acquiring IT experts' opinions through extensive interviews to expand significant strategic parameters at the workplace. The framework was further tested using data collected from a sample of 400+ users in the UAE.

Keywords

Single Sign-On, Cloud Computing, Security, Value Added Services

1. Introduction

Cloud computing is a fast growing branch of information technology which is highly on demand. It is an opportunity to enhance capacity and capabilities based on hardware resources at distant locations with broader network access and reliable sources of data storage. It provides secure and quick access for applications to the cloud users on the multi-platform architectures in order to ease the use of dynamic request over the internet. Nowadays, various industries are exploiting cloud computing to facilitate business needs. The trend is moving towards a single browser tool on portable devices to access cloud applications and perform most of the business functions with the help of smart devices over the cloud through the internet. Security has been a major concern for cloud computing due to unavailability of an IT Infrastructure, lack of application manageability and control, and multiple accesses to the platform. The traditional client and server authentication process was adopted by

*Corresponding author.

How to cite this paper: Watfa, M., Khan, S. and Radmehr, A. (2014) Implications of SSO Solutions on Cloud Applications. *Communications and Network*, **6**, 186-190. http://dx.doi.org/10.4236/cn.2014.63020

different application vendors such as Microsoft, Oracle and Citrix. They increased the complexity to remember multiple user credentials for various applications which resulted in the need for having Single Sign-On authentication (SSO). Once client-server applications are transformed into web based applications, SSO was the only solution that can facilitate the broader access for these cloud applications. This research study is important due to the high usage of Single Sign-On features in cloud applications where the IT strategy demands the integration of this technique into business and organizational related applications.

2. Related Work

In recent years, it is becoming very common to use your single social login credential for logging into different websites. Although this is still increasing rapidly but privacy concerns and implications should also be considered as well. One of most successful single sign-on is OpenID [1] which provides a framework for deploying flexible centralized user authentication for web applications. In OpenID, user provides a variety of identity which may be any website or web-based application where user already has an user account (e.g. Google). Research studies on SSO suggest that while it greatly improves user experience by relieving them of the burden of remembering multiple user ids and passwords, it also noticeably reduces help desk calls, and improves security. However, it also cautions that an SSO product is not a cure-all. Without very careful planning, implementation and verification, SSO products can introduce new security holes [2]. There are several works discussing the implications of SSO on several factors. In [3] [4], four different methods were discussed in order to sort out issues associated with SSO and service continuity maintenance. Facebook was used as an example case to discuss all the undertaken privacy issues arising whenever you use your Facebook account to access many other websites. Several disadvantages including loss of anonymity, revealing of user's social cycle, loss of track, propagation of advertisements, disclosure of user's credentials and reverse Single Sign-On semantics were highlighted. Technically SSO appears like a simple solution; however, its implementation reveals hidden complexities. For example, a study by Josang *et al*. [5], analyzed some of the trust requirements resulting from various identity management models. The authors found that trust requirements for a particular authentication technology are directly correlated to the user's perceived risk exposure and that this trust is necessary for user acceptance of the technology. With respect to SSO technologies, it suggests that trust relationships between federated parties are harder to establish particularly if one party has a significantly higher risk exposure than the other.

Meniya *et al*. [6] bridged the gap between different cloud applications by introducing the federation of open cloud and invited different cloud service providers to be part of this body where only identical SSO is accepted across all cloud services providers and facilitated through interoperability. Zhu *et al*. [7] described the problems faced by web applications when different web services were offered to a viewer like: news management system, video on demand system, bulletin board system and the laboratory management system. As each system user has its own authentication system and verifying processing logic, this results in data inconsistency.

3. Research Objectives & Proposed Framework

In this paper, we focus on the effects and implications of Single Sign-On authentication in cloud applications from different viewpoints. We study the nature of current web applications and the benefits that can be utilized through single sign authentication. This research starts with the analysis of currently implemented single sign features across several companies. On the basis of this judgment, we would be able to evaluate whether companies can apply Single Sign-On as an effective solution to improve accessibility to their cloud applications and to increase productivity in the organizational processes. Our study is non-contrived and our primary source of data includes the people working in the IT industry in the UAE. We used a marketing database to find the IT companies utilizing Single Sign-On solutions. We conducted interviews with ten IT specialists in four UAE IT organizations. Our analysis is based on user preferences, productivity, efficiency, accessibility and some other key attributes related to our proposed framework as depicted in **Figure 1**.

Our proposed framework consists of three strategic dimensions summarized as follows.

3.1. IT Strategy—Data Protection

1) Security:

- Passive mode of authentication: It is difficult to impersonate the actual user credentials because the system is designed in such a way that accepts the response from the SSO assistant.

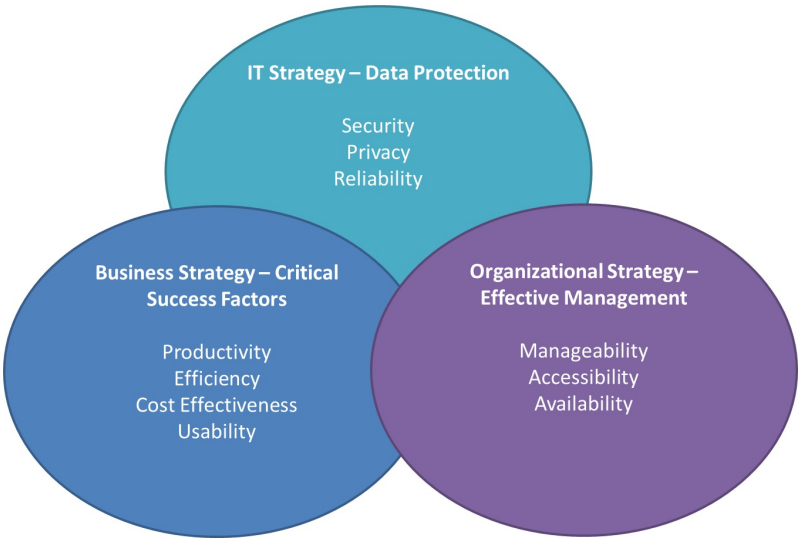

Figure 1. Proposed framework reflecting three different strategic dimensions.

- Dual factor authentication: Authentication through both the user and the SSO assistant where each session has a unique identity.
- Secure: Authenticated Single Sign-On access to the applications they need when they are outside the corporate firewall.

2) Privacy: To increase privacy control and access resources with privacy protection.

3) Reliability: Preferably zero down time including effective control of stolen Single Sign-On credentials.

3.2. Business Strategy—Critical Success Factor

1) Productivity: Continuous flow of tasks with increased number of assignments performed.

2) Efficiency: Time savings and more accurate results in a committed time frame.

3) Cost Effectiveness: Centralized authentication server for Single Sign-On has evident advantages over distributed authentication servers including user productivity enhancement resulting in higher revenues.

4) Usability: Back end plug-ins eases the access to web apps with greater user convenience.

3.3. Organizational Strategy—Effective Management

1) Manageability: Centralized management of user credentials with one time session identity utilized and two ways of credentials handling, one handled by the plug-in and the other by the user through the system.

2) Accessibility: Easily accessible from any web browser.

3) Availability: Unified authorization provides access to multiple web-apps with maintained service continuity in case of authentication server failure.

4. Data Collection and Analysis

In this section, we will introduce our descriptive and inferential analysis. Our sample included interviews of ten IT managers and a survey of 400 IT professionals utilizing SSO.

As summarized in **Figure 2**, the majority of our samples were extremely satisfied with the security of SSO. Also, it is evident that the majority witnessed no or rare effect on the interruption of the services through SSO whereas only about 10% believed in high frequency of failures. Also, about 70% of our sample believed in higher service availability after transitioning into SSO solution whereas the rest didn't notice any or noticed minimal impact on service availability. We also investigated the following hypotheses and performed inferential hypothesis testing using SPSS:

H1: There is an association between SSO mechanism or traditional mode of authentication and service availability.

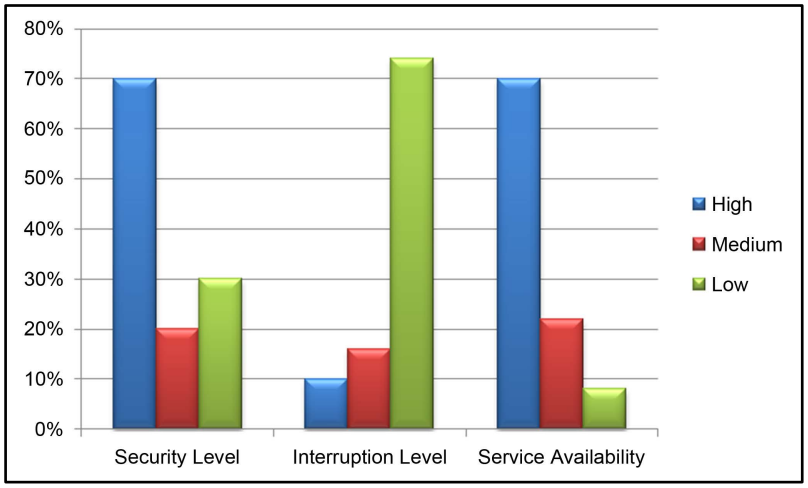

Figure 2. Results from the sample regarding security, interruption and service availability satisfaction levels of Single Sign-On solutions on cloud applications.

Result: Reject the null hypothesis and conclude that there is sufficient evidence to say that service availability is associated with SSO usage.

H2: Single Sign-On solution will be widely acceptable once all the cloud service providers come under the single federation of cloud computing.

Result: Reject the null hypothesis and conclude that there is sufficient evidence to say that the single federation of cloud computing will affect the acceptance of SSO solutions.

5. Conclusions and Recommendations

This study highlighted the effects and implications of Single Sign-On solutions in cloud applications using our proposed framework. More specifically, the following major points were concluded from the detailed interviews and surveys of our sample of 400+ IT professionals utilizing SSO authentication solutions.

5.1. Business Strategy—Critical Success Factors

The following major points were concluded regarding utilizing Single Sign-On solutions where the demand is high for productivity to speed up organizational processes.

- Reduced time to access and log on to IT systems.
- Reduced helpdesk contacts for password resets.
- Reduction in out of hours password “lock outs”.
- Reduced time to switch between applications affecting positively on productivity.
- Support “terms and conditions” for access to critical business systems.

More specifically employees having more interactions with customers gain more benefits from Single Sign-On solutions to increase productivity. Moreover, Single Sign-On solutions reduce the pain for users to access their applications and data from different locations leading to higher performance and better usage. Also, the respondents agreed that SSO can lead to the following competitive advantages:

- Easing the process of job and duty transfer among the employees.
- Maintaining confidentiality of data on staff exit.
- Making the business environment more secure, manageable and credible.
- Leveraging the company productivity by minimizing the need of multiple accounts.
- Making new employee setup faster.
- Making remote assistance more effective and efficient.

5.2. IT Strategy—Data Protection

The below experiences were concluded from our selected sample in measuring the privacy control of the users

when accessing cloud services through SSO:

- The common feedback that users are always concerned about is privacy.
- Credentials are stored and encrypted within the central authentication server with no data leakage.
- Unified access for all.
- User details are controlled in one location.
- SSO by itself cannot guarantee the integrity of the data.
- SSO can remove the need to re-authenticate, by logging in user tickets.

The following recommendations were essential to build strong control over privacy with the SSO mechanism:

- Eliminate password sharing for individual applications by using SSO.
- Develop a strong SSO usage policy and then stick to that policy.
- Each user must have their allocated storage with encryption.
- Cloud providers need to implement multiple factor authentications to use all services seamlessly.

5.3. Organizational Strategy—Effective Management

The implementation of SSO for cloud applications can make manageability of access control more effective as follows:

- Less administrative overhead and configurations.
- Easy deployment of applications through SSO.
- User login can be monitored in real time.
- Once SSO is in place, organizations will have the King Key access.
- Easy implementation of governance policies including centralized audit and reporting.
- Increased efficiency and reduced efforts with more discipline in the attitude of the IT staff.
- Less chances and burdens for users to forget their passwords.

To conclude, with the increasing number of cloud applications in the business environment, the need to have a Single Sign-On to access all of those applications at once in order to accomplish different tasks in a shorter period of time will be growing. To make SSO as a portable and widely applicable solution for most of the cloud applications, it is suggested to reduce compatibility issues between different cloud vendors in order to build a uniform structure which is feasible to the needs of the organizations. Through SSO, an organization can obtain improved access with less complexity and increased productivity with better safeguard against any malicious activity. As technological advancements in central hardware authentication systems continue to grow with the flow of approvals in the organizational hierarchy, SSO solutions will be an added value for a faster and safer access.

References

[1] OpenID. www.openid.net

[2] Anchan, D. and Pegah, M. (2003) Regaining Single Sign-On Taming the Beast. *Proceedings of the* 31*st Annual ACM SIGUCCS Conference on User Services*, 166-171. http://dx.doi.org/10.1145/947469.947514

[3] Kakizaki, Y., Maeda, K. and Iwamura, K. (2011) Identity Continuance in Single Sign-On with Authentication Server Failure. *Proceedings of the* 5*th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (*IMIS*-2011), Seoul, 30 June-2 July 2011, 597-602.

[4] Kontaxis, G., Polychronakis, M. and Markatos, P. (2012) Minimizing Information Disclosure to Third Parties in Social Login Platforms. *International Journal of Information Security*, **11**, 321-332. http://dx.doi.org/10.1007/s10207-012-0173-6

[5] Jøsang, A., Fabre, J., *et al.* (2005) Trust Requirements in Identity Management. *Australasian Information Security Workshop*, Newcastle, 99-108.

[6] Meniya, A. and Jethva, H. (2012) Single-Sign-On (SSO) across Open Cloud Computing Federation. *International Journal of Engineering Research and Applications*, **2**, 891-895.

[7] Zhu, F. and Diao, H. (2010) Single Sign-On Assistant: An Authentication Broker for Web Applications. 3*rd International Conference on Knowledge Discovery and Data Mining*, 2010, 146-149.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.