REVIEW OF SINGLE SIGN-ON AUTHENTICATION FRAMEWORK

AISHWARYA U¹ & DR. CHETHANA R MURTHY²

¹Student, R V College of Engineering, Bangalore

²Assistant Professor, R V College of Engineering, Bangalore

ABSTRACT

Single sign-on abbreviated as SSO is a framework which uses one verification operation to enable an approved person to connect all connected but independent software applications without having to log in once again for each during a given session. It is difficult to a human being to remember authentication credentials for all the applications that he uses. It may also create confusions in logging in various applications. As a solution to this the person may save his passwords in mobile or he may write it in a book. But this is the wrong way as if another person can misuse these details. In order to provide a permanent solution, this single sign on system came into picture. Using this system, the person does not have to memorize all the passwords and can be able to login different related accounts easily using simple and single log in credentials. The person has to just authenticate once to use multiple accounts. The important point to remember here is, the person also needs to logout once he finishes using. SSO system deals with ease of use, reliability and confidentiality. This paper discusses in detail about SSO including what it is, how the system works, the different types of SSO and the technologies used to implement single sign on in various fields.

KEYWORDS: Single Sign On, Authentication, Log In Credentials, Software Applications, Confidentiality

Received: Jun 01, 2020; **Accepted:** Jun 20, 2020; **Published:** Jul 22, 2020 **Paper Id.:** IJMPERDJUN2020417

INTRODUCTION

Single Sign-on (SSO) is a technique that enables user to login mobile or web application using common username and password to open different programs using the same provider for authentication. SSO is used to authenticate and permit. Authentication represents the act of confirming who you really are. Typically, it is not realistic to ask one person for this to keep separate identity pairs and credentials for various service providers as this may maximize the volume of work from both service providers and users, and overhead communication technologies. Online application systems are now widespread in use. Companies, Faculties, educational institutions and associations have their own normally used equipment's. In general, such systems require authentication while service is being offered. Consequently, the consumers must note each system's accounts and passwords note. That is really uncomfortable. Single Sign-on (SSO) is a network access feature for the different, related, but standalone software systems. Using this property, a person is signed in once and is able open to all systems without signing in again at each time. Supporting different technologies and tools various authentication methods, SSO has to convert distinct credentials into and store them internally evaluated with what is used in initial authentication. The below figure 1 shows the overview of single sign on process. The user who wants to use the SSO system has to register as an initial step. Then he needs to authenticate a web application and set a master password which he wants to use for the all the applications. Using this single password, he is able to sign in for all the related and independent web sites.

Figure 1: Overview of Single Sign On.

Protection can be enhanced since authentication is required at just one authorization authority that should be particularly guarded. In more, users will remember only one solid password, rather than several passwords for every single service provider. In addition, time and costs could be rescued as consumers need to just operate in one of the authentications only. In the end, the main benefit of SSO is an improvement in user satisfaction because of a variety of burdensome authorization procedures may be removed though still in gaining access to a series of diverse secured infrastructures at the same time. A very broad range of applications brings a large number of pairs for usernames and passwords to remember. In certain instances, credentials are issued at the start of an application as a hidden term, and because humans are inclined to forget items, such credentials are recorded on notification labels or other unsafe resources that can be viewed by someone. Therefore, this user interface needs to be removed that the user must enter the login details with each and every facility he needs to use. The SSO principle eliminates this feature and offers a simpler way of providing the access control without having to use separate sign-in processes to access various services.

LITERATURE SURVEY

Iadalin Nongbri et. al., [1] discussed the description of single sign on including how it works and diverse procedures used for it. The user will register with the IDP to obtain OpenID credential. The user wishes to use Application X. Application X forward the User to the IDP. Using his OpenID passwords, the user logs in to the IDP. On Effective IDP authorization the user is redirected to Application X again. When the user needs the Y Web Application, the request is sent to Web application Y. Upon reception of the request, it will go to the Identity Provider and ensure if the user who requested is active or inactive. If the user is active, application B is made accessible to user. This process is followed for other applications also. Application X will not know what is happening in application Y, and similarly Y will not get to know about X.

SSO is the process for log in to application only once and sign it to other related applications mechanically. Protection is the significant concern in all the technologies. There will be many types of attacks such as session attack, man in the middle attack and phishing which will misuse the consumer's information. But still some of the papers will provide the precautionary techniques for this.

RinkyChhatwani et. al., [2] given a far-reaching audit of current work performed on Single sign-on. At that point for protection of single sign-on, constraints and assaults ought to be secured. Development of Single Sign-on for circulated registering utilizing client id and secret word alongside biometric confirmation. At that point security examination is finished. Authors presented the correlation and finally concluded, determining the future work. Many of the Single sign-on plans experience the ill effects of different security concerns and are powerless against various assaults. Authors have actualized User-id and secret key alongside biometric based SSO validation plot. They have applied One-way hash capacity and AES encoding and decoding calculation for the record activity for the application. They have introduced Security investigation of how the assaults are anticipated and parameters are enclosed.

Radha et. al., [3] investigates different strategies for SSO and the benefits of it. It additionally talks about on executing different kinds of SSO and the conventions that are being utilized. Single sign on without a doubt makes it simpler and more secure by decreasing to just one account for every client for all administrations, number of passwords, focal administration of jobs to characterize assets get to control. It can be exceptionally advantageous to end-clients, overseers and help work area. Single sign-on can increase considerably more significance with the developing Cloud computing innovation giving administrations and furthermore it diminishes the odds of phishing assaults yet as single sign on provides access with single login, it ought to be executed in a protected manner. Single sign on has its qualities and shortcomings and one should cautiously gauge the utilization of the framework and the assets accessible for its organization and the executives previously picking SSO arrangement or, in all likelihood it can make a big weakness in an associations security if it is certainly not actualized appropriately.

TayibiaBazaz et. al., [4] presents survey on SSO empowering innovations and examines SSO models, conventions and examination identified with developing utilization of SSO. A large portion of the clients want to utilize SSO system since it is advantageous for them as it permits them to get to scores of individual records just by recollecting a solitary secret word and consequently sparing them from the problem of setting one of a kind arrangement of username and secret phrase to every one of their records. Other than these advantages, SSO have negative effect too yet at the same time the dangers of SSO clients are not exactly those of non-SSO clients as the last will in general keep practically same secret key to get to their all applications and for the most part to store their passwords in hazardous zones.

SSO frameworks can bring together validation on uncommon servers as they are regularly founded on complex frameworks of board applications. In this manner it can make a positive commitment to a data security procedure of a venture. This should be possible by utilizing devoted servers that hold SSO modules. These servers go about as guards, in this way ensuring all the traffic passes through the SSO server first, which at that point goes along the certification it has put away for confirming the specific application enlisted with the SSO framework.

Ashish Revar et. al., [5] developed Cloud for Virtual Machines pictures and storage to perform the SSO on the top layer of Cloud. This has involved a survey and examination of current single sign-on designs and arrangements, the improvement of another design for single sign-on, an investigation of single sign-on dangers inside a Cloud setting, an inference of single sign-on goals in Cloud, paving the way to the security necessities for single sign-on in Cloud. Security and usefulness are the primary driving variables in the structure. The goal of this examination is to estimate the worth, in terms of capability and productivity, of a particular security activity to actualize a Single Sign-On framework. Adequacy is estimated as far as secret word consistence; get to related occurrences, and the time needed to arrangement also, de-arrangement accounts.

Pratap Murukutla et. al., [6] implemented single sign on for cloud clients. The proposed plan permits client to utilize one set of accreditations, even a client keeps up with various types of cloud conditions. Authors proposed an answer with defected tests of open approval where there is a confidence party reviewer which keeps up all the certifications and cloud supplier can extra ordinarily recognize one client from other. They additionally keep up secure direct for client so as to guarantee the privacy. Typically, the client communicates the application in the cloud of Service supplier A. the adaptability of the evolving specialist organization can be dealt with moving the assets from one supplier to other supplier. The assets can be moved from specialist organization A to B within the sight of the client.

Arvind Meniya et. al., [7] centers around the idea of SSO over all the open cloud to utilize their figuring assets in single or collective way. We additionally investigate the situation of interoperability norms between various clouds. This will quicken purchaser in explicit effective cloud asset sharing component. Here the vision is to make a productive and increasingly explicit open distributed computing alliance that expels the multifaceted nature of cloud client in conventional cloud environment. By executing this kind of alliance, there will be a widespread method to give diverse cloud administrations at one spot and client doesn't have to sign-in for various clouds on account of acquainting the Single-Sign-On with the organization and testing among clouds.

Fei Zhu et. al., [8] set up a confirmation representative for online applications, called Single Sign on Assistant (SSOA). With SSOA, a client does not have to continue verifying when incoming in various online applications. SSOA takes client's post information when he signs in some online application framework for the initial run through, and afterwards builds a prerequisite by which SSOA recreates login technique and guides consequently login, in this manner taking out client's physical personality approval and, in this way, accomplishing single sign on.

ANALYSIS OF SSO TYPES AND TECHNOLOGIES

Various types of SSO authentications, technologies involved in it and the attacks on SSO are explained in this part.

Types of SSO

- **Shared Sign On**

One master password is maintained for logging into all the accounts. It should be constructed of capital and small letters, numbers and can be easily remembered.

- **Trouble-Free Sign On**

It can be developed on homogeneous intranet, where every technology is performing on the single operating system and believing the similar validation authority.

- **Password Manager**

There are several password management's tools which can identify the user when he logs in more than once and makes him to verify the identity by using password management tool.

- **Composite SSO**

It can be executed on either Extranet or Internet. It is developed in diverse platforms and administrated by distinct associations.

- **Central Login**

Central login works as plug-ins that keeps on observing the browsers for credentials and is able to accumulate the information.

- **Social Login**

This is concerned with the social networking sites such as Facebook, twitter etc. And allow the user to use all the related sites with single log in.

Technologies of SSO

- **Token Dependent SSO**

Tokens are created which are encrypted and data with concerned token is only allowed to access.

- **Browser ID**

Browser ID is developed using validated protocol. It always recalls the email id instead of usernames and passwords. And using email is it allows the user to access.

- **OpenID**

Open ID is a decentralized protocol for authentication.

- **Kerberos**

Kerberos is a traditional development of Token-based circulated authentication protocol.

- **XML and SAML**

Extensible markup language (XML) and Security Assertion Markup Language (SAML) both are standards that assists substitution of user verification and approval information across protected areas.

Various Attacks on SSO

- **Impersonation Attack**

This is an attack where an opponent productively assumes the uniqueness of the legal in a framework.

- **Man in the Middle Attack**

Here the attacker tries to eaves drop the information.

- **Privacy Attack**

This attack is performed by stealing the login credentials where the hacker acts as the authorised user.

- **Injection of SQL to Cloud**

This type of attack uses the information of user stored in database.

- **Replay Attack**

In this attack, verified and valid information is transferred in a delayed manner and not in an unauthorised manner.

- **Side channel Attack**

An attacker tries to store spiteful virtual machine in cloud and then using that perform this type of attack.

- **Denial of Service Attack**

Here the attacker sends multiple authorisation requests to the users to log in using malicious addresses that users will not get to know.

- **Authentication Attack**

Authentications are weak and are continuously targeted in this type of attack.

Figure 2: Advantages of SSO.

The above figure 2 depicts the benefits of SSO from in various fields. The below figure 3 shows the top 10 enterprise solutions that provide single sign on framework and the number of users it can support. The pricing per month per user is also shown in the figure 4.

CONCLUSIONS

Single Sign-On can be utilized to settle numerous issues identified with various authentications for various applications. Single Sign-on access to the fundamental validation community empowers clients to gain admittance to every single other asset accessible. SSO serves to improve client and engineer profitability by keeping away from the client to recall different passwords and furthermore decrease the measure of time the client waste on composing different passwords to login. SSO additionally sorts out the organization by overseeing single authentication rather than numerous accreditations. This paper summarises the working of SSO framework and different kinds of SSO. Brief information is also provided about the technologies involved in SSO and attacks on SSO.

Figure 3: SSO Service Providers.

Figure 4: Pricing Per Month.

REFERENCES

1. IadalinNongbri, PynbianglutHadem and Sarat Chettri, "A Survey on Single Sign-On," *International Journal of Creative Research Thoughts*, pp. 595-602, Vol. 6, 2018.
2. Rinky G. Chhatwani and D.G.Harkut, "Implementation of Single Sign-On Mechanism for Distributed Computing" *International Journal of Computer Science and Mobile Computing*, pp.623–632, Vol. 3, June 2014.
3. V. Radha and D. Hitha Reddy, "A Survey on Single Sign-On Techniques," *Procedia Technology*, pp. 134-139, Vol. 4, 2012.
4. TayibiaBazaz and Aqeel Khalique, "A Review on Single Sign on Enabling Technologies and Protocols," *International Journal of Computer Applications*, pp.18-25, Vol. 151, 2016.
5. Ashish G. Revan and Madhuri D. Bhavsar, "Securing User Authentication using Single Sign-On in Cloud Computing," *IEEE Explore*, pp. 1-4, 2011.
6. Pratap Murukutla and K.C. Shet, "Single Sign On For Cloud," *International Conference on Computing Sciences*, pp. 176-179, 2012.

7. Arvind D Meniya and Harikrishna B Jethva, "Single-Sign-On (SSO) across open cloud computing federation," *International Journal of Engineering Research and Applications*, pp. 891-895, Vol. 2, 2012.
8. Fei Zhu and HongjunDiao. "Single Sign-On Assistant: An Authentication Broker for Web Applications" *International Conference on Knowledge Discovery and Data Mining*, pp. 146-149, Vol. 2010.
9. Mohamed, Samer I. "Innovative Software Delivery Framework to Wards Software Applications Modernization." *IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)* 4.5 (2016):77-98.
10. Mahajan, Rini., and Dheerendra Singh. "Step By Step Securing Cloud Environment." *International Journal of General Engineering and Technology (IJGET)* 6.4 (2017):47-54.
11. Gaikwad, Kirankumar, Rupali Nikhare, and Rahul Jiwane. "Enhanced Unified Authentication and Authorization Architecture Based on Desktop Virtualization." *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)* 5.1 (2015):71-78
12. Sriraghavendra, M., and Prateek Jain. "Virtual Machine Vs Container: An Application Performance Review." *International Journal of General Engineering and Technology (IJGET)* 6.4 (2017):29-40.