Challenges in Single Sign-On

Prashant Pandey and T N Nisha*
Symbiosis Centre for Information Technology,
Symbiosis International (Deemed University), Pune, Maharashtra, India
Email: nisha@scit.edu*

Abstract. Single sign-on uses a centralized session concept, and it is a service that authenticates one and one-on-one designated platform. Later, with this, we can use various services and products without logging in every time. However, there are sure demanding situations in implementing SSO. Business enterprise no longer is most effective and needs to integrate user network logon with a nearby application and software program (SaaS) cloud offering. Simultaneously, in an enterprise, SSO’s centralized solution does not include all the users, applications, devices, and equipment. Another undertaking from the records angle is that the user can log on outside SSO answers. Its user identification may also exist in exceptional forms. Simultaneously, the enterprise desires to cope with bequest desktop programs that do not coordinate with users’ listing logins which may be the frail hyperlink that reasons SSO to fail in the company. With the efficiently applied SSO and designing framework keeping in mind the challenges, we can enable and disable users to enter more than one system, platform, apps, and different resources. Also, it may effectively resolve and dispose of the problem of password-related downtime and reset expenses. Simultaneously, it removes the danger of threat from an insider, improves authentication processes and user experience, delivers authority to the company, and simultaneously provides them with the right of entry to firmly on top of the user’s things.

Keywords: Single Sign On (SSO), Multi-Factor Authentication (MFA), Information Technology (IT)

1. Introduction
Single sign-on (SSO) works on a centralized service concept. The user could be authenticated using one set of login credentials. With the help of cookies generated and session control, the same may be used to get the right of entry to more than one application. An example of social sign-in may be seen via Facebook or Google as reliable SSO platforms, with every platform empowering in getting access to several third-party services.

There was a preference for SSO, which changed into the upward push of password-related fatigue. The developer adopts new methodologies, mobility in company, public cloud, and cloud-related
programs and applications, specifically cloud application-specific, each a threat a hindrance. In line with the latest research, businesses are anticipated to consume and utilize an average of at least 17 cloud applications to improve their IT-related operations and strategies regarding the enterprise due to which agency at the identical time individuals sense that Identity Management (IM) and Identity Access Management (IAM) is much more complex today than it was some time ago.

The scalability provided by SSO is one of the greatest benefits of Single Sign-On. Since there is a mechanism of automatically controlling the credentials of the user, the system admin is not any further formally required manually in order to make arrangements and take regarding access-related roles and responsibility of the user as a result of this, successively it reduces the error which can be because of human issue and in turn give sufficient and free up much IT time with a goal other important tasks can be focused. Another blessing encompasses quicker provisioning for cloud-related first applications; if a Single Sign-On solution supports the growth of open standards, like Security Assertion Markup Language, the applying may be quickly monitored via SSO admin. The same can be extended to employees. At the same time, Single Sign-On also increments security, particularly when combined with two-factor authentications, increasing productivity gains and reducing the number of IT help desk password resets.

SSO, will not be able to achieve its purpose if certain challenges they cannot meet, like integrating network logging credentials of a user with a local application, but at the same time whether it can integrate with a mobile application and all SaaS application. The requirement to integrate with these additional services has driven the need for alternatives.

The latest identity services are known as identity as a service (IDaaS), bridge the gap between traditional enterprise SSO and cloud offerings. Vendors include OneLogin, Okta, and Microsoft's Azure Active Directory, which use identity services such as Security Assertion Markup Language (It is used for identity management), WS-Federation, and OpenID (one of the foremost important Single Sign-On protocols used for delegated authentication. It is utilized by companies like Amazon, Google, Microsoft, and PayPal). Accounts can be imported from the Active directory. The products can be configured to allow seamless access to thousands of supported SaaS products.

Another upcoming challenge is uncontrolled and unsanctioned use of SaaS is a major concern for information security departments. By integrating these services with enterprise SSO, organizations can determine what data is leaving the network and apply security policies and controls like MFA (Multi-Factor Authentication).

In SSO, there are sure more challenges, much like SSO's solution is not compatible with all applications, customers, and gadgets which is in use throughout an organization. There are chances that customers can still able to log in and get access to packages through of doors of the SSO solution, which makes the organization mandatory to gather a couple of listing or directory structures. At the identical time, User identities can also exist in numerous ways within distinctive frameworks. Furthermore, the SSO arrangement is incapable of synchronizing these and supply one identity for every commercial enterprise user.

While designing SSO permit answer and if its miles implemented efficaciously maintaining in mind the challenges, it will be extraordinary in terms of productivity related to IT monitoring and management, and control safety. According to roles, access can be allowed or revoked for the user in getting entry to more than one system, platform, apps, and other resources with the help of one security token.

2. Literature Review
Single sign-on is a mechanism that utilizes centralized session for authentication and allows a legal user with one credential to access and at the same time be authenticated by various service providers.
The process allows users to log in only once. After that, automatically, its identities will be checked and verified using each application they want to access. The provider authenticates on the one-on-one designated platform, allowing one to use various services then without logging inside and outside anytime. The purpose of one test is to have a central identity provider which will control identity also as web.

The prototype had been designed and implemented for the device which is being proposed and showed its efficiency. Within the conducted experiment and tested, SSO was operational between Hokkaido University and Kitami Institute of Technology. Additionally, utilizing this centralized authentication infrastructure and the followed GSI technique conceive developing a Single Sign-On system. Quantitative measurements like delay in authentication and protection threats were among the other related aspects considered when establishing the system [1].

The OpenSSO framework gives center personality administrations to disentangle the execution of straightforward single sign-on as a security segment in a system framework. OpenSSO provides the establishment to coordinating various web applications that may ordinarily work against a dissimilar arrangement of character storehouses and are facilitated on an assortment of stages such as web server and application server. This task depends on Sun JavaTM Framework Access Director's codebase, a center personality foundation offered by Sun Microsystems.

The proposed version was defined by designing how to establish two cloud servers to store encrypted account information and cryptography keys. Further, a cloud-based SaaS (software as a Service) application was designed to bring together clients and SaaS service providers. Using SSL and AES256 in the defined model further improved the cloud-based SSO algorithm’s protection [2].

Simultaneously, Java Open Single Sign-On based on the J2EE framework is an open-source SSO framework planned to provide a solution for unified, stage nonpartisan, client validation and approval. The system permits different web servers and web applications, such as the Apache Tomcat, ASP, JBOSS, and to verify clients with accreditation stores. Java Open Single Sign-On imparts with certification stores over the Lightweight Directory Access Protocol. Java Open Single Sign-On uncovered Single register administrations utilizing Cleanser over HTTP convention, permitting it to coordinate with applications that are not java handily. JOSSO actualizes JAAS (Java Validation and Approval Administration) to substantiate and authorize clients’ controls [3].

Similarly, models have been designed and proposed, thru the implementation of the simplest sign-on mechanism for project construction; a unified database of persons was established. The blending of an isolated gadget is easy and useful for the user, and handy for the manager. The Digital Campus Enterprise Service Bus’s development changed into additionally accustomed reaps synchronization of know-how between databases [4].

However, a solution has been given, which explained that it could also provide robust client-side authentication in single sign-on domains. It has been proposed to be an area application having cordial standards because it does not require a program to verify. Moreover, various local applications can be overseen utilizing a solitary Versatile SSO Specialist at the cell phone. It is a client neighborly verification instrument [5]. It does not include multifaceted confirmation or a one-time secret phrase, which diminishes client acknowledgment of cloud. The entrance can be repudiated to a specific client whenever just by denying the comparing declaration. The proposed framework can likewise improve the correspondence convention's transmission capacity effectiveness; just the authentication address is sent over the system [12].

The framework employed for implementing Google application is Security Statement markup language (SAML) Single Sign-On (SSO). By utilizing SAML, an internet specialist co-op can contact a unique online character supplier to verify clients who try to make sure about substance. Google Applications
offers a SAML-put together Single Sign-On with reference to single sign-on administration that provides accomplice organizations full authority over the approval and confirmation of facilitated client accounts, which will get to online applications like Google or Gmail Schedule. Utilizing the SAML model, Google goes about because the specialist organization offers varieties of assistance, such as Gmail and Accomplice Start Pages (PSP)[6].

With the wide spreading of circulated PC systems, different system administrations have picked up significance and prevalence in late hardly any years. Therefore, client confirmation has been generally utilized in appropriated PC systems to recognize a lawful client who requires organizing administrations. Shared validation ought to be thought of to forestall false servers, and a meeting key foundation is ordinarily required [7].

Be that as it may, planning proficient and secure shared verification conventions is trying in PC systems. Additionally, with the expanding utilization of system benefits, a client may need to keep up increasingly more ID/secret key sets for getting to various appropriated specialist organizations, which force weight on clients and specialist co-ops even as the correspondence, overhead of PC systems. The single sign-on component gives a decent solution for this issue. It permits a client with a solitary qualification to get to numerous specialist organizations [8].

Instinctively, there are three fundamental security prerequisites for SSO plans: specific fulfillment, sufficiency, and qualification protection. In any case, supposedly sufficiency has not been officially concentrated and how to save both adequacy and accreditation security is as yet a test [9].

Another challenge that lies ahead is uncontrolled, and unsanctioned SaaS utilization is a significant worry for data security divisions. By incorporating these administrations with big business SSO, associations can figure out what information is leaving the system and apply security strategies and controls like MFA (Multifaceted Confirmation) [10].

In SSO, there are sure more difficulties, similar to the SSO arrangement is not comprehensive everything being equal, applications and gadgets being used over the association. A few clients are ready to sign into applications outside of the SSO arrangement, making the association required to unite numerous catalog structures. Simultaneously, Client personalities may exist in various structures inside various frameworks. The SSO arrangement cannot synchronize these and give a solitary character to every business client [11].

3. Challenges in Single Sign-On

3.1 Major Challenges

Whenever an organization decides to implement SSO, the major challenges they faced are mostly during the implementation phase, which is when it comes to integrating various systems, usually in terms of both architecture and security. Since organization mostly operates with an application with obsolete architecture irrespective of regular updates and modern application or mobile application or any e-commerce sites are built with newer technology and concepts. So, to empower participation between these different advances, a few middlewares are required. The arrangement will be in between all these frameworks and give them fully functional Single Sign-On. The number of integration focuses is colossal, but it could be a significant challenge to guarantee that all these frameworks work together legitimately to supply the client with consistent SSO involvement[13].

At the same time, SSO must be outlined, created, and executed simultaneously in all the important frameworks. On the off chance that we do so, the benefits for both the company and the client will be prompt — the client will be able to log in once and be authorized in any other site or app given by the company, which could be a noteworthy advantage for the client, but a major challenge for the company, which needs to confront the coordination of the method of SSO usage in numerous systems. Not each
group has got to begin the users simultaneously [14]. However, they all need to simultaneously wrap it up to instantly empower the client to take advantage of the arrangement.

However, when it comes to establishing, implementing, and maintaining SSO, the organization usually faces challenges [15].

- **Infrastructure**: During implementation, it takes longer than anticipated to set up SSO. Each environment is distinctive, so included steps in usage can edit up.
- **User and access**: Identity management and Identity access management are much more difficult and complicated since user identity exists in different forms while providing access to different applications incorporating SSO functionality. When SSO is facing some issues, getting access to all associated applications is halted.
- **Security**: Maintaining security in SSO-enabled applications is another challenge on the off chance that a hacker breaches one's identity supplier client account. All of one's connected frameworks can be open to assault.

### 3.2. Major Challenges concerning Development of SSO

In today's digitalization era and the growing use of cloud applications, there is a necessity for a Single Sign-On, which will help the user simultaneously maintain the user's identity and access. However, along with it, there is some hindrance in the growth of SSO like:

While developing, implementing, and maintaining SSO in any organization, some challenges will be faced by an organization, which needs to be taken care of while establishing and effectively implementing SSO. Classification under this management is shown in Table 1. Overall, various challenges concerning the development of SSO can be classified into four categories in Figure 1.

- User Management
- Security Management
- Infrastructure Management
- Access Management

| Table1: Major challenges in the implementation of SSO |
|---|---|---|
| Category | Challenges | Description |
| **Access** | Access Management | Identity access management (IAM), since organizations are moving towards using cloud applications, must have access defined per roles and responsibilities. |
| | Access Management | SSO is not inclusive of all applications and users. |
| **User** | User Management | User identity exists in a different form; therefore, it is important to have a single identity for every business user. |
| | Identity Management | Identity management, as the user increase in an organization, is important for a single authentication mechanism. |
### Infrastructure Management

An organization needs to integrate local application, mobile application, and SaaS cloud offering with the SSO platform.

### Infrastructure Management

It is important to address legacy desktop application since it does integrate with user directory logon, which does not fulfill the purpose of SSO.

### Security Management

SSO needs to combine with 2-factor authentication to improve its productivity gain and maintain the security of information.

### Security Management

Uncontrolled and unsanctioned use of SaaS application, which is major challenges in the implementation of SSO.

### Security Management

Some users could log on outside the organization, which made it mandatory for an organization to come up with multiple directory structures, which need to be integrated with SSO.

---

**Figure 1:** Category of Challenges in Implementation of SSO

- **User Management**
  1) *User Aspect:* The majority of users prefer to use a previous system that is multiple login systems and preferably at the same time want to move from the existing traditional previous system to a new model of
the single authentication mechanism. They mostly tend to utilize a feature of the browser that is a password manager. Another important aspect is that the users and clients frequently falter to supply their individual and personal data to the various websites utilizing single sign-on. Frequently, the applications or websites utilizing a single sign-on service include enquiring the clients to provide them the access to get to know their list of contacts, area, and various delicate and private data that make users rethink before taking a decision agreeing to the agreement. Depending upon the notoriety and the belief relationship between the client and the site, the client either embraces the SSO approach or chooses to go for numerous logon sessions, subsequently maintaining a strategic distance from the circumstances where their data may get compromised by one means or another.

- **Security Management**
  2) **Security Aspect:** Most of the individuals believe that, that by utilizing a single sign-on mechanism, they are giving their credentials straightforwardly in the form of usernames and passwords to the server, and subsequently, their delicate data is put away locally someplace. The clients highlight the encounter of phishing assaults as one of the most primary reasons that ruin the SSO selection as they could not truly discover any recognized or distinguished contrast between the genuine websites and the fake websites.

  Even though the SSO execution diminishes security risks but sometimes dangers can be complex. On occasions, a true blue client might, in some cases, fair walk absent from his framework taking off his/her account logged in. A malevolent client can effortlessly pick up get to it, and consequently, all the authorized assets are compromised. Even though this issue can be experienced with security, by and large, the impacts after implementing with the single sign-on solution are more awful as without implementing SSO, as if it were a single asset, gets comprised since isolated logins are required, and necessary for logging on to other applications.

- **Infrastructure and Access Management**
  3) **Infrastructure aspect (linkage of various accounts):** The clients are not generally recognizable with an account connecting handle, and when inquired by website or application to login by their already existing social organizing accounts, they usually get confounded and baffled and inevitably drop the plan that is the implementation of Single Sign-on authentication mechanism. The arrangement simultaneously is inclined and prone to DOS attack as the mechanism for verification and authentications centralized, basically flooding the target with activity in the form of traffic or sending it data that triggers a crash. Sometimes, SSO usage is troublesome; the time needed will be more costly to adjust into existing applications.

- **Access Management**
  4) **Access Aspect:** While accessing Single Sign-On and Multifactor authentication concerning various applications and users, there are some challenges which organizations will face while implementing SSO and MFA.

  Even though Multi-Factor Authentication reduces security issues on control, but there are still a few security issues, just like the one-time password tokens, it can be compromised or stolen by a Man-in-the-Middle phishing attack, smart cards it can also be hacked or stolen, threat agent can utilize the malware Trojan horses to piggyback the client sessions after they have logged in. Although multi-factor authentication can also be broken, it usually improves the security of systems or the website. However, usually, threat agents keep changing their attacking strategy.

  The actual progress in implementing single sign-on and multi-factor authentication usage depends on client acknowledgment. The clients stand up to carry and have tokens with them or get fingerprinted.
Tokens can effortlessly get lost by clients or stolen by assailants. In this way, client acknowledgment could be a key challenge to single sign-on and multi-factor authentication usage.

According to the organization's estimate and size and the sort of single sign-on and multi-factor authentication innovation utilized, sometimes the framework's cost can be very high. A few frameworks, e.g., client-side software, sometimes may not back MFA devices, and thus, modern. New compatible devices (equipment and program) ought to be obtained, arranged, and at the same time also installed. Subsequently, a legitimately fetched examination can accurately decide the worth of SSO and MFA.

3.3. Risk Factor of SSO concerning various challenges

SSO makes a difference to avoid the circle of verification and loop of authentication, but at the fetched of a few downsides and drawbacks. The clients may be incapable of confirming themselves if the SSO supplier faced some issues and stopped. Subsequently, it brings the entire working of the system to a stop. This particular failure is defined as a single point of failure. Moreover, it is likely and quite conceivable for a single sign-on server to be breached or hacked, leading to information loss. Moreover, a client's confidential and private information may get access or compromised by a threat agent in a single shot since the complete confirmation accreditations and credentials are within the same container. The bushel's key may get uncovered on the off chance that SSO and MFA's coupled utilization is not actualized. Hence, it cannot be considered an add-up to a security tool. Another factor that enhances the risk factor in implementing single sign-on is sharing client information with a third party. The proper identity provider choice is crucial to arrange and cover a wide range of potential clients. Consequently, the dependence on a third party has overwhelming drawbacks. It has to be addressed and planned in that approach to reduce the risk factor included in SSO.

4. Proposed Framework for implementing SSO and eliminating major challenges

In order to implement and fully achieve SSO authentication mechanism solution functionality and objective, an organization needs to address the following pointers are shown in Figure 2.

i) Remote access to the application and Network Access

Several SSO arrangements are accessible, but they either cater to on-premise applications or cloud and SaaS applications. The organization will be centering on a multi-vendor arrangement that caters to conventional and cloud and SaaS applications. However, they often disregard SSO arrangement capability to supply further information, information, and other organized assets. So as an organization, before choosing an SSO arrangement, the organization must make beyond any doubt that it oversees get to all applications counting undertaking apps, web apps, and VDI, in any case of their sending in a data center, cloud or as a SaaS. Moreover, guarantee that one's clients can also safely and effectively get to corporate assets, like organizing file share.

ii) On-premise Client Catalog for Getting to SaaS Applications

Ventures are progressively depending on SaaS applications such as Office 365. These applications require undertaking clients to get to the cloud exterior of their inner arrange. Most arrangements require clients to move their client registry to the cloud, which might become a security risk to actualize SSO for these applications. This issue can be overcome by picking an SSO arrangement that permits an on-premise client registry for getting to SaaS apps.
iii) Back for Multi-Factor Verification Mechanism and Protocols
Nowadays, most companies have individuals who work remotely; it can be their possess representatives or third-party temporary workers. Whatever the reason may be, organization applications and assets will most likely be gotten to by individuals that are not a portion of one’s client catalog. Depending exclusively on usernames and passwords is not enough. It is merely selecting an SSO arrangement that bolsters other confirmation instruments and conventions of one’s organization. The arrangement ought to permit based on variables like user's area, validity, and app affectability without pointless confinements that can ruin efficiency. An arrangement that can lead intellectuals to identify and react to potential dangers will fortify one’s organization’s security protocols.

iv) Simple Integration into the Company’s Existing Environment
An SSO arrangement does not effortlessly coordinate. One's company's environment will inevitably lead to expanded upkeep and integration costs and destitute client involvement. The correct SSO arrangement ought to effectively fit together with one's existing applications, conclusion gadgets, and confirmation components and conventions. Coordination of the SSO arrangement ought to not require noteworthy adjustment in one's existing environment. The right provider will empower the SSO arrangement without compromising one's company's other arrangements. It ought to too consistently coordinate together with one's Identity providers and also support access based on roles and responsibility.

Figure 2: Framework for implementation of SSO
5. Results and Discussions
In expansion to companies with several diverse sorts of apps, clients utilize different gadgets to get to those apps. Whereas this is often great for efficiency, the related risks have to be tended to fittingly. A multi-vendor arrangement for diverse sorts of applications implies different observing tools that can impressively delay investigating an issue. Subsequently, an organization should select an SSO arrangement that caters to numerous app sorts with checking devices that permit fast settling of issues in any case of the app sort. Furthermore, the SSO arrangement ought to give reports and reviews that permit fortifying one's organization's security conventions based on risk information.

6. Conclusion
The SSO allows users to log in to various applications and maintain its session across the network, with the help of one-time authentication and maintaining a single identity quickly and efficiently without needing users to remember the password every time.

However, along with it, there are various challenges which are there in implementing SSO, at the same time while maintaining, which we have discussed in this paper like main authentication key can be breached or at that the same time due to phishing or man in the middle attack, etc. However, there are sure demanding situations in implementing SSO. Business enterprise no longer most effective and needs to integrate user network logon with nearby application and software program as a service (SaaS) cloud offerings.

Thus, there are lots of benefits of SSO. However, to achieve its full benefit, the challenges need to be tackled efficiently to be convenient and help users use a different range of applications across the network with ease and security.

References
[1]. Courtney Powell, Takashi Aizawa, Masaharu Munetomo, Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments, 2014 IEEE 3rd International Conference on Cloud Net
[2]. 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.
[3]. Yang Jian, An Improved Scheme of Single Sign-on Protocol, 2009 Fifth International Conference on Information Assurance and Security.
[4]. Jian Hu, Qizhi Sun, Hongping Chen, APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS, 9781-4244-6769-3/10/$26.00 2010 IEEE
[5]. [Online] https://www.ijcsmc.com/docs/papers/December2013/V2I12201312.pdf
[6]. Villanueva, J. 2014 "5 Big Business Benefits of Using SSO (Single Sign-On)" Managed File Transfer and Network Solutions.
[7]. Patil, A., Prof. Pandit, R., and Prof. Patel, S. 2013. Analysis of Single Sign on for Multiple Web Applications. J. Advanced Research in Electrical, Electronics and Instrumentation Engineering, (Aug. 2013), 4104-4107.
[8]. C.P. Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol. 4, no. 3, pp. 161-174, 1991
[9]. C. Fan, Y. Chan, and Z. Zhang, “Robust remote authentication scheme with smart cards,” Comput. Secur., vol. 24, no. 8, pp. 619–628, Nov. 2005
[10]. N. Koblitz, A. Menezes, and S. Vansstone, “The state of elliptic curve cryptography,” Designs, Codes Cryptogr., vol. 19, no. 2/3, pp. 173–193, Mar. 2000
[11]. 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
[12]. David J. Boyd, "Single Sign-On to the Web with an EMV Card," 978-1-4244-2249-4/08/$25.00 ©2008 IEEE
[13]. 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
[14]. Ashish G. Revar, Madhuri D. Bhavsar, Securing User Authentication using Single Sign On in Cloud Computing, Institute of Technology, University, Ahmedabad 382 481, 08-10 December, 2011.
[15]. Jian Hu, Qizhi Sun, Hongping Chen, APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS.9781-4244-6769-3/10/26.00 2010 IEEE