e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:02/February-2023 Impact Factor- 6.752 www.irjmets.com

A SURVEY ON SINGLE SIGN-ON TECHNIQUES

S.P. Ghare[*1], Sanskruti Modak[*2], Prerana Jadhav[*3], Tejas Patil[*4]

[*1,2,3,4]Third Year, Information Technology, Jayawantroa Sawant Polytechnic,
Pune, Maharashtra, India.

ABSTRACT

Unmarried sign-on (sso) is a session and consumer authentication carrier that permits a person to apply one set of credentials -as an example, a username and password - to get entry to a couple of applications. Sso can be utilized by companies, small and medium-size groups, and people to simlify the control of more than one credentials. Single signal-on is a federated identity management. Using the sort of device is occasionally referred to as identification federation. Open authorization (oauth) a is the framework that lets in an give up person's account information to be utilized by third-birthday party services, inclusive of facebook, without exposing the user's password. Single signal-on is a federated identity management. The sso idea can be used within an intranet, extranet or internet. This file examines diverse sso techniques and their related blessings through adopting it. It additionally discusses on implementation of various kinds of sso and the protocols used.

Keywords: Single Sign-On, Open Authorization (OAuth), Intranet.

I. INTRODUCTION

In today's digital global, consumer access security refers back to the set of strategies with the aid of which legal users get right of entry to a computer system and unauthorized customers are averted from doing so. However, to make this difference a piece extra sensible, it is crucial to remember the fact that user get admission to protection, even for legal users, is restricted to the parts of the machine that they are explicitly allowed to use (which, once more, is primarily based on their want-to-know). Subsequently, there may be no purpose why someone from payroll ought to have get admission to to confidential scholar statistics. While there's no question that an employer has the right to shield its computing and statistics resources through consumer access security measures, customers (whether or not authorized or now not) additionally have rights. Reasonable efforts should be made to tell all customers, consisting of uninvited hackers, that the machine is being monitored and that unauthorized pastime can be punished and/or prosecuted if deemed suitable. If such efforts aren't made, the employer might also without a doubt be violating the privateness rights of its intruders! An high-quality manner to inform customers of monitoring activity is to display the opening display to them. Through reading a warning like the one underneath, customers explicitly receive both the phrases of the tracking and the punishment once they flow to the subsequent display. Consequently, the primary display screen a user sees while logging into a relaxed pc device have to look something like the following. It makes it less difficult to manipulate the rights of a person who joins, changes roles, or leaves the company, to quickly combine extra programs, and to switch get right of entry to rights throughout holiday durations without increasing the workload of the help table.

II. TYPES OF SSO

Some SSO services use protocols, such as Kerberos or Security Assertion Markup Language (SAML):

Intranet SSO: Intranets improve discoverability and findability by organizing content by task rather than department, using mega-menus to present in-depth content, providing clear cues to orient users, and providing shortcuts to important pages and tools

Extranet SSO: An extranet is a private network that companies use to provide trusted third parties - such as suppliers, vendors, partners, customers, and other companies - with secure, controlled access to business information or operations.

Internet or Web: Web SSO is a browser-based mechanism that enables single sign-on access to applications deployed on web servers.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:02/February-2023 Impact Factor- 6.752 www.irjmets.com

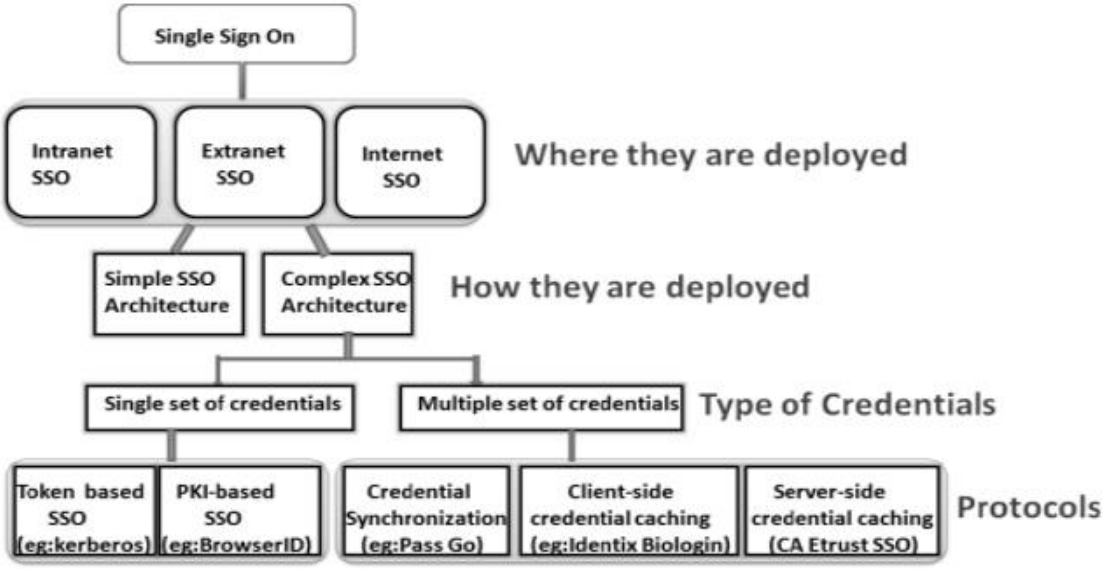

Fig 1: Classification Signal-sign-on

III. SSO ARCHITECTURE

In an average sso structure, identification providers and service carriers change virtual certificate and metadata to set up believe. They interact via open protocols which include security assertion markup language (saml), oauth, and openid (mentioned in more detail under). When integrating sso platforms into your enterprise's it structure, you must cautiously consider present security mechanisms. As an instance, in an sso system, downstream security gear may not understand the supply ip address of a consumer trying to log in to the device. To keep away from disrupting other get admission to control and alerting systems, you ought to make sure that the security gear can nevertheless become aware of the user.

PKI-based Single Sign-On:

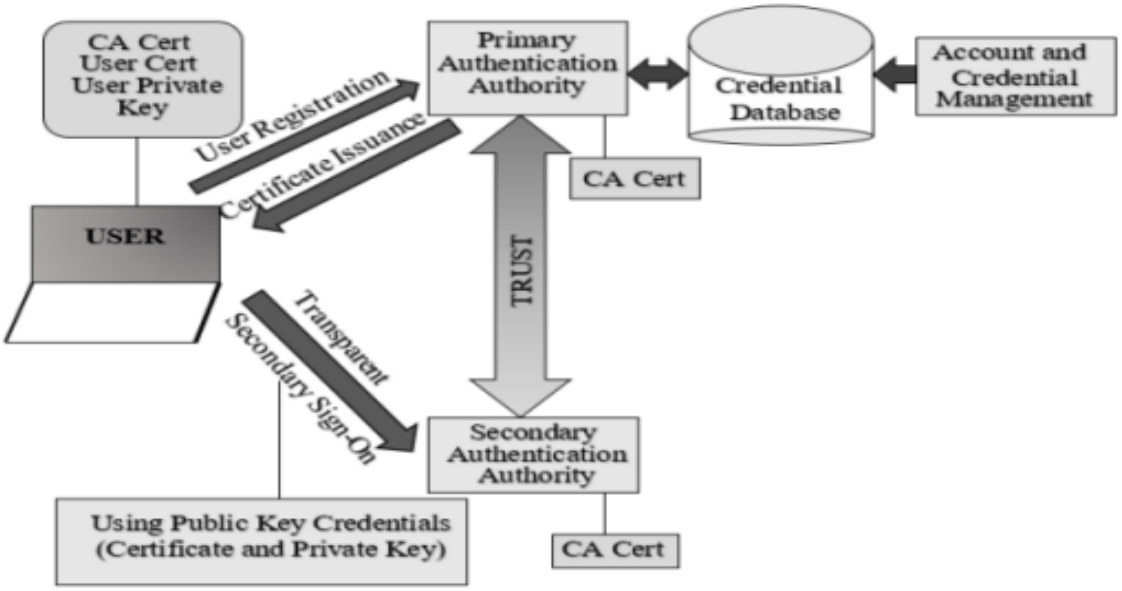

Fig 2: PKI Based SSO

This method uses public key cryptography for user authentication. The gadget is based on the role of the certification authority (ca) for issuing and dealing with the digital certificate and hence the digital identities of the users. The person ought to first identify himself to an authentication authority, which problems a public key certificate to the authenticated user (see figure 4). Whilst the authenticated consumer desires to get admission to a included useful resource in a next authentication request, he/she creates a token and inserts his/her virtual certificates (public key) into it and signs and symptoms it together with his/her non-public key. Upon

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:02/February-2023 Impact Factor- 6.752 www.irjmets.com

receiving the request, the goal server contacts ca to verify the identity of the asking for user. There may be a accept as true with relationship between the number one ca and the secondary ca, because the latter's certificates is issued via the previous. This permits any secondary ca to just accept the certificate issued by using the primary ca. The non-public secret is a protracted string of random binary records and is hard to preserve or keep on paper, but the key may be easily transmitted over a community and is consequently at risk of robbery by means of intruders.

Trust Models of SSO: With a view to examine one of a kind sso answers, distinctive consider fashions want to be described. These fashions range depending on the business situation in which they're applied. The model usually defines the one of a kind entities and their interplay in addition to the overall machine houses. Based on the services that the sso environment supports, three models have been defined.

Token-based Single Sign-On: In this structure, after logging in to the primary authenticator, a person receives a temporary token (see figure five) that he or she will be able to use to maintain getting access to sources or offerings without re-authentication. That is feasible because of the consider dating that exists among the number one and secondary authentication authorities. Determine five suggests that a consumer makes use of his temporary token to get right of entry to the useful resource without having to re-authenticate with the secondary authenticator. An example of this authentication method is the kerberos authentication protocol.

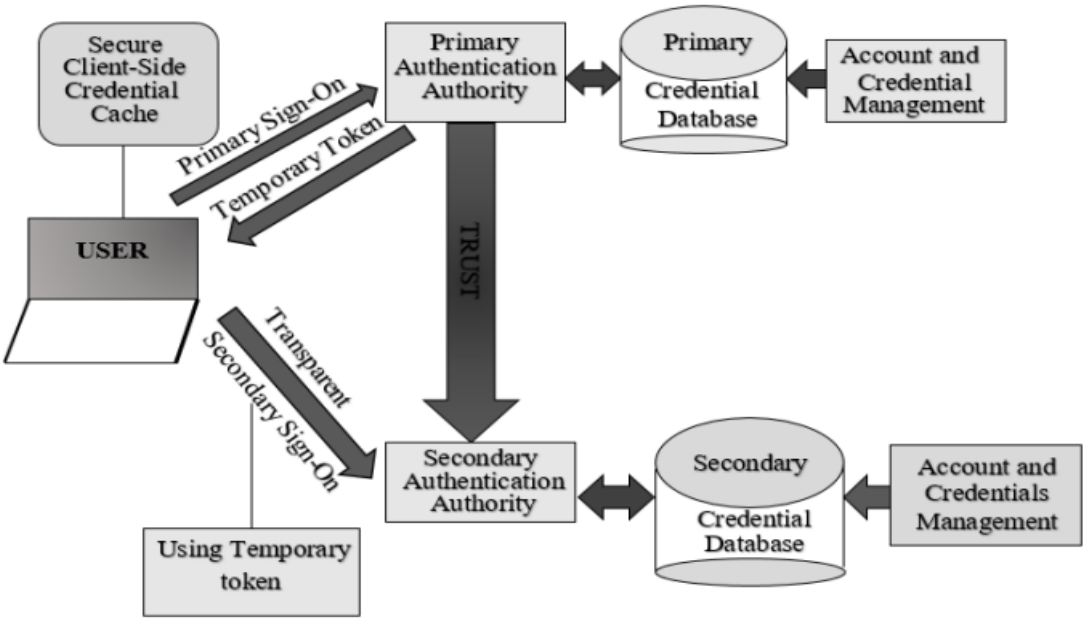

Fig 3: Token Based SSO

OpenID:

Openid join 1.Zero is a simple identification layer built on top of the oauth 2.Zero protocol. It allows customers to verify the identification of the cease person based on authentication executed via an authorization server and to reap simple profile records approximately the give up user in an interoperable and rest -like way. Openid join permits clients of every kind, consisting of net-based totally, cellular, and javascript customers, to request and get hold of information about authenticated periods and quit users. The specification suite is extensible, allowing subscribers to take advantage of elective capabilities together with identification encryption, openid issuer discovery, and signal-out while it makes feel for them to accomplish that.

There are mainly four methods used in OpenID Protocol:

1. Discovery
2. Authentication
3. Association
4. Verification

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:02/February-2023 Impact Factor- 6.752 www.irjmets.com

Discovery: it defines a login flow that permits a client application to authenticate a consumer and gain statistics (or "claims") approximately that person, together with username, email cope with, and so forth. The consumer identification statistics is encoded in a comfortable json net token (jwt) referred to as id token.

Authentication: the oidc specification states that authentication can comply with one of 3 paths: the authorization code go with the flow, the implicit waft, or the hybrid drift. The drift determines how the identity token and the get admission to token are back to the purchaser.

Association: op makes use of this association to sign next messages, and rp to verify those messages; this gets rid of the want to confirm the signature without delay after each authentication request/response.

Verification: verification of the statistics discovered, verification of the signature, and so forth

Browser ID:

Browser id is a complex, real-worldwide single sign-on (sso) device for internet programs nowadays advanced through mozilla. It makes use of new html5 capabilities (along with internet messaging and net storage) and cryptographic assertions to permit decentralized login at the same time as respecting consumer privateness. It may perform in a primary and secondary identification provider mode. Whilst browser identification runs in primary mode with any identification issuer, in secondary mode there is most effective one identification business enterprise, mozilla's default identification provider.

Primary Identity Authorities (Primary): Identity and access management (iam) is a framework of enterprise strategies, rules, and technologies that helps the control of electronic or virtual identities. With an iam framework, it managers (it) can manipulate person get admission to to vital facts inside their organisation. Structures used for iam include unmarried sign-on systems, multifactor authentication and privileged get admission to management. Those technologies additionally offer the ability to safely save identification and profile records, in addition to facts governance abilties to make certain that most effective records this is important and relevant is shared.

Depending events (rps): show the authentication

The implementation company (ip): it's miles used for native aid of the web browser to implement the patron a part of the device.

Certificate provisioning: it assessments the e-mail addresses of the primary customers and the signed certificates.

Statement generation: it's miles a system that produces the declaration to one's e-mail address.

Assertion verification: it's far the technique of verifying the declare of ownership of the person.

IV. CONCLUSION

SSO is an access control method that allows a user to access multiple domains with a single authentication step. This eliminates the need for the user to remember numerous passwords for multiple applications. SSO is used for ease of use. However, if the authentication master key is cracked, important user data can be compromised. Single sign-on can become much more important with the emerging cloud computing technology that provides ICT services and also reduces the likelihood of phishing attacks. However, since single sign-on provides single sign-on access, it should be implemented in a secure manner. Therefore, the benefits of SSO are worth mentioning, and if the drawbacks are properly addressed, it will be convenient for users and help them access applications with ease and security. As part of future work, we would like to focus on implementing security mechanisms in combination with SSO.

V. REFERENCES

[1] Li, B., Ge, S., Wo, T. Y. and Ma, D.F. 2004. Research and Implementation of Single Sign-On Mechanism for ASP Pattern. In Proceedings of the Third International Conference on Grid and Cooperative Computing.

[2] [Online]http://blogs.vmware.com/vfabric/files/2013/03/a uthentication_chart.png

[3] 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.

[4] Ardagna, C. A., Damiani, E., Vimercati, S. C., Frati, F.and Samarati, P. 2006. CAS++: an Open Source Single Sign-On Solution for Secure e-Services. In Proceedings of the 21st International Information Security Conference on Security and Privacy in Dynamic Environments.

[5] Elisa Bertino, Kenji Takahashi. Identity Management: Concepts, Technologies and systems. 685 Canton StreetNorwood,MA02062,ArtechHouse,2011;55-9,77-9,86-7,98-100,119. http://books.google.co.in/books?id=UrmDGxt-8IC&printsec=frontcover#v=onepage&q&f=false.

[6] Web Single Sign-On System for WRL Company. Si Xiong, Department of Internetworking, Royal Institute of Technology (KTH), Sweden; 2005; http://web.it.kth.se/~johanmon/theses/xiong.pdf

[7] OpenID Foundation website. http://openid.net/.

[8] BrowserID by Mozilla. https://browserid.org/.

[9] Web Single Sign-On System for WRL Company. Si Xiong, Department of Internetworking, Royal Institute of Technology (KTH), Sweden; 2005; http://web.it.kth.se/~johanmon/theses/xiong.pdf.

[10] Two SSO Architectures with a Single Set of Credentials.

http://www.cs.auckland.ac.nz/courses/compsci72 5s2c/archive/termpapers/zlu.pdf. 6. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, OASIS; 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.