ISSN:0975-9646

A Review on Single Sign on Based Secure User Authentication Scheme and Technologies

Dr. Jaishri M. Waghmare[#1], Divya Kalyankar[*2]

[#]*Associate Professor, Computer Science and Engineering Department*
SGGS Institute of Engineering and Technology, Nanded
[1]jmwaghmare@sggs.ac.in

[*] *Computer Science and Engineering Department*
SGGS Institute of Engineering and Technology, Nanded
[2]2019mns017@sggs.ac.in

***Abstract*—Nowadays in today's digital world, everyone uses different applications for various purposes. To use these application services the user must have its login credentials. The user uses so many applications, for that purpose user needs different username and passwords for every application. It is difficult to remember this username and passwords. This led to the concept of a single sign on (SSO). SSO is an implementation of single a step of authentication which allows a user to use all system applications. SSO manages a user centrally. It has large productivity. The SSO system does not centralize account information for all application rather than it stores account information in a single account. Security Assertion Markup Language (SAML) is used in Single sign on protocol. This paper presents review on a Li et al's scheme and dynamic ID based scheme using smart cards for multi-server environments and discuss architecture, protocols, benefits, analysis related to SSO. The combination of SSO with Multi Factor Authentication (MFA) helps to reduce the risk of an authentication.**

***Keywords*— SAML, Single Sign On (SSO), Multi-factor Authentication (MFA), Authentication.**

I. INTRODUCTION

SSO Limits access to system resources. It authenticates a user once and permits access to use resources and all services after authentication. It does not prompted to sign in again. Therefore, SSO method login securely to each application. Every application has its own process of authentication, user need to do all login steps [1].

Previously a user has to sign up in an application before using it. Sign up contains information about the user. Then it stores username and password. Each time to login to that application a user needs to give username and password. A user has to remember so many passwords for different applications. So usually the user uses easy password and also they can use one password to all applications. This method is easy, but it may cause a threat. An attacker can easily crack that passwords and may steal confidential information. By the SSO method user are being escape from this threaten. A user needs to login once and then they can easily use various applications securely.

In SSO approach, once a user login then he can get access to multiple applications easily. These applications could be from a single organization or multiple organizations, that is some are from one domain and some from multiple domains. This federation allows user to access the third party application after login once from the different organization. This makes SSO easy to use as shown in fig. (1).

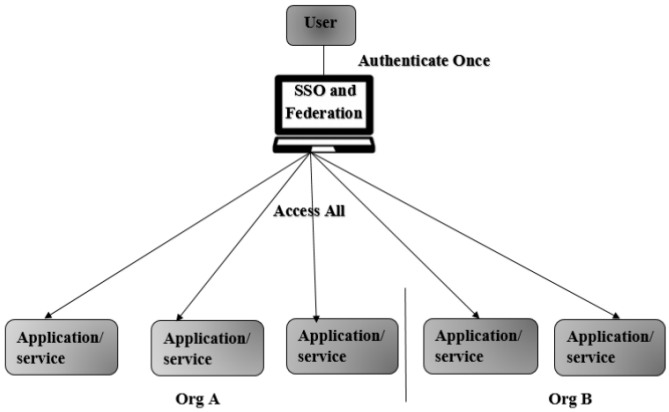

Fig. 1: SSO overview

Recently, the smart card based password based authentication scheme have been proposed. These schemes classified as static ID and dynamic ID schemes. Static ID discloses some information about a user's confirmation messages. A user uses the same static ID in every session to login into server. From this, an attacker gets a chance to discover a valid user. The dynamic ID requires two-factor authentication i.e. using password and identity. Dynamic ID preserves the user's confidentiality. As each new authentication process arrived, the user's id changes. In this case there is no possibility of verifier attack because server does not keep verifier table

II. A REVIEW OF LI ET AL.'S SCHEME

In 2013, Li et al [6] proposed a new dynamic ID based remote user authentication scheme using smart cards. In this scheme there are three participants that are the registration server, the server and the user. RC chooses 'x' i.e. a master key and 'y' i.e. a secret number. This x and y calculate h(x||y) and h(SID||h(y)) and then shares with server over a secure network. This scheme involves four phases that are registration, login, verification and password change phase.

In registration phase, a user submits its credentials like identity, ID, password to RC. RC calculates security parameters by using master key x and secret number y, and then saves it in a smart card. RC sends a smart card to the user through a secure network. In login phase, the user types his identity and password in a given smart card. The smart card checks the password and if it is correct then it sends the login request. A user sends a request to server. In next phase, user and server mutually authenticate each other. The password change phase allows changing password.

This scheme has drawback i.e. vulnerable to server spoofing attack and forgery attack.

III. Dynamic ID based multi-server authentication scheme

A. Architecture

This architecture has four main components that are Registration Server (RS), Service Provider (SP), Authentication Server (AS) and a user. RS and AS work together. A user tries to get access to services. The identity provider (IdP) consists of RS and AS. RS and AS has trust relationship. Firstly, a user and SP need to register with RS then they can become part of a whole system. Then SP submits all information and details to RS. RS job is to check credentials of SP. If given credentials is right then the RS send a confirmation request to a user or system. A user has to register on RS before using services of SP. A user has to click on registration link which is shown on a web page of SP side. Further, that link is redirected to RS's page. Hence, RS gives a single registration for all SP's.

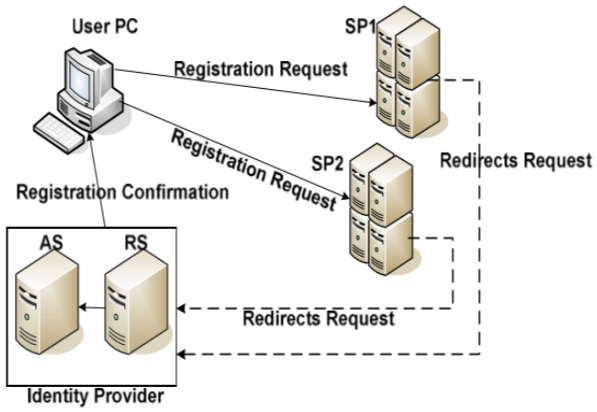

Fig. 2: User registration and confirmation

B. Security Assertion Markup Language (SAML)

SAML is a core feature of federated SSO. It is based on XML language. SAML exchanges data between IdP and SP. It permits conveying between domains which has different authentication mechanisms. It stores the user's information which is mandatory for SP to identify a user. The IdP gives an assertion about the user's identification. Then, at last SP make a decision and provides specific services to target applications.

C. Authentication phase

A user tries to get a resource through a browser on a SP. At an initial stage, browser and SP does not have a connection. When browser requests, the SP checks a user is authenticated or not. If a user is not authenticated SP generates SAML request for the user. The SAML request contains SID of the SP. IdP get to know from SID which SP send the request. IdP checks for a valid session and if it is not an available then it will ask for login. An IdP sends login request form to user. A User submits its credentials in form. After that the IdP validates credential. IdP generates SAML response and send to user in POST form. A user sends HTTP POST with SAML response to SP. SP check login credentials. If credentials are valid, it redirected to various applications [3].

For example, a user wants to access GOOGLE for using its application. The SP decides whether to perform a requested action for that specific user or not. SP request to IdP to give an assertion based on which SP make a decision.

In password change phase, when a user tries to change his password then he inserts smart card along with ID and password. The smart card checks the password and redirected to login. The user is not directed to server for changing password.

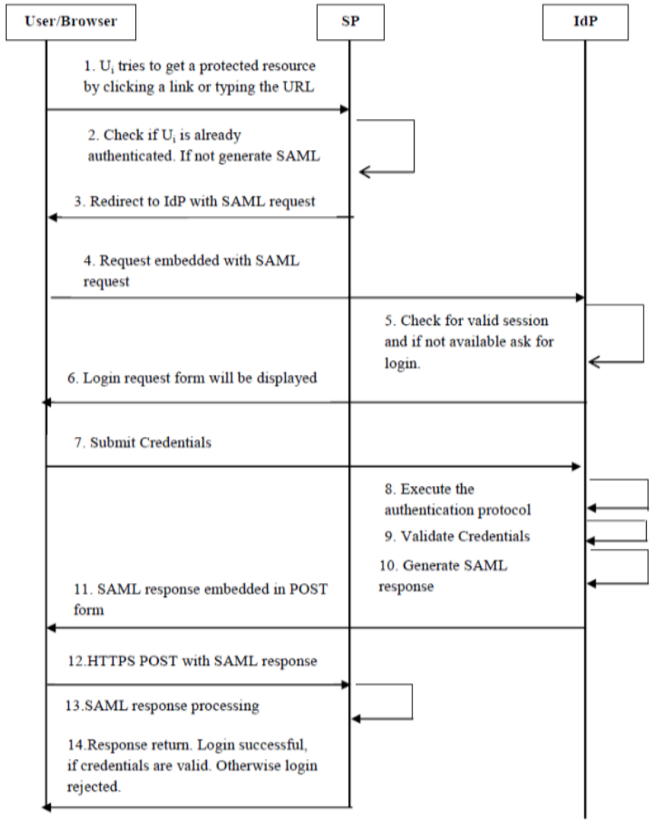

Fig. 3: Authentication phase

IV. Architecture of SSO

The types of SSO architecture are Token-based single sign on and Public key infrastructure based single sign on which needs only one set of credentials. This architecture is applied

to various situations, based on their characteristics and usage. This architecture is discussed below [5]:

A. *Token-based Single Sign On:*

In this authentication method, a user can get a temporary token after logging into primary authentication authority. A token provided by primary authentication authority used further to access the services. The primary authentication authority and secondary authentication authority has trust relationship. As shown in below figure, a user uses the same token to secondary authentication authority without revalidating itself again. The Kerberos authentication protocol is an example of Token-based single sign on.

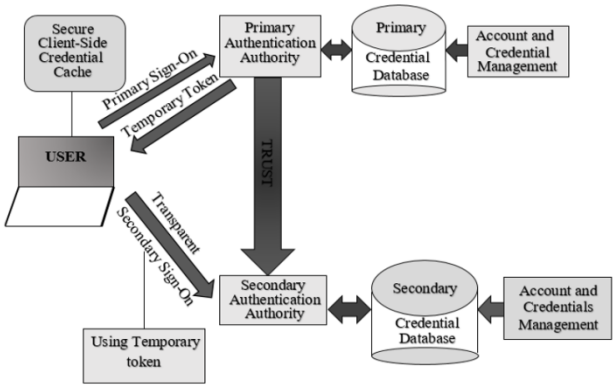

Fig. 2 Token based SSO

B. *PKI-based Single Sign On:*

In this authentication method, public key cryptography is used to authenticate a user. For this purpose, Certification Authority (CA) issues and manages digital certificates of users. An authentication authority checks user identity and then provides public key certificate to valid users. If a user wants to use some particular resource then he/she needs to create a token, which includes digital certificate or public key and must sign it with private key. On getting request CA checks the identity of requested a user. The primary CA and secondary CA has a trust relationship between them. Because of this secondary CA accepts the certificate through primary CA.

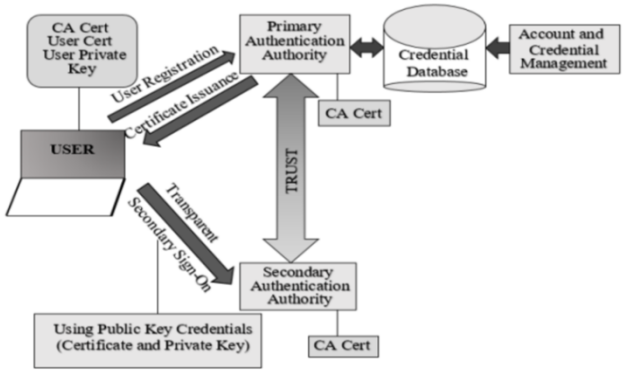

Fig. 3 PKI based SSO

V. SECURITY ANALYSIS AGAINST DIFFERENT ATTACKS

A. Masquerade user attack:
To perform masquerade attack, the attacker has to get unauthorized access and he has to pretend a valid user. To create valid login request an attacker must know nonce n1. If an attacker has a smart card then also he cannot login without knowing the password.

B. Denial of service attack:
In the suggested scheme, the password is mandatory, if an attacker wants to login into the system. In addition to this, the smart card also checks the validity of the password. These authentication methods restrict an attacker to send fake login requests. Thus, the scheme is safeguard from DOS attack.

C. Reply attack:
In the suggested scheme, the system generates nonce value to prevent reply attack. Nonce values are unique, generated for each session from an additive cyclic group. Thus, values are different to guess for an attack.

D. The password guessing attack:
A smart card contains encrypted value which is converted to hash value. If an attacker wants to login, he/she needs to decrypt the hash value and also that value is not possible to guess hence, SSO prevents login from password guessing attack.

VI. SSO SUPPORTED TECHNOLOGIES AND PROTOCOLS

Following are the protocols and technologies that are supported by SSO:

A. *Kerberos:*
A Kerberos is the best technology for an organization to verify a user who wants to use SSO with multiple applications but Kerberos should be supported by system applications. Kerberos is a protocol which uses KDC as a server. KDC validates a user for the specific time period.

B. *LDAP:*
The directory server used to store information regarding an organization such as employee name, an employee id, an employee contact number and employee credentials in a single database. LDAP is used to extract information from directory servers. Microsoft's version of LDAP is an active directory which gives authority to SSO. But the active directory works on a window's operating system only. For SSO, a central LDAP is used as a single database for all applications rather than using a database for each application.

C. *Cookies:*
Cookies are a small piece of information which stores on a user's machine. The cookies are used in SSO technology to validate session for the fixed period of time. When the cookie expires then a user has to re-authenticate.

D. *Digital certificates and public key infrastructure:*
Public key cryptography is used to authenticate a user. For this purpose, Certification Authority (CA) issues and

manages digital certificates of users. An authentication authority checks user identity and then provides public key certificate to valid users. If a user wants to use some particular resource then he/she needs to create a token, which includes digital certificate or public key and must sign it with private key. On getting request CA checks the identity of a requested user. The primary CA and secondary CA has a trust relationship between them. Because of this secondary CA accepts the certificate through primary CA.

VII. BENEFITS OF SSO

SSO authentication method has some pros as discussed follow [2]:

A. *Enhanced user productiveness:*

SSO allows a user to login into multiple applications using a single ID and password which reduces the burden of memorizing different IDs and passwords. SSO saves user's time and increases productivity.

B. *Increased developer productivity:*

SSO implementation gives a monotonous authentication framework to developer. As the mechanism of SSO is independent, developer need not think of authentication. If a request to application comes with a username then developers can presume that the authentication is already done.

C. *B2B collaboration:*

In recent years, some companies are working together to get better outcome. This combination of various companies is compatible when they are a link with their different IT systems and those are able to share data easily. An enterprise allows clients to use data and its own applications. Thus, SSO place authentication information in one database and allow users to login once. Therefore, a user is allowed to use all applications of other organizations also.

D. *Security:*

In SSO, A user has to create only one password. That is why the user can create strong, difficult to guess password rather than creating many easy passwords.

VIII. COLLABORATION OF SSO WITH MFA

Authentication is the process in which one needs to prove his/her identity and verify a name. There are different types of mechanisms used for authentication like digital signatures, passwords, one time password (OTP), etc. If a user satisfies at least two of the below listed mechanisms, then that authentication is known as Multi Factor Authentication (MFA). The something which is known to you that is a PIN or a password. Next one is something already is with you like ATM card or cell phone. Next is something represented by you that is fingerprint, iris recognition. .

A well-known example of MFA is an ATM card transaction where two of the three conditions listed above are fulfilled. A user must need ATM card for doing the transaction. This satisfies the condition "something already is with you". Apart from this ATM pin code is also required for doing a successful transaction. This satisfies another condition that is "something represented by you". If MFA is used in addition with SSO, then this collaboration will decrease security concerns of SSO and hence it increases security.

The figure (4) shows SSO in addition with MFA in which first user logs in through SSO approach. Then he/she goes via the next authentication step like the OTP, then a user able to use the resource. A user can get OTP via different channels. OTP has the time limit. If it is not used within the time limit, then it expires.

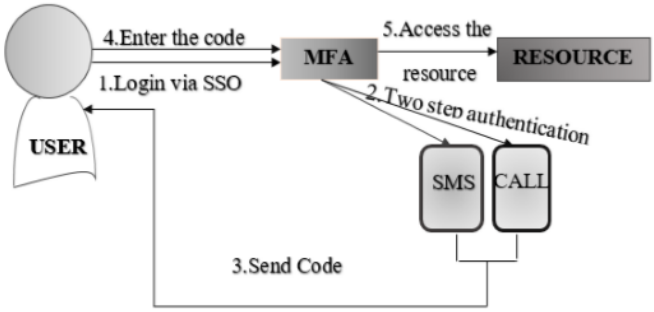

Fig. 4: A combination of SSO with MFA

IX. CONCLUSIONS

SSO is an authentication method in which a user can get access to multiple domains using a single authentication step. This reduces the user's burden of memorizing many passwords for different applications. In 2013, Li et al proposed a new dynamic ID based remote user authentication scheme using smart cards. This scheme is vulnerable to forgery attack and server spoofing attack. This scheme adopts SAML single sign on feature and maintains various authentication credentials. It provides more security and avoids security weaknesses. Compared to the other scheme, the proposed scheme is more secure and provides proper authentication method. The problem of losing data can be decreased by using SSO with MFA. The combination of SSO with MFA requires second step authentication for user login. So that user credentials cannot be by knowing only a master key.

REFERENCES

[1] Tayibia Bazaz, "A Review on Single Sign on Enabling Technologies and Protocols", in Int journal of computer Applications, vol. 151, no. 11, October 2016.

[2] V. Radhaa, D. Hitha Reddya, "A Survey on Single Sign-On Techniques", 2014.

[3] Sumitra Binu, Mohammed Misbahuddin, Pethuru Raj, "A Single Sign on Based Secure Remote User Authentication Scheme for Multi-Server Environments".

[4] Patil, A., Prof. Pandit, R., and Prof. Patel, "Analysis of Single Sign on for Multiple Web Applications", J. Advanced Research in Electrical, Electronics and Instrumentation Engineering, Augest 2013.

[5] Yebin Chen, Bing Xia, Baozhu Wu, Lianghong Shi, "Design of Web Service Single Sign-on Based on Ticket and Assertion", 2011.

[6] X. Li, J.Ma, W.D. Wang, Y.P. Xiong and J.S. Zhang, "A Novel Smart Card and Dynamic ID-Based Remote User Authentication Scheme for Multi-Server Environments", Mathematical and Computer Modeling, 58, pp. 85-95, 2013.

[7] [online] https://dacurry-tns.github.io/deploying-apereo-cas/setup_initial-setup-tasks.html#install-development-tools-on-the-master-build-server

[8] [online] https://apereo.github.io/cas/6.3.x/index.html