Securing e-Governance applications with Single Sign On - eGovSSO

Amit Shah[1] & Shailesh Khanesha[2]
[1,2] National Informatics Centre (NIC), Govt. of India, Gandhinagar (Gujarat), 382010

Received: July 06, 2018 Accepted: August 13, 2018

ABSTRACT *The increasing demand of information security has opened up a window for research and innovative services development opportunities for single on approach. Government system anticipates delivery of secure electronic transactions in an integrated manner. This paper has made an attempt to develop user friendly Single Sign On paradigm to for e-Governance applications in faster and cost-effective way. The eGovSSO framework provides an improved mechanism for User Management, Authentication, Authorization, and Integration of common identity and sharing of common dimension for various e-Governance applications.*

Keywords*: SSO, e-Governance, LDAP, e-Pramaan, Security, Login, OTP, Biometric, eGovSSO*

I. Introduction

SSO is categorized by Peterson as 1) Password synchronization – It is an old approach where multiple systems have unique usernames but a common password. 2) True SSO – It is one username and one password based system. Microsoft built this for windows with Active Directory. 3) Web SSO – It uses standards such as SAML or Windows Federated Authentication to create a trusted relationship 4) Enterprise SSO – It is flexible and allow user to preserve password for individual application, but this system is difficult to implement due to integration issues [1]. Now a day, the Single sign-on (SSO) for enterprises and individuals is considered one of the significant regulations of implanting the e-Government transactions. Such regulations provide that each individual shall have a unified login credential for e-Governance applications. The said unified login credential will be able to fulfill all requirements of concerned officer or user to e-Government Transactions and their applications. The SSO can be considered as an electronic referential identity relating to individuals in government [9].

In the single sign-on approach the system is required all the identification and user credential information which is necessary to support the authentication of the user to each of the secondary domains or applications that the user may require to interact with. The information supplied by the user is then used by Single Sign-On Services to support the authentication of the user to each of the secondary domains with which the user actually requests to interact. From a management perspective the single sign-on model provides a single user account and its management interface through which all domains or applications may be managed in a coordinated and synchronized manner. Single Sign-On model provides significant security aspects such as the secondary domains have to trust the primary domain to correctly assert the identity and authentication credentials of the end user and protect the authentication credentials used to verify the end user identity to the secondary domain from unauthorized use. Also the authentication credentials have to be protected when transferred between the primary and secondary domains against threats arising from interception leading to possible masquerade attacks [10]. Governments are moving to improve their services by adding new paradigm such as citizen's unique identity; with this new demand single sign on system provides a way for security of government transactions as well as more attention and concentration on effectiveness of governance, public services delivery, accountability and responsiveness.

This research aims to identify, describe and produce an integrated framework of Single Sign On for e-Governance applications. There are below objectives are set for undertaking this research.

- To evaluate how Single Sign On approach can be used as a tool for government applications.
- Addressing the issues of user authentication, authorization and user management for e-Governance applications.
- Better Single Sign On mechanism for e-Governance application.
- Integration of common identity among various e-Governance applications
- Sharing of common dimensions amount various e-Governance applications (e.g. District, Block, Village, Schools, etc.)

The rest of the paper is organized in the chapters of Existing Systems, eGovSSO Framework,

Implementation, Impact, Result and Conclusion. Existing Systems chapter gives a brief survey of related works on existing systems. eGovSSO Framework depicts the proposed model of Single Sing On and its development, Implementation chapter depicts implementation and validation. Impact and Result chapter shows the implementation result of eGovSSO model and the last chapter specifies the conclusions.

II. Existing Systems

Stephen Lawton [1] has discussed the challenges comes in implementation of SSO and some SSO solutions for enterprises. Such SSO provides an extra layer of security to authenticate and authorize users based on Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). One of the biggest challenges to work SSO efficiently is that to indentify the user is not always consistent throughout the enterprise. Other challenges are global profile of each users need to be include, audit and access control policies for users, risk associated with single system may cause damage to other connected system, different systems linked with SSO have varying access credentials and weak password policy creates potential security gaps it should be complex, long and frequently changed [1].

Andreas Pashalidis et.al [2] has classifies SSO approaches to take the decisions about the design and selection of SSO for the organization. Also identifies important differences of security properties provided by various approaches. From the classification, it is clear that all SSO architecture has its own strength and weakness and must carefully consider the environment before adopting particular SSO. Such as pseudo-SSO systems are probably more suitable for closed systems where privacy protection is less required. Identity management in the closed system is just management of life cycle user credentials. On the other hand identity management in open environment (internet) needs to incorporate privacy protection.

Yang Jian [3] has undertaken the issues of several potential security vulnerabilities such as password attack and replay attack in the traditional single sign on protocol (Kerberose). To prevent password and replay attack, he has proposed a new improved scheme for single sign on protocol by adding two data flows while client request for service. One is from authentication server to ticket granting server and second flow is from ticket granting server to application server, meanwhile add an authenticated customer database for authentication validation and authorized customer database for authority validation of client request. Implementing the proposed protocol, replay attach is prevented through double time check and greatly reduce the client security risk and its workload.

Jingquan Wang et.al [4] has addressed the issues of existing SSO schemes that do not satisfy the security concepts (unforgeability, impersonation and soundness) and require a high trust level on trusted third party (TTP). They have proposed a generic SSO scheme by using nominating signature algorithm which involves signer(S) and nominee (N). Implementing the proposed scheme they have formalized a security model of single sign-on in which service provider (SP) is not required to communicate with TTP at the time verification of user's credential. Also observed that the soundness is satisfied and reduced dependency on the trusted third party.

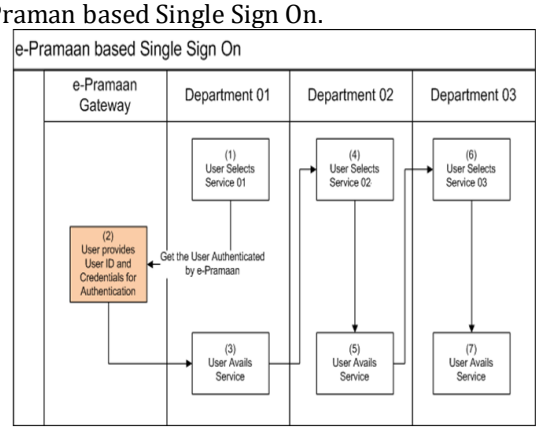
One of the simplest ways to implement SSO is by using LADP (Lightweight Directory Access Protocol) server. SSO implementation using LDAP is described in [5]. In this approach user logins to web application "A" that validates the user information and generates an authorization identifier. Request is route with this authorization identifier to LDAP server. The routed request is validated against the user information at LDAP Server, if validation result is true then the application will populate the user credentials along with the authorization identifier. Now when user clicks on SSO site link, application will send the user information to web application "B" with the authorization identifier. Web application "B" will route the request to LDAP server for user validation. On LDAP server, user is authenticated and identified against user information stored in LDAP server and will automatically log on to the web application "B" if correct user credentials are passed. In this method user login to the web application "A" to initialize the session and send session ID to web application "B". Web application "B" will always check the user session by passing the session ID on the web application "A" before performing the business processing.

The drawbacks of SSO approach using LDAP server are (1) Additional licensing cost and maintenance support for LDAP server (2) Enhanced network security is required to communicate with the applications and (2) Required customization of application for integration with other system [5].

OneLogin is a Single Sign On tool that connect LDAP infrastructure and cloud applications. Advantages in OneLogin are single password, unify multiple directories, avoid point to point application integration, centralized access control and centralized audit trial [6].

Alka Mishra et.al [7] has addressed the issues of login management in MyGov portal and its various sites. They have developed oAuth based Single Sign On system for accessing various sites and apps of MyGov. It provides seamless participatory activities without multiple times signing in for citizen. Also provides a mechanism to use this solution by any client application. The focus of this system is to provide login for citizen.

The e-Praman framework suggested by government of India to address the requirement of access management and authorization associated with e-Governance applications [8]. The key components of this framework are (1) Identity Management to ensure trusted and reliable online delivery of government services to the authenticated user (2) e-Authentication to verify the identity of the user (3) Authorization for verifying that the user has the permission to perform a certain operation in the application (4) Credential Registration such as login password, digital certificate or biometric fingerprints (5) Permission Assignment to provide user access to online services (6) Deregistration to deactivate the user from the system and (7) Single Sign On to enables a user to authenticate once and gain access to the resources of multiple applications. Also user may be prompted an additional authentication credential such as OTP (One Time Password), digital certificate or biometric finger prints, etc. depending on the sensitivity level of application or transaction. Below figure shows e-Praman based Single Sign On.



[Fig. 1: e-Pramaan based Single Sign On]

From the analysis of existing Single Sign On system, it is stated that several key requirements in government domain are not satisfied by the existing system. These are

- Authentication levels such as password, OTP, biometric finger prints, etc. based on sensitivity level of application to verify the identity of the user of various e-Governance applications.
- Access privileges or role based access to users for various e-Governance applications.
- Management of user transfer from one government office to other
- Management of common master records such as city, block area, village area, health facilities, police station, hospitals, schools, banks, etc. for all e-governance applications. It is useful to integrate all applications to evaluate on the same dimensions.
- Dedicated government agency for the development and maintenance of Single Sign On hosted on government data centre. It prevents the issues of licensing cost and maintenance support.

To face the above challenges and fulfill the government requirements, eGovSSO is designed and developed to achieve secure user authentication and authorization for various e-Governance applications as well as reduce development cost of user management module.

III. eGovSSO Framework

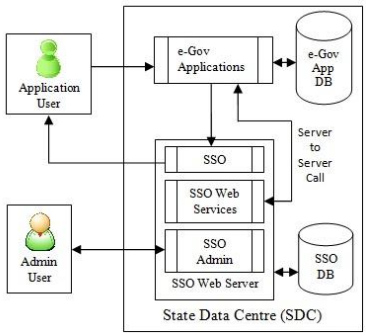
The literature review findings and subsequent analytics to ascertain parameters to be considered with their existing levels need and enhancement. A framework is needed to be developed to facilitate single sign on with secure mechanism for all e-Governance applications. The eGovSSO framework is an integrated solution for common master codes, user management and user authentication

A. Technology Adoption

eGovSSO is web based system developed on Microsoft platform using .NET framework as frontend and MSSQL server as backed. Also integrate SMS module for OTP (One Time Password) and alerts of significant event to the concern user. Biometric finger prints of user is captured and validated for authentication purpose. XML and WCF (Windows Communication Framework) based web services are developed for authentication on smart client or mobile applications and sharing of common master data and necessary user information to the application using SSO. This system is hosted in government state data centre and managed by government officials only. Also web service access of the system is validated using secure token as well as limited to server of e-Governance applications which are using single sign on.

B. Architecture of framework

Architecture of the framework is shown in fig. 2. System of eGovSSO is hosted in secure environment of government data centre.



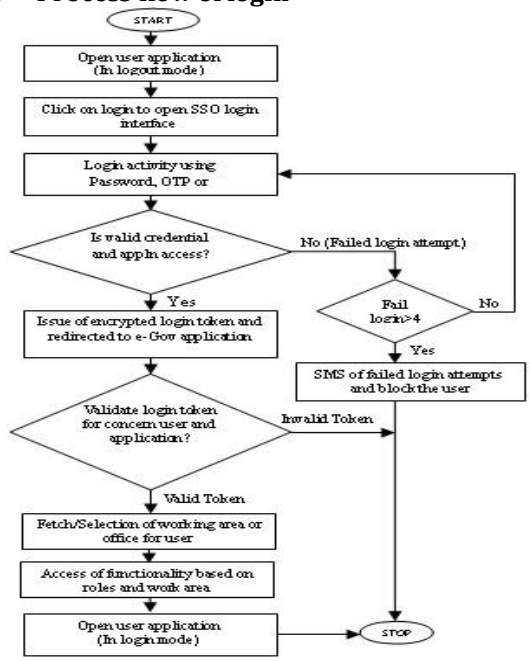
[Fig. 2: Architecture of eGovSSO]

As shown in the architecture, SSO web server having three different modules hosted in the government data centre.

1. SSO: it is only for the purpose of user login in different e-Governance systems including SSO Admin. Also, this module enforces centralized username/password policies as decided by government. It has an option of authentication through OTP and Biometric finger prints depend on the sensitivity of application.
2. SSO Web Services: Web services are provided to access user data and concern dimension or master tables such as office, user roles, district, blocks, villages, urban local body, etc. by the registered e-Governance applications only. The web service access call is restricted to the server of e-Governance applications for security purpose. All the servers of e-Governance are installed in the network of government data centre.
3. SSO Admin: It is developed and hosted only for user administrator to manage users under concern territory. State administrator has an access of full module including management of common masters and all user details. There is second level user authentication using biometric finger prints or mobile/email OTP while login into this module. Also, second level authentication option is provided to the other applications based on its sensitivity. Administrator have privileges to create users, reset password, enrollment of biometric figure prints, mobile verification, to give access of concern applications and roles into it, posting of user in office, etc..

All these three modules are integrated on the same platform. Two user groups are identified, one is application user or normal user and other is admin user or super user. Users are further classified by roles in the application and designation in the office category.

C. Process flow of login



[Fig. 3: Process flow of user login]

Fig. 3 shows the complete steps happening while login process. SSO login interface issues an encrypted login token and redirect the user to calling application after successfully login. Calling application validates the token through SSO web service and access the user profile from SSO server. Also access of SSO web service is validated through web service access code provided to the application which is using SSO. In addition, SSO web services are available to the web servers of e-Governance applications only other IP addresses are restricted.

D. Features of the eGovSSO system

- Single login interface across multiple system
- 2nd level authentication OTP or Biometric for critical e-governance applications
- Centralized enforcement of username and password policy
- Aadhaar based biometric finger prints verification and authentication of users as per new IT Act. and switching to new rules and condition.
- Office Dictionary of government with office details such as Head of office, Phone no., fax, address etc.
- User/Employee dictionary of government with details such as contact details, office, designations, phone, mobile no. etc.
- Application access control
- Detailed user access logs and reports
- User transfer facility
- Centralized access of masters such as Offices, Designations, Districts, Talukas,

Village, Regions, Gram Panchayats, Nagar Palikas etc.
- Authentication using web service or web APIs
- SMS interactions for reset user password(forgot password), acknowledgment of user creation, users
- transfer, intimation of locking users due to failed login attempts, etc. on verified mobile numbers
- Application user management by application manager/project leaders/Concern Authority.
- Mobile Application for state and district administrator to manage users

IV. Implementation

Different **SSO** protocols share session information in different ways, but the essential concept is the same, there is a central domain, through which authentication is performed, and then the session is shared with other domains in same way as shown in Fig. 4.

[Fig. 4: SSO Login]

Implementation of this system incorporates below mentioned activities which satisfy the needs of governance.

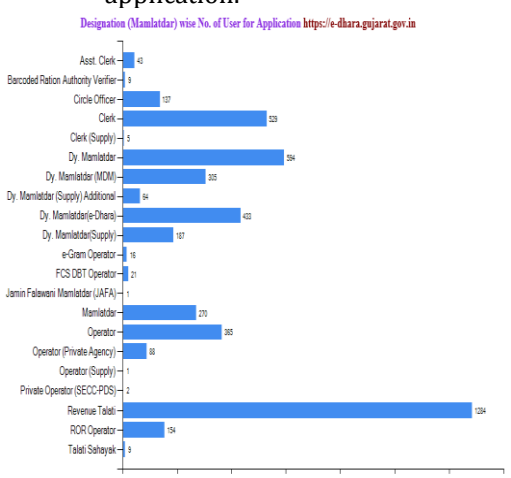
1. Application Management
   - Registration of application with application/project leader, name of application, URL, Logo, Login policy (Captcha, OTP, Biometric) etc.
   - Define user roles in application
   - Aapplication and role access and denied for users
   - Office level restriction to access application
2. User Management
   - User creation with all details including biomatrics and photo
   - User posting or access for particular office and designation in the office
   - User access rights for applications with roles in application if any
   - Partial restriction to access functionality of the application
   - System sharing with third party to manage its users
3. Office Management
   - Office Level i.e. State, district, region, taluka (sub-district), village, division, etc. For Revenue department, Secretary at State, Collector at District, Mamlatdar at Taluka and Talati at Village level. For Post department, CPMG at State Circle, PMG at State/Region and Post master at Division and/or post office. For Forest department, from lowest to highest, Beat Guard → RFO → DCF → CCF → APCCF → PCCF → Secretary → Minister
   - Office Application link Master for pparticular application can be accessible to specific office and specific designation. Also, bulk assignment of application to existing designations.
   - Office creation with office details including parent office hierarchy.
   - Designations addition in office with flag of HOD, Single or Multiple and for government or private user.
4. Security and Audit
   - Login with password – Single Factor Authentication
   - Login with OTP or Biometric finger print – 2 Factor Authentication
   - Audit trails including records of user activities such as login, logout, failed login attempt, change password, etc.
   - Application access rights to define application level roles/permission for user
   - Application access restriction at office and designation level.

V. Impact and Result

Successful implementation of eGovSSO model in Gujarat (India) having more than 200 e-Governance applications, 98 thousand offices and 1.08 lakh active logins. Below are some case studies on result of eGovSSO implementation

- Banks have to be given access land records data and going to have right to insert/modify.
  - For user management Lacks of user id to be created and maintained. Super Admin (SA) of each bank created and in turn SA created further SA and all SA created last mile users
  - One officer is responsible for down the line user management

  - Application Roles for working in style of entry and approval
  - For audit trail, application has logs of functional logs and eGovSSO has access/login logs
  - Banks Master and their hierarchy created in eGovSSO.
- Implementation of Aadhaar(UID) based authentication
  - In e-Dhara (Land Record Computerisation), system having 2 factor authentication i.e. Password and biometric (local stored)
  - In Aadhaar, you cannot have local biometric storage and have to use RD Service XML block to verify biometric
  - Office at taluka requires using biometric verification but at the same time in the same system another model requiring OTP based. It will possible due to flexible model of eGovSSO
  - Fig. 5 shows block level various user logins in eGovSSO for e-dhara application.



[Fig. 5: Block level users for e-Dhara]

- Implementation of Dashboard for CM, Ministers and Secretaries
  - Create individual logins
  - Assign departments
  - When CM office approved authority logs in, he will get all departments details
  - For Revenue Minister, one gets individual department screen and comparative parameters
- Management freedom at individual department or section level such as Bank, ITI, etc. and ease of using it.

VI. Conclusion

This framework of single sign on and common master management provides ccoding freedom as well as time and cost saving while development of e-Governance applications. Starting of application development becomes easy by integration of eGovSSO for user management module and just start working on functionalities. Thus it gives tremendous features for eGovernance Implementation, Manageability, Accountability, Authentication and Authorization.

VII. Future Extension

Future work can be focused for registration of citizen and citizen authentication. Other functionalities can also included such as mass e-Mailing, mass SMS, SSO Gateway (Page base and Web service based authentication).

References

1. Stephen Lawton, “Secure Authentication With Single Sign-On (SSO) Solutions”, http://www.tomsitpro.com/articles/single-sign-on-solutions,2-853.html, Jan 6, 2015, Dt. 15/05/2017
2. Andreas Pashalidis and Chris J. Mitchell,"A Taxonomy of Single Sign-On Systems", Information security and privacy, Springer, 2003
3. Yang Jian, "An Improved Scheme of Single Sign-on Protocol", Fifth International Conference on Information Assurance and Security, IEEE, 2009, pp. 496-498
4. Jingquan Wang, Guilin Wang, and Willy Susilo, "Secure Single Sign-on Schemes Constructed from Nominative Signatures",12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp.620-627
5. Arun Khurana, “Single Sign-On (SSO) implementation using LDAP server”, http://www.webportalclub.com/2011/12/single-sign-on-sso-implementation-using.html, Dt.16/06/2018
6. "LDAP Integration", ONELOGIN WHITEPAPER, OneLogin, Inc., 855.426.7227
7. Alka Mishra, D.P.Misra, Narendrakumar Jain, Ravi Kumar, “oAuth Based Single Sign On”, Informatics, Vol 25 No.1 July 2016, pp. 36-38
8. “e-Pramaan: Framework for e-Authentication”, Department of Electronics and Information Technology, Government of India, October, 2012, Version: 1.0
9. "e-Government Program", SAUDI, https://www.yesser.gov.sa/EN/BuildingBlocks/Pages/The_Single_sign-on.aspx, Dt. 22/08/2018
10. “The Open Group”, Inroduction to Single Sign On, http://www.opengroup.org/security/sso/sso_intro.htm, Dt. 22/08/2018