International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Implementation of Single Sign on (SSO) for College websites

Nirmit Dagli[1], Mihir Deorukhar[2], Sarvesh Sawant[3], Kaushiki Upadhyaya[4], Nahid Shaikh[5]

[1,2,3]Student, Dept. of Information Technology, A P shah Institute of Technology, Thane (Maharashtra)-400615
[4,5] Professor, Dept. of Information Technology, A P shah Institute of Technology, Thane (Maharashtra)-400615

Abstract - *Consider a university education website need to provide different courses and tutorials to its students. But to include numerous resources and tutorials onto one education portal are often tedious and space constraint. Having multiple systems typically require multiple sign-on dialogues to access the resources. Users need to register on multiple portals to access the contents and courses and it involves the headache of remembering multiple sets of credentials. Users even have to present credentials multiple times they login to those portals/websites. With these scenarios, more the portals, the more sign-ins are required. It also requires to limit access to unauthorized users when log-ins are authenticated. If there are redundancy of resources and inconsistent information across multiple websites across the systems, users may show lack of interest. Single check in system is the proposed method to supply access to the educational learning resources/contents. In this approach just one set of credentials is required, user can access the multiple services with those same credentials since integrated into all systems. This approach provides a secure way to authenticate users and provides access to all or any services.*

***Key Words*: SSO, LDAP, Single Sign on, Active Directory, Single Credentials, API, Central Database, Single login, Security**

1. INTRODUCTION

Nowadays with the university data system increasing day by day, colleges aren't ready to share all information in one place instead they build different systems in sort of websites/portal to share this information. These systems play a crucial role within the university data system. The growing number of systems brings convenience for users, but also exposed a wide range of issues: Between the isolated systems, there is information redundancy and knowledge inconsistent, so it's difficult to maintain; Too many logs in points, each system has its own authentication mechanism. If a user wants to access some systems, he/she must go online several times, which brings inconvenience to the user. Users must to remember many usernames and passwords, it could result in forgetting password and cause password leading to security concern. Our single sign-on implementation mechanism is by using LDAP to function a personnel database, who personnel information between various systems. LDAP is brief for Lightweight Directory Access Protocol. LDAP server is employed to store and retrieve information, which is analogous to ordinary relational database. the most differences between LDAP servers and the general electronic database are as follows: LDAP using tree model instead of rational model to arrange information; Mainly provides data query services, the query speed faster than the standard relational database; Excellent ability to repeat the knowledge makes it highly robust. LDAP tree information organization model is similar to the particular hierarchical relationships between the various departments of a corporation. So, using LDAP to store personnel information made management easier. Single sign-on (SSO) may be a session and user authentication which gives user the way of *service that permits a user to use one set of logins* credentials (e.g., name and password) to access multiple applications. The service authenticates the top user for all *the applications the user has been given rights to and eliminates* further prompts when the user switches applications during an equivalent session. On the rear end, SSO is useful for logging user activities also as monitoring user accounts. Single sign-on reduces human error, a serious component of systems failure and is therefore highly desirable but difficult to implement. SSO avoids the monotonous task of confirming identity over and once again through passwords or other authentication systems. By increasing the users of the distributed systems that should often access to remote resource, different authentication techniques are needed when users want to enter the systems. Therefore, SSO technology has been introduced as a special sort of authentication mechanisms. This technology is supposed to facilitate the work for users during a way that with one credentials they might be able to access to many software resources on different servers.

1.1 LITERATURE REVIEW

[1]The growing number of systems brings convenience for users, but also exposed a wide range of issues: Between the isolated systems, there is information redundancy and information inconsistent, so it's difficult to maintain; Too many log in points, each system has its own authentication mechanism, If a user wants to access some systems, he/she must log on several times, which brings inconvenience to the user. Users must to remember many usernames and passwords, it could result in password fatigue and lead to password disclosure, so it has security risks. Single sign on is a good solution to these problems. The so-called single sign is that after a user logs on a system can logs on other systems which integrated into a single sign system without reauthentication. Our single sign-on implementation mechanisms: Using LDAP to establish a unified personnel

database, so that personnel information between various systems was unified and information redundancy were reduced. At the same time, it will provide authentication information for single sign-on. Establish single sign-on authentication service center and integrate all existing applications with the center.

[2] The several single sign-on schemes have been proposed. However, most of them have security flaws, and even worse, their improvements are also insecure against possible attacks. Thus, this paper aims to give an approach into the foremost recent SSO schemes, identifying their flaws, issues and challenges. The second aim of this paper is to formalize the Single Sign-On (SSO) and its security model to formally resolve the Issues identified. Also, an efficient and provably secure single sign-on authentication scheme without the identified drawbacks will be provided according to the formal model. It provides efficient and secure identification services with further security requirements for users in distributed systems and networks. In general, the identification services may require three factors, i.e., password, symmetric key and signature's characteristics. The authentication which is based on password is called password-based authentication. Password-based authentication together with another factor, symmetric key, is called two factor authentications. In which, a successful user authentication can be achieved if the user has a correct password together with a corresponding signature. The two-factor authentication consists all of these three factors, i.e., password, symmetric key and signature characteristics.

[3] Multi-database system is a complete global logical database which is composed by multiple database servers, and it can achieve data sharing and transparent accessing. In the multi-database system, the computer architecture, operating system, DBMS and so on, are heterogeneous, and each part has own authentication mode. The earliest theoretical research on the multi-database environment can be traced back to the seventy's in 21st Century. Institutions in foreign countries mainly are Almaden research center database group of the United States IBM company, Stanford University, TONA, etc. Foreign major database vendors have launched commercial products which support multi-database environment according to the forming theoretical system, including DB2, Sybase, etc. [1, 2, 3]. Technology developed the Paronama system based on the COBAR, etc. In order to improve the limitations of the traditional multi-database authentication model, we put forward a new identity authentication scheme of Single Sign On for multi-database, as they respectively describe the new authentication model and the authentication process. In the new scheme, we first introduce the concept of a multi-database coalition domain. A number of database systems trust each other, they have alliance relationship. Aiming at the access of the union domain in multi-database system, this paper designs a general and customizable SSO engine, in union domain system only need SSO to achieve a security access. It adopts distributed authentication mode, so it avoids single point failure and single point overload in centralized authentication mode

1.2 PROBLEM STATEMENT

To provide a service for accessing multiple platforms using single credential. By using LDAP, a single central database will maintain information of multiple accounts at the same time. Making Authorization process more Secure. Reducing the database chunk with one central database and to maintain security and monitor the user activity(log).

The solution for the above problems will be handled by the software, as we will be providing a separate module of validation where all the constraints will be checked for providing an optimal solution and all the constrains will be satisfied by our system. The proposed system will be used for SSO.

This ensures the following features:

- Sign-up Website
- API
- LDAP server
- Admin Access
- Android Application

2. EXISTING SYSTEM

Our college has various services for students/staff. For example, Moodle, IT Server, Internet Password, Hand Book, etc. Each student/staff has to maintain different Id's and Password for different services. For that college has to maintain different data servers. Admin has to maintain several data server and the user have to maintain several credentials to access different service and also have to login several times for Different accounts.

Here in the below figure, we have multiple accounts each account has their own database and servers. To access those accounts, we need different id and password

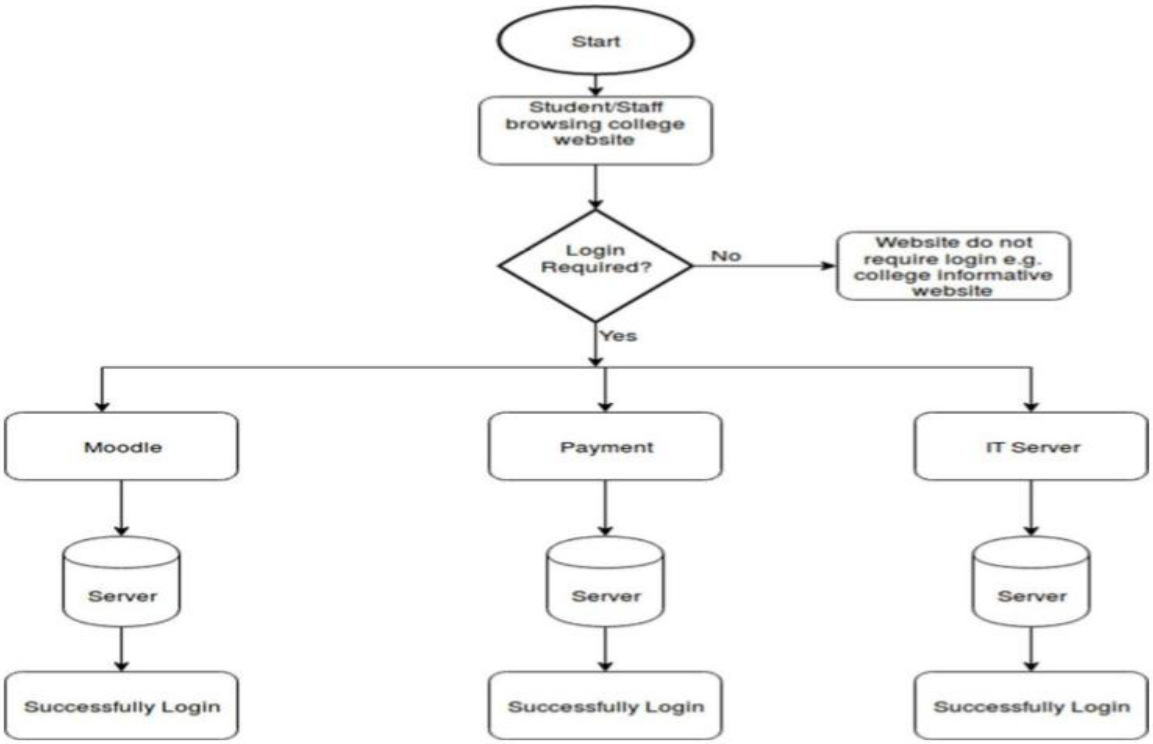

Fig -1: EXISITING SYSTEM

3. PROPOSED SYSTEM ARCHITECTURE

- User needs to register.
- User will be redirected to login page.
- User details will be stored in LDAP Server.
- Admin can also create user and maintain the user.
- Once the user will login to Single Sign On portal, the user will be able to access the websites which are integrated with the LDAP Server.

1) User will login to the college website/portal if they have an account. Otherwise if user wants to use SSO service he needs to sign up through the Registration page.

2) User will be redirected to the registration page where he/she will register for the SSO service to create his/her login credentials.

I. Student -Registration form includes username, personal details, email address, password.
II. Staff - Registration form include Username, password email ID, mobile number.
User can generate his own password or a default password will be provided.

3) Once registered the user will be redirected to the login page where he is required to enter his SSO login credentials. SSO system which can accept the parameter and validate it.

4) User information (student/staff) and password generated will be stored in LDAP server. To maintain security these passwords will be encrypted using hash value. LDAP will authenticate user credential via token which will be redirected using Single Sign-on website and host website. LDAP will work as central database and will maintain all the logs & Application. To ensure security we can provide multifactor authentication

4. METHODLOGY OF PROPOSED SYSTEM

Algorithm Design for SSO

A. Algorithm for users SSO:

1. Start.

2. Create an account using Users Registration page.

3. Once the Account is created you can login into all the website or android application that have integrated our API in their application.

4. In case of forget password or changing profile details you can Login in your account and go to update profile section.

5. Stop.

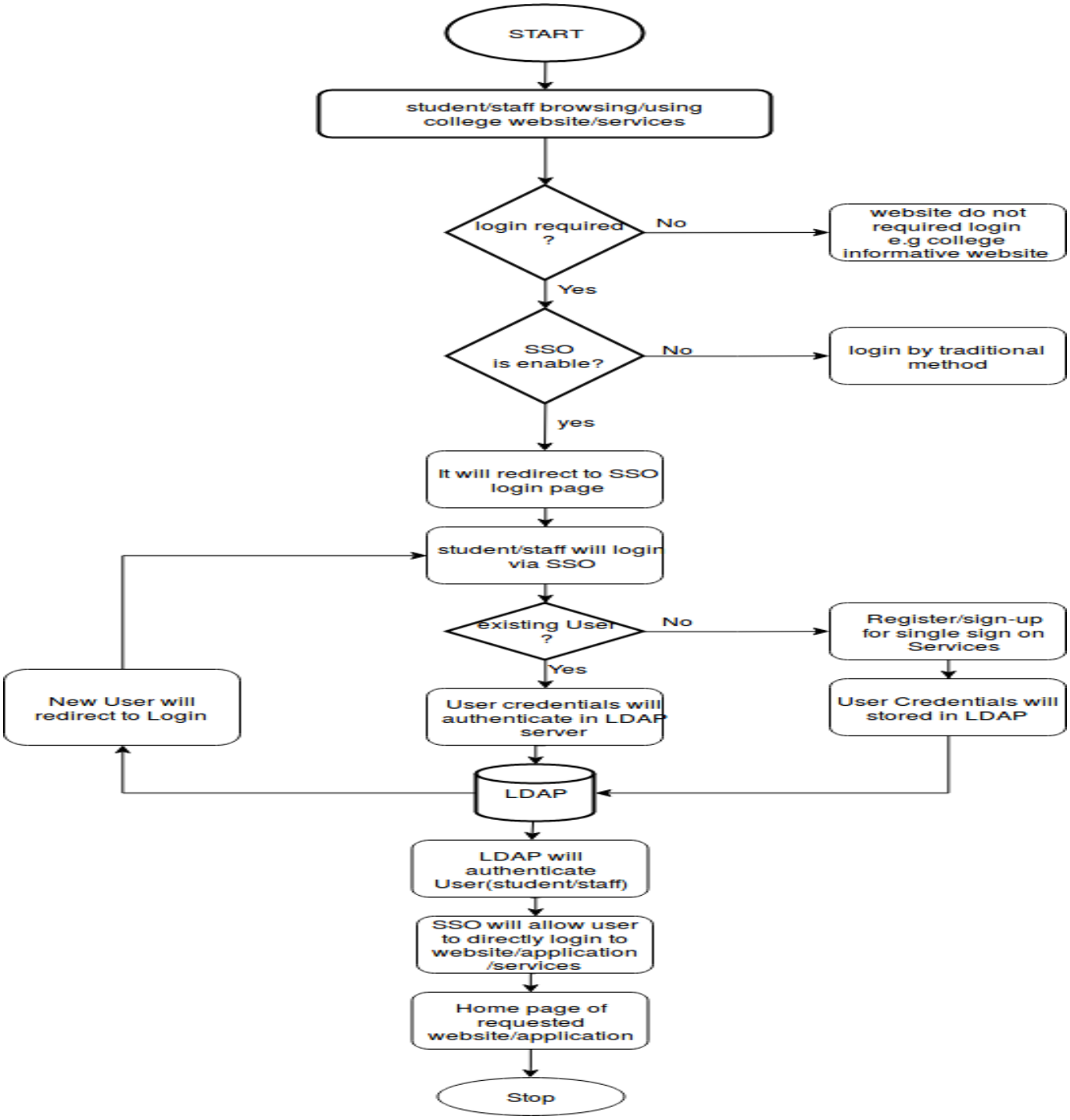

Fig -2: PROSPED SYSTEM

B. Algorithm for clients SSO:

1. Start.

2. Create an account using Website Registration page and obtain the API key.

3. Integrate the API with your application you can refer to the videos for integrating the API.

4. Stop.

The background technical aspects revolve Active Directory LDAP protocol where API which is built with java libraries act as a third-party connection between LDAP and website.

5. CONCLUSIONS

The Single Sign On System is developed with the aim of reducing the burden of the users of remembering different set of credentials for different websites, web application, mobile apps, etc. and also reduces the burden of login to applications again and again that is if they login into one website they are automatically logged into all other website.

By going through the previous surveys and IEEE papers, SSO system using LDAP was implemented. Single Sign on is used for multiple access for different applications and LDAP is used as Central Database. SSO eliminates the job of requiring different credentials for each application and rather uses single credentials for multiple applications. The password would be encrypted using hashing algorithm which will lessen the chances of the account being compromised

Future Scope for the System

• There can be profile picture of the user & tracking feature for the usage of the API.

• There can be appropriate documentation for the API usage.

• Single Sign out (Security Purpose).

ACKNOWLEDGEMENT

REFERENCES

[1] Application of single sign-on (SSO) in Digital campus Jian Hu, Qizhi Sun, Hongpin Chen College of Information Engineering, North China University of Technology, Beijing, China (IC-BNMT2010)

[2] SSO-Key Distribution Centre Based Implementation Using Serpent Encryption Algorithm for Distributed Network Ms. Durga Prasanna, Ms. Roopa S - 2015 IEEE International Advance Computing Conference (IACC)

[3] A New Identity Authentication System of single sign on for multiple databases. Lan Zhang Hongyun Ning, Yunyun Du, Yan-xia Cui

BIOGRAPHIES

Nirmit Dagli
Dept. of Information Technology
A.P Shah Institute of Technology
Thane (MH), India – 400 615

Mihir Deorukhar
Dept. of Information Technology
A.P Shah Institute of Technology Thane
(MH), India – 400 615

Sarvesh Sawant
Dept. of Information Technology
A.P Shah Institute of Technology Thane
(MH), India – 400 615