A Synopsis on

SINGLE SIGN ON

Submitted in partial fulfillment of the requirements
of the degree of

Bachelor of Engineering

in

Information Technology

by

Nirmit Dagli (16104013)
Sarvesh Sawant (17204013)
Mihir Deorukhkar (16104065)

Kaushiki Upadhyaya
Nahid Shaikh

Department of Branch Name
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI
2019-2020

CERTIFICATE

This is to certify that the project Synopsis entitled ***"SINGLE SIGN ON"*** Submitted by ***"Nirmit Dagli (16104013),Sarvesh Sawant (17204013),Mihir Deorukhkar (16104065)"*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology.***to the University of Mumbai,is a bonafide work carried out during academic year 2019-2020

Nahid Shaikh
Co-Guide

Kaushiki Upadhyaya
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane
Date:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

(Nirmit Dagli and 16104013)
(Sarvesh Sawant and 17204013)
(Mihir Deorukhkar and 16104065)

Date:

Abstract

Consider a college education portal needs to provide different courses and tutorials to its students. But to incorporate numerous resources and tutorials onto one education portal can be 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 also have to present credentials multiple times they login to these portals/websites. With these scenarios, more the portals, the more sign-ins are required. It also requires to restrict access to unauthorized users when log-ins are authenticated. If there are redundancy of resources and inconsistent information across multiple website across the systems, users may show lack of interest. Single sign on system is the proposed method to provide access to the educational learning resources/contents. In this approach only one set of credential is required, user can access the multiple services with those same credentials once integrated into all systems. This approach provides a secure way to authenticate users and give access to all services

Introduction

Our single sign-on implementation mechanism is by using LDAP to serve as a personnel database, who personnel information between various systems. LDAP is short for Lightweight Directory Access Protocol. LDAP server is used to store and retrieve information, which is similar to ordinary relational database. The main differences between LDAP servers and the general relational database are as follows: LDAP using tree model rather than rational model to organize information; Mainly provides data query services, the query speed faster than the ordinary relational database; Excellent ability to copy the information makes it highly robust. LDAP tree information organization model is similar to the actual hierarchical relationships between the various departments of an organization. So, using LDAP to store personnel information made management easier.

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications.The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session.

On the back end, SSO is helpful for logging user activities as well as monitoring user accounts. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable but difficult to implement. SSO avoids the monotonous task of confirming identity over and over again through passwords or other authentication systems

Objectives

To provide a service for accessing multiple platform 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.

To maintain security and monitor the user activity(log)

Literature Review

The papers referred are mentioned below:

[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)

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] 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)

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 possibleattacks. Thus, this paper aims to give an approach into the most 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 twofactor authentication. 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] A New Identity Authentication Scheme of Single Sign On for Multi-Database.Lan Zhang, Hongyun Ning, Yunyun Du, Yan-xia Cui

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 21 st 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 these forming theoretical system, including DB2,SyBase, etc[i , 2 , 3] . 4Technology 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.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

Problem Definition

In our college we have multiple services like Moodle, Payment Portal, HandBook, Webstore, IT Server, Internet Password,etc. To access them students need to remember various ID's and Password. To maintain these services different databases are use. To solve this problem we can use LDAP, in which student/staff will require just a single password to access multiple services.

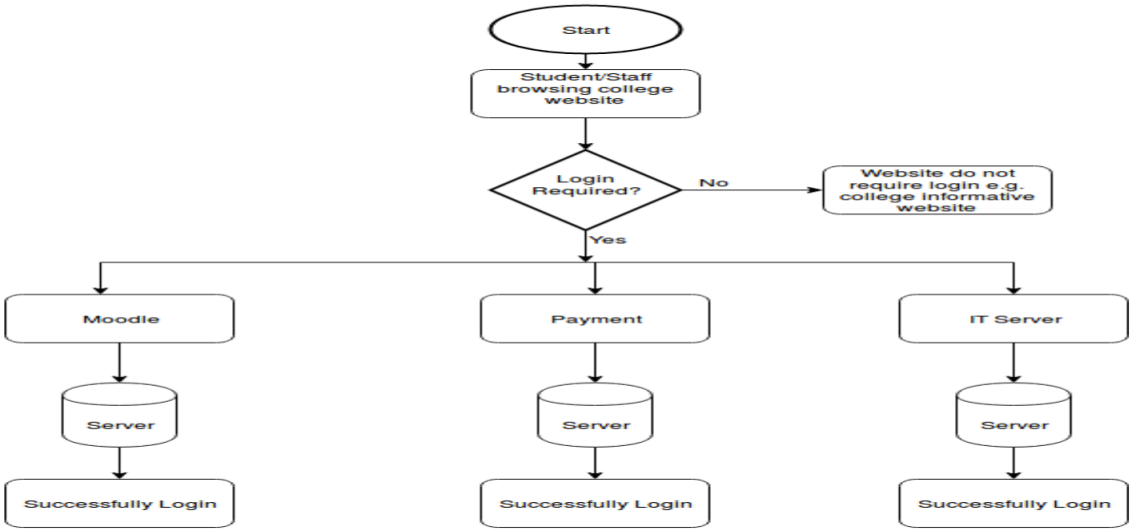

Figure 1: Existing System

Proposed System Architecture/Working

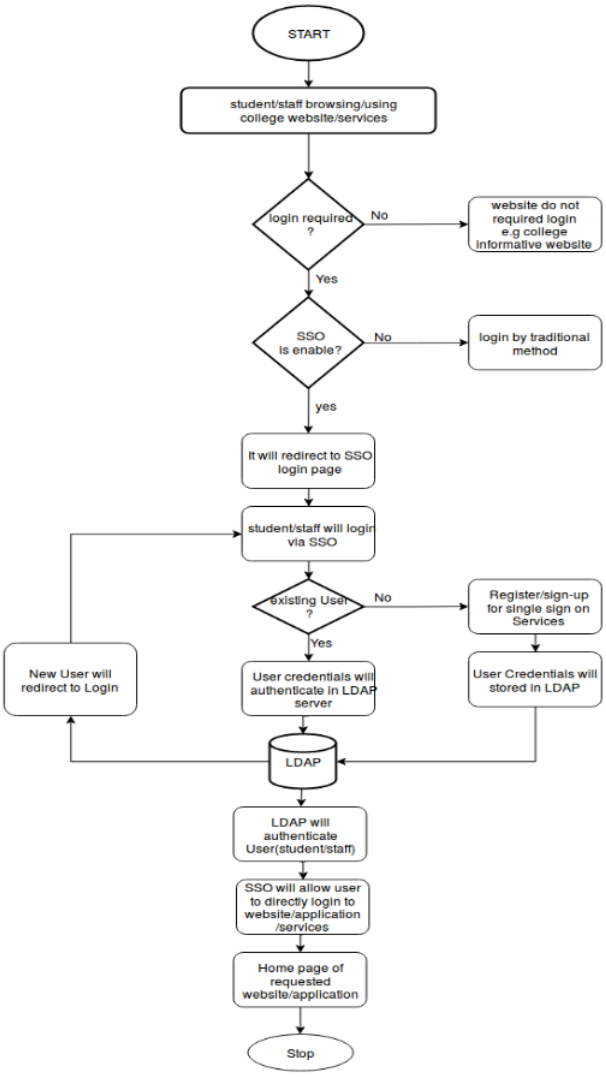

Figure 2: Proposed System

LDAP,the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

Design and Implementation

Register with Sign-on service:

In this service the user(student/staff) first need to register for the service. Registration form includes personal details, academical details(student/staff).Student details includes Department, Year, Student ID, academic details. Staff details include Department, Staff ID. Contact details include Email ID, Mobile Number, User can generate his own password.

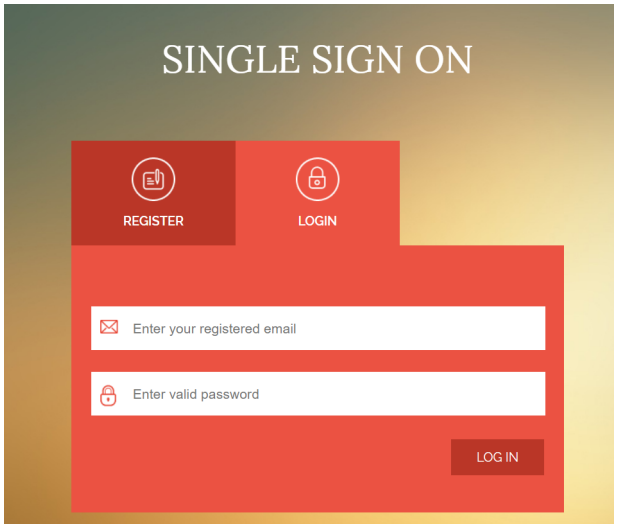

Figure 3: Register/Login

LDAP Server:

User information(student/staff) and password generated will be stored in LDAP server. To maintain security these password 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.

Applications/Service provided by institute:

Applications/Services can be accessed by single credentials.To ensure security we can provide multi-factor authentication.

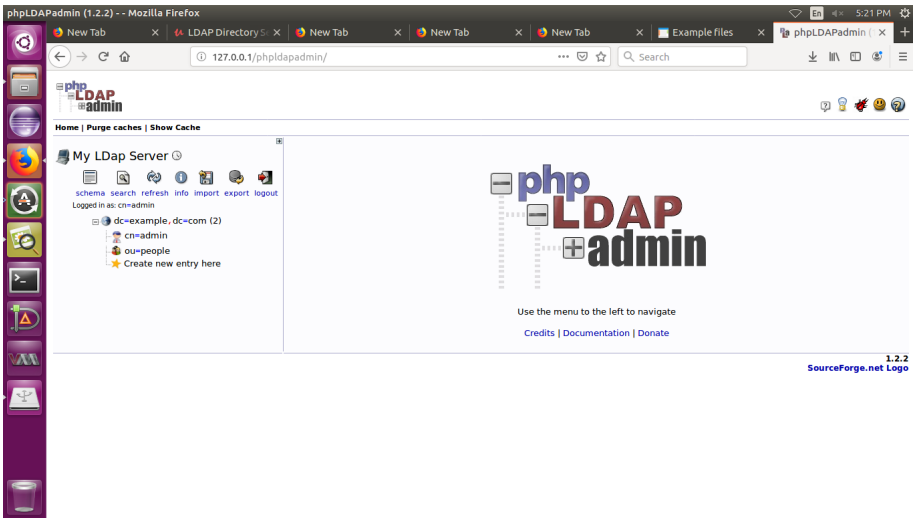

Figure 4: LDAP

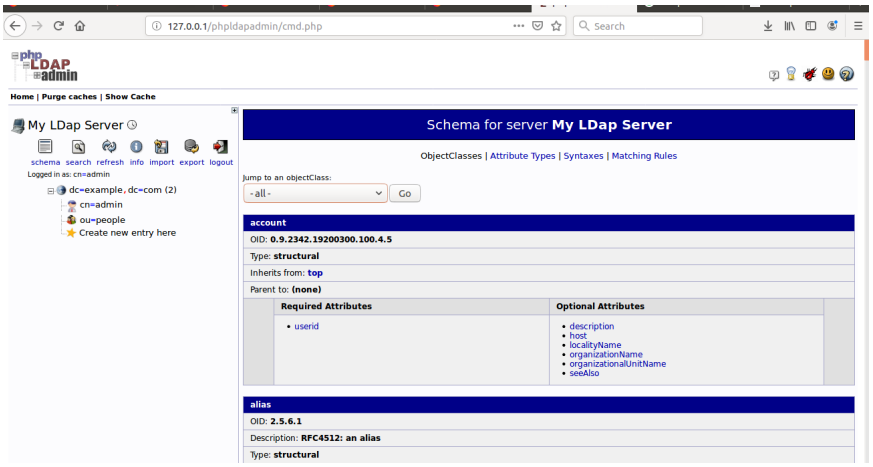

Figure 5: User Creation

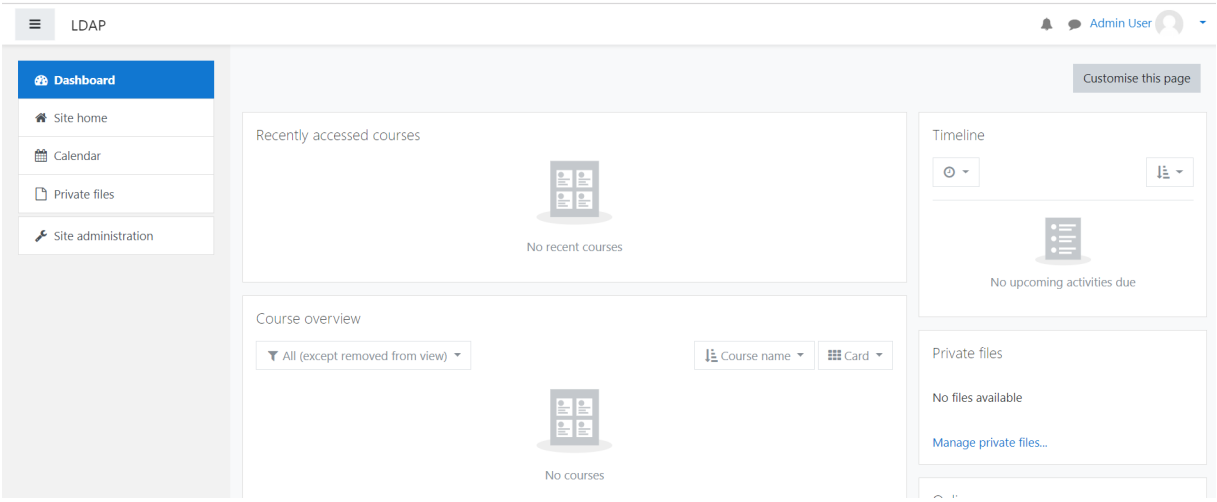

Figure 6: Moodle

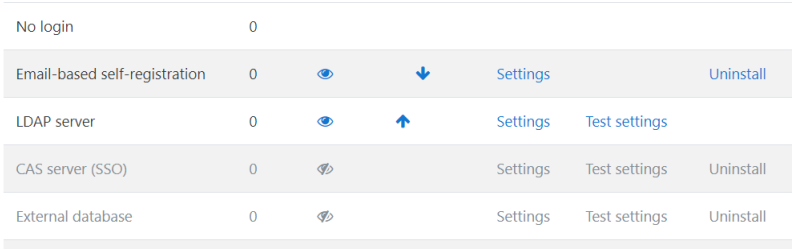

Figure 7: LDAP Enable

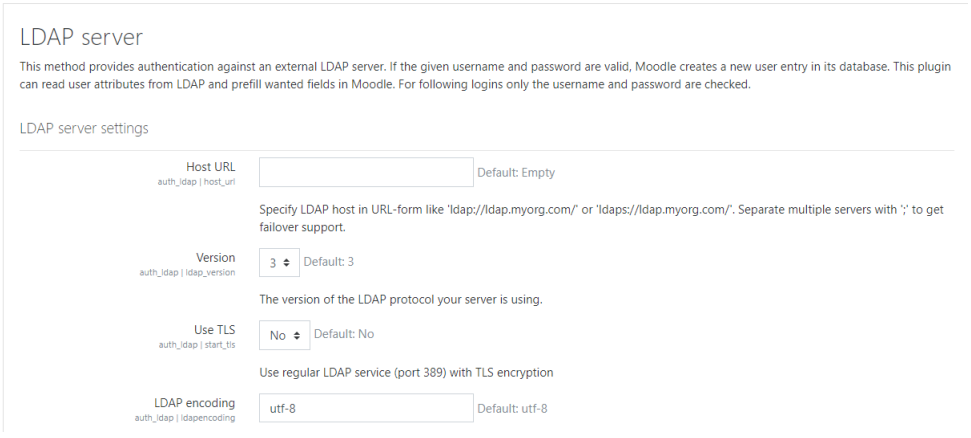

Figure 8: LDAP Configuration

Summary

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 form of authentication mechanisms. This technology is meant to facilitate the job for users in a way that with one credentials they could be able to access to several software resources on different servers.

References

[1] APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS Jian Hu,Qizhi Sun, Hongping Chen

[2] An Automated Enterprise IT Management System Based on LDAP

[3] OAuth-SSO: AFramework to Secure the OAuthbased SSO Servicefor Packaged Web Applications

[4] Moodle Server, https://cloudcone.com/docs/article/how-to-install-moodle-on-ubuntu-18-04/,

[5] LDAP Server, https://computingforgeeks.com/install-and-configure-openldap-phpldapadmin-on-ubuntu-18-04-lts/,

1 Publication

Paper entitled **"SINGLE SIGN ON"** is presented at **"IEEE Conference"** by **" Nirmit Dagli, Sarvesh Sawant,Mihir Deorukhkar".**