

Design And Implementation Of Enhanced Single Sign On System For Education Systems

Pranay B. Sahare

Scholar Student, M.Tech,
Dept of CSE, Nagpur Institute of Technology, Nagpur, MH, India

Abstract - Consider a college education portal needs to provide access to different domain courses and tutorials to it's students. But to incorporate numerous resources and tutorials onto one education portal can be tedious and space constraint.

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 indulge 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, when there are more security domains, the more sign-ins required. It also requires to restrict access to unauthorized users when log-ins are authenticated. If there are redundancy of resources across multiple websites, users may show lack of interest due to redundancy and authorization. headache. Single sign on system is the proposed method to provide access to the educational learning resources/contents. In this approach, one-time login is required and the logged in user can access the relevant authorized service provider's resources without need to login to their UI facing.

This approach provides a secure way to authenticate users by the unique hash password validation and time stamp validation. If both the validation are performed, the requesting user will be provided access to other website resources as well where the user's authorization is done with the valid token and access key.

Hence, the other websites can share common resources across multiple domains without the technology barrier.

Key Words: Resources, authorization, token, service provider, portal, session, affiliate

1. INTRODUCTION

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.

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 time authentication they could be able to access to several software resources on different servers.

2. AUTHENTICATION PROCESS

1. The first step is logging into the main service (Facebook or Google, for instance).
2. When you visit a new service, it redirects you to the original (or parent) service to check if you are logged in at that one.
3. An OTP (One-time password) token is returned.
4. The OTP token is then verified by the new service from the parent's servers, and only after successful verification is the user granted entry.

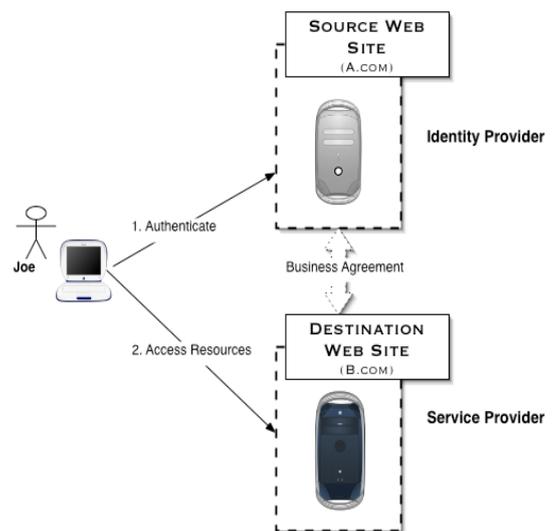


Fig: Basic process diagram

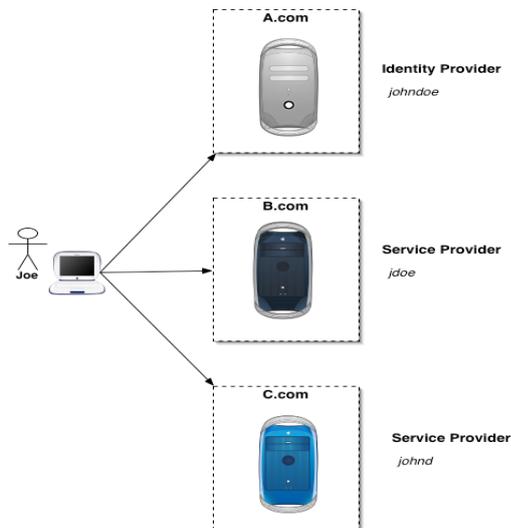


Fig. Federated Identity

3. RELATED WORK

1. Kirti Bhandari, Parminder Kaur, "Implementation of Single Sign-On Technique in Heterogeneous Distributed Environment", Volume 4, Issue 3, March 2014

In this paper they have implemented the Single Sign-On Scenario in Distributed Heterogeneous Environment. They proposed research that most distributed systems are assembled from different components. Each of the component acts as an isolated security domain independently. In the multi sign-on environment, the end-user who wants to use services housed in different servers has to sign-on multiple times. User has to remember large numbers of passwords. With multiple sign on, user may have some bad habits that reduce the system security, such as, using the same password for all the systems. Therefore, multiple sign-on is very troublesome, so the single sign-on solution has been introduced to solve this problem.

2. Daniel Kouřil, Luděk Matyska, Michal Procházka, "Multi-mechanism Single Sign-On in Grids" Masaryk University, Botanická, Czech Republic.

Being based on one of the mechanisms, most grid environments today provide strong authentication protocols, however, they are usually bound with only one, in most cases based on public key infrastructure (PKI). Such an arrangement works pretty well, but unnecessarily limits users since they are required to use only the one mechanism, which may not be flexible or convenient. A better solution would be to offer users a freedom to choose their own authentication mechanism—provided it is strong enough—and provide automatic translations that guarantee that all services and components are securely available regardless of the choice of authentication mechanism. This technical report surveys several authentication mechanisms that are used in contemporary grid and other distributed systems

and also discusses possible transitions to translate credentials. The report summarizes recent results in this area, many of which have been achieved by the authors.

3. Gguilin Wang, "Security analysis of a single sign-on mechanism for distributed computer networks", Industrial informatics, iee transactions on (volume:9, issue: 1) Feb. 2013.

Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, Wang demonstrate that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, he present two impersonation attacks. They proposed an improvement for repairing the Chang-Lee scheme.

4. V.Priya, M.E, A. Rajeswari, J. Nithya, P. Shrivithya, "A Secure Single Sign-On Mechanism for Distributed Computer Networks", (IJETCSE) Volume 7 Issue 1 –MARCH 2014

In this paper, however, we describe that their scheme is actually insecure as it fail to meet credential privacy and soundness of authentication. Specifically, we represent two impersonation severities. The first attack allows a malicious service provider, who has easily communicated with a legal user twice, to resume the user's credential and then to impersonate the user to deal with the resources and services offered by other service providers. In next attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. Here, they identify the flaws in their security arguments to explain why attacks are possible against their SSU scheme. Our attacks also apply to another SSU scheme proposed by Hsu and Chuang, which has inspired the design of the Chang-Lee scheme.

5. In 2007, Maryam *et al* demonstrates a centralized password-based authentication system using SSO for Web-based application in distributed environments. Centralised, Distributed and Federated Approaches are introduced and Cookie capabilities are used for implementation of this system that is called centralized cookie-based SSO or CC-SSO. In 2009, Magyari *et al* proposed a single sign-on mechanism which is based on certificates generated on request for client applications.

4. PROPOSED APPROACH

Single sign on system is the proposed method to provide access to the educational learning resources/contents. In this approach, one-time login is required and the logged in user can access the relevant authorized service provider's resources without need to login to their UI facing.

This approach provides a secure way to authenticate users by the unique hash password validation and time stamp validation. If both the validation are performed, the requesting user will be provided access to other website

resources as well where the user's authorization is done with the valid token and access key. Hence, the other websites can share common resources across multiple domains without the technology barrier.

This approach can be applied in distributed environment as well with few customization.

5. METHODOLOGY

A) User Registration Process

User / Institute need to register onto the Web portal before they can start sharing their resources with the other portals or website users. This will be the first time registration. After registration they will be provided with the valid unique access key that they can use to allow users to directly login to their website without login credentials. That means when any user tries to access the other websites content, that website can check it's access key generated by the SSO service and authenticate it.

B) Setup web service to authenticate client request

This service will allow a website to validate the requesting user's identity and authenticate it with the valid token and access key. If it is valid then the requesting user will be given access to the website resources. This web service generates token and access key each time for new registered user.

6. MODULES FOR PROPOSED SYSTEM

Scope of the system can be fixed by the modules divided in the project.

A) Design the Graphical User Interface (GUI) and database

First have to design a graphic user interface and database for proposed system, where all aspects and functionality is covered in this module a user-friendly GUI and Database can be created. We use MySQL for database and PHP and other web technology for GUI. This Includes College Website Login, Home Portal and Registered Institutes / portals links.

B) Login Process

Login process includes College Website Login form which will redirect the user to Home Screen where they can see the SSO links to navigate to the different registered portals.

C) Web Service

Web service is required to redirect authenticated SSO users to the registered portals to access

the resources. This will be a restful API that will tell other hosts that the user trying to access the resources is a valid user and allow to login without credentials.

D) One Time Log out

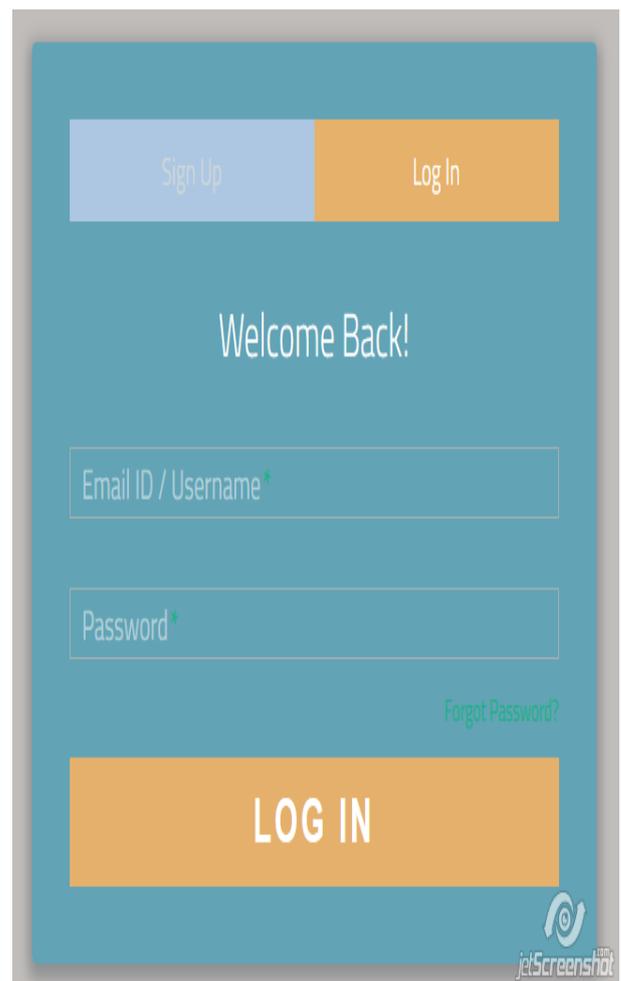
This module will allow to sign out the sessions completely from all the portals even if user logs out from any of the portal. This is an advantage of the SSO technique.

F) User Authentication

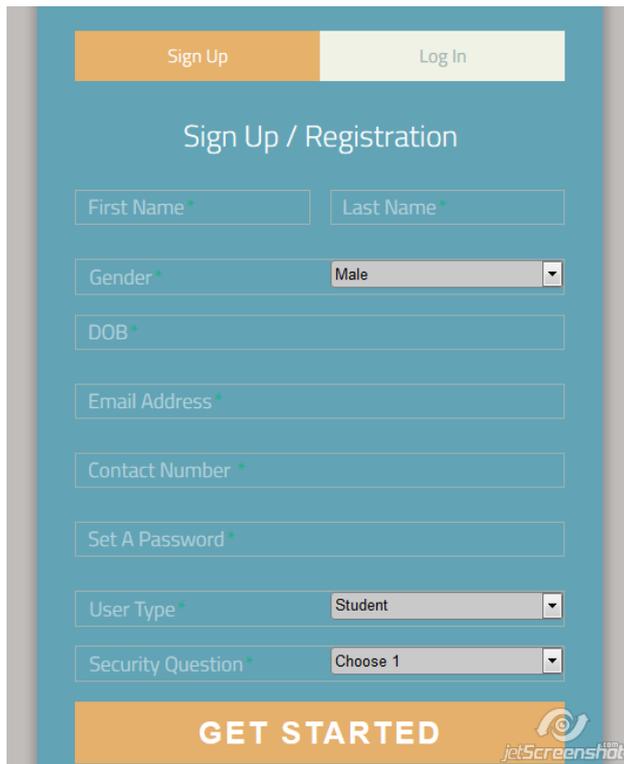
User Authentication via Hash Password and optionally face recognition technique for the first time login to the main website comes under this module.

7. IMPLEMENTATION

- a) User will login to the college website/portal if have an account. If user doesn't have an account he needs to sign up through the **Registration page**.



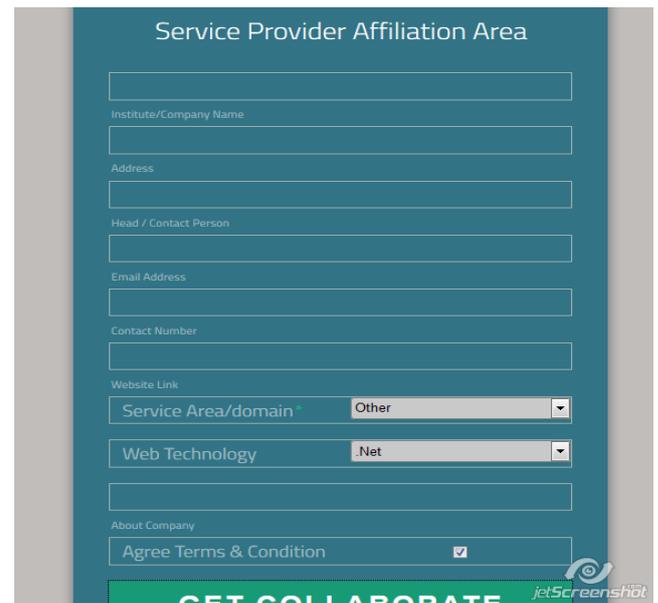
A) Login Form



B) Sign-up Form

C)

- b) After login user will see the dashboard. On content area there will be Affiliated/collaborated institute/website links.

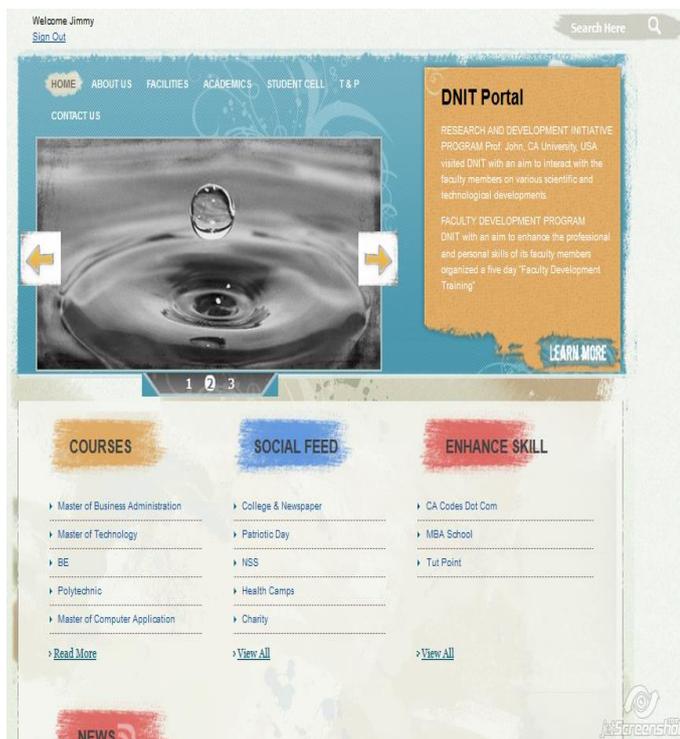


A) Company Affiliation Form

- f) If a user directly goes to the Service provider website and he doesn't have an account there, SP will popup a login page for SSO system.
- g) User have to provide login credentials that he created on college portal and the SSO system will authenticate it from the database and provide access to user of the SP website.
- h) If a user login to SP website and goes to college website, it's session is validated to provide direct access to dashboard in this instance.
- i) Another point to note - user and SP will have a common shared secret key that they both will use to generate access key and validation purpose. Only SSO module will know this shared secret to authenticate the requests.

8. CONCLUSIONS

The Proposed Single Sign On System provides access to resources on different websites/portals from the institute website. Only authenticated users/students can access the resources and study materials.



A) College Portal Dashboard

Single Sign On is now a standard to exchanges and share resources across users of different domain using standard protocols and authentication technique. It eliminates the job of providing authorization on each application instance.

It also includes high level security for user credentials. Hash Password authentication and tokens based on time duration are used to manage the SSO process. It can accommodate large bandwidth of users. The technique can be implemented without technology barrier.

ACKNOWLEDGEMENT

We would like to express our appreciation to our parents and all the lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

- [1] Kirti Bhandari, Parminder Kaur, "Implementation of Single Sign-On Technique in Heterogeneous Distributed Environment", Volume 4, Issue 3, March 2014
- [2] In 2004, Gang *et al* [2] proposed two designs of Single Sign-On and discuss its advantages and disadvantage of these two versions.
- [3] In 2007, Maryam [6] *et al* demonstrates a centralized password-based authentication system using SSO for Web-based application in distributed environments. Centralised, Distributed and Federated Approaches are introduced and Cookie capabilities are used for implementation of this system that is called centralized cookie-based SSO or CC-SSO.
- [4] In 2009, Magyari *et al* [5] proposed a single sign-on mechanism which is based on certificates generated on request for client applications.
- [5] In 2010, Moo Nam Ko *et al* [7] discussed Facebook Connect services which allow users to login to other websites using their Facebook identity and information and which will then potentially feed back to a users Facebook network information about their actions on the site. Facebook Platform allows users to import their identity, profile, privacy policy, social graph and content from Facebook to third-party sites.
- [6] Daniel Kouřil, Luděk Matyska, Michal Procházka, "Multi-mechanism Single Sign-On in Grids" Masaryk University, Botanická, Czech Republic.
- [7] Gguilin Wang, " Security analysis of a single sign-on mechanism for distributed computer networks", Industrial informatics, iee transactions on (volume:9 , issue: 1) Feb. 2013.
- [8] Arul Princy. A, Vairachilai.S, "A Survey on Single Sign-On Mechanism for Multiple Service Authentications", IJCSMC, Vol. 2, Issue. 12, December 2013, pg.40 - 44.
- [9] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. of CRYPTO', 1993, pp. 232-249.
- [10] T.S. Wu, C.L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed

computer networks", Computers and Security 23 (2) (2004) 120-125.

[11] V.Priya,M.E, A.Rajeswari,J.Nithya,P.Shrivithya, "A Secure Single Sign-On Mechanism for Distributed Computer Networks", (IJETCSE) Volume 7 Issue 1 -MARCH 2014

BIOGRAPHY



Pranay B. Sahare
MTech CSE Student
NIT, Nagpur
Email: pranay.bbt@gmail.com