Abstract:
Single Sign on (SSO) protocols are today integrated in millions of web services so end users can authenticate to a third-party identity provider (IdP) to access multiple services. The proposed system allows other websites to retrieve the personal information about user from our website as per the requirement. On the backend single sign-on is helpful for logging user activities as well as monitoring user accounts. In web SSO service agent module on the application server retrieves the specific authentication credentials for an individual user from a dedicated SSO server.

Keywords: Identity Provider, Service Provider

1. INTRODUCTION
Web services need to verify the identity of their users to guarantee user security and privacy, or offer a personalized user experience. Web users have traditionally had to replicate the same personal data (e.g. name, address, bank account, telephone number, etc.) to create their user accounts. Such site-centric identity management forces users to replicate their identities all over the web and to authenticate to services, each with their own credentials, and one after the other.

The well-known Single Sign-On (SSO) approach permits users to log in once and to access multiple services by delegating user authentication from service providers to authentication services. Service providers and authentication services form identity federations that enable importing identity information from one domain to another. The advantage of the single sign on model is the central authentication server that authenticates users. The central database maintains and manages the user's identity information.

2. LITERATURE REVIEW
In recent years a lot of work has been done in the field of “Single sign on” by number of researchers.

1. Xin-e YOU, Yan ZHU, in paper [1] make a comprehensive introduction to popular Single Sign-On model currently. Single Sign-On solution designed in the thesis is efficient, safe, easy to implement, and has the application and promotion of value in Information integration of enterprises.

2. Authors of Paper [2] have provided an assertion-driven analysis of web SSO protocols to help developers assessing the nature of the flows and data items of these protocols. The article highlights the importance for service developers to be aware of the user resources involved in SSO login events and how these resources may be compromised. The article aims to bring out the need for further improvements in user privacy in SSO on the web.

3. In paper [3] authors have stated how identity management systems store attributes associated with users and employ these attributes to facilitate authorization. Single sign on systems issue authentication assertions to multiple service providers after a single user authentication.

3. PROBLEM STATEMENT
To develop single identity provider to authenticate users belonging to different accounts on different servers as well as to create a more efficient and streamlined work environment.

4. PROPOSED SYSTEM
When an user attempts to access an application from the service provider, the service provider will send a request to the identity provider for authentication. The service provider will then verify the authentication and log the user in.

4.1 OUTLINE
1. Registration: All the users have to register on the main website.
2. Authentication: Our website will provide easy authentication facility to other web applications.
3. Transfer of user information: Main website will transfer the user information as per the requirement of the requesting website.
4. Parallel changes: If user made changes in the information on the main website, those changes will be reflected on all websites that are linked with main website portal.

4.2 SYSTEM ARCHITECTURE/BLOCK DIAGRAM

Figure 1. System Architecture of Single Sign On
5. WORKING

5.1 METHODOLOGY
We are using RSA algorithm to provide security for data that will be transferred from the identity provider to the service provider after successful authentication.

5.1.1 ALGORITHM
RSA ALGORITHM
A. Key Generation Algorithm
Step 1: Randomly and secretly choose two large primes: p, q and compute n = p × q
Step 2: Compute \( \phi(n) = (p - 1) \times (q - 1) \)
Step 3: Select Random Integer: e such as 1 < e < n and \( \gcd(e, \phi) = 1 \)
Step 4: Compute d such as \( e \times d \equiv 1 \mod \phi(n) \) and \( 1 < d < \phi(n) \)
Step 5: Public Key: (e, n)
Step 6: Private Key: (d, n).

B. Encryption process
Step 1: Suppose entity R needs to send message m to entity S (represent m as an integer in the range of 0 < m < n).
Step 2: Entity S should send his public key to entity R.
Step 3: Entity R will encrypt m as \( c = m^e \mod n \) and will send c to entity S.

C. Decryption Process
Step 1: Entity S will decrypt the received message as \( m = c^d \mod n \).
The most important advantage of RSA is ensuring about the privacy of the private key because this key will not be transmitted or revealed to another user.

5.2 IMPLEMENTATION

5.2.1 MODULE 1: REGISTRATION
1. To create a web based interface to accept information from user using HTML5, CSS3, PHP, etc.
2. To validate that entered information for selected criteria.
3. After validation accepted information will be inserted into the database.

5.2.2 MODULE 2: AUTHENTICATION
1. The first step is to accept an API call from other websites asking for the correctness of username and password.
2. Check these credentials in the database of main website.
3. If the credentials are correct, pass the details to requested website and start the session for the respective user.
4. Otherwise pass the error message to respective website.

5.2.3 MODULE 3: TRANSFER OF USER INFORMATION
1. First accept the different parameters which are required.
2. Then check for the appropriate fields in identity provider.
3. If the fields are matched then transfer the information.
Otherwise pass the error message to respective website.

6. ASSUMPTIONS
1. Adequate internet speed.
2. Compatibility with different registration fields across all websites.

7. ADVANTAGES
1. No need to fill the same registration form again and again.
2. Unique username and password for all accounts.

8. LIMITATIONS
1. The main site that is the identity provider must be very secure.
2. High speed internet requirement.

9. CONCLUSION
Thus, in proposed system we are using a set of techniques that will allow users to access multiple services of any domain by signing in only once. This will drastically reduce the time spent on log in actions as well as security complexity related to sign on operations.

10. REFERENCES
PAPERS

WEB LINKS
[5]. www.onelogin.com/product/sso
[6]. www.phpreferencebook.com