# SINGLE SIGN OFF RESOLVING PRIVACY ISSUE

**Aksshita Gupta[1], Avnish Singh Jat[2]**

[1,2]*Manipal University, Jaipur, Jaypee Institute of Information Technology*

## ABSTRACT

*Today almost every website requires user to register and sign in to access the full contents of the website or just security issues in cases where payments are made. To ease the process users are also provided the option to login via their Google or Facebook accounts. This is known as Single Sign On. The main thrust of this paper is to analyze the privacy issues concerned with single sign on which renders single sign off irrelevant but why it is also required to protect our privacy.*

***Keywords: Single Sign Off; Single Login; Privacy; Security; Website Survey;***

## I. INTRODUCTION

Many of us considered the security as their top priority, but are we really secure in every sense? The answer is big "NO", life is unpredictable anything can happen on the very next time. But we can fill some of the loopholes with regards to web security. With the help of this paper we have pointed out one of the loopholes in web security and implemented the possible solution for this problem.

Most websites make use of single sign on, but there is no system of single sign off that means your user data is still lurking on the third party website even if you have signed out of your Google/Facebook account. We have proposed an solution by giving alert to the user that his Google or Facebook account is still accessible

## II. BACKGROUND

Single Sign-On or SSO refers to access of multiple software systems via a single login entity.

It means a user logs in with a single login ID and password to gain access to many connected systems without having to use their login credentials again and again.

The system uses Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on directory servers.

A less complicated version of single sign on can be achieved over IP networks using cookies but only if the sites share a same parent domain.

SSO is strictly used for authentication of identity. It establishes the authenticity of identity and shares the data with other connected systems that require this data.

### 2.1 Usage

Suppose we access two websites A and B. We login with the given credentials at site A but we want that we are simultaneously logged in at B. We can share session information across domains, but for security reasons web browsers do not allow other domains to access other domain's cookies. This is when SSO comes into play.

Although there are different methods to implement SSO, their basic concept is to send data to a central domain where identity is authenticated and then the session is shared with other domains via the implemented protocol.

So now if a user accesses website B, when he has already logged in at A, he will be taken to the authentication domain of B where the central domain will send the necessary data and secure login at B is complete without the user having to enter his details again.

Categories of SSO:

1. Password Synchronization
2. Enterprise SSO
3. Web SSO
4. True SSO
5. Federation

## 2.2 Benefits

- Access to user data is not given to any third party site using SSO.That is user passwords are not stored externally.
- Reduced password fatigue as there will still be availability of many user-password combinations.
- Time spent in re-entering passwords for same identity is reduced.
- Reduced IT costs due to lesser password issues.
- Websites using Security Assertion Mark-up Language (SAML), provide an extra layer of security when used with SSO.
- In case of leakage of data or cases of hacking, which specific accounts were breached and by whom can be easily tracked and also a trail can be made as to how the breach was used.

## 2.3 Possible Vulnerabilities

- Reduced sign-on is used to reflect that SSO is impractical as a standalone method to address the need for different levels of secure access in enterprise and requires more than one authentication server and application synchronization as well.
- SSO provides access to many resources once a user is initially logged in. Hence if the details were available to some other person it could create a serious negative impact and misuse.
- SSO relies heavily on its one authentication system and database. If the system were to fail, access would be denied to multiple systems connected under that SSO system. System Failures can be fatal in cases where sign in must be guaranteed at all times such as security systems.
- It also renders third party applications useless in places where social networking sites are blocked or the data is censored such as Offices, libraries, workplaces etc.

### Single Sign Off

Single sign off means to logging out simultaneously from Identity Service Provider and relaying party at the same time. Currently, something remotely similar to single sign off, where the user is logged out of all accounts is only by clearing the cache data and cookies of the web browser.

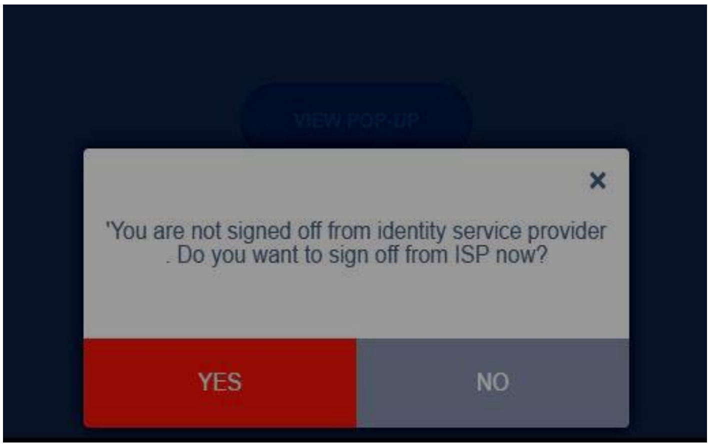
## III. PROPOSED WORK

When a user clicks on “Logout” on the main identity provider page, a single sign off detail page opens up. It lists the sites where the user has logged in via the said email-id or account. A confirmation is asked as to whether a user wants to logout of all the websites. On clicking of OK, if the sign-off is successful a tick (check mark) is placed in front of all the websites using the sign in feature via that website. And the user is again redirected to the homepage of the said website. If the sign-off is unsuccessful, the user is asked to try again.

An example of Java Script code in this case would be:

```
<script>
If(window.confirm(‘))
{//Redirect to ISP if clicked yes
// Page with list of applications using details is displayed
{if(window.confirm(‘))
{// If yes,intiate sign-off and after completion redirect to page
}
Else
{ //ask user to try again
}
}
Else {
//Redirect to homepage if clicked No.
}
</script>
```

The output of above code is given below:



'You are not signed off from identity service provider
. Do you want to sign off from ISP now?

Single Sign Off is really a big issue as far as web security is concerned; flipkart and many other websites have stopped the use of SSO. The need of the hour is to identify the problems related to it and try to achieve a secure SSO system.

## IV. FUTURE WORK

We have worked on an issue related to single sign off, but the mystery of its full proof solution is still unresolved. We will now test this work on some of the websites that have this issue and will work on a cure which can eradicate this problem.

## V. ACKNOWLEDGMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. Especially, please allow us to dedicate our acknowledgment of gratitude towards Mr Avnish Singh Jat for his support and encouragement.

## REFERENCES

[1] Jat, Avnish Singh, Menlam Choden, and Kinley Dorji. "Single Sign off Issue: A Possible Threat to our Privacy." (2016).

[2] Vaibhav Rastogi and Ankit Agrawal, ""All Your Google and Facebook Logins are Belong to Us: A Case for Single Sign-off,"IEEE, 2015.

[3] Delignat-Lavaud, K. Bhargavan, and S. Maffeis, "Language-based defenses against untrusted browser origins." in Usenix Security. Citeseer,2013.

[4] Y. Cao, Y. Shoshitaishvili, K. Borgolte, C. Kruegel, G. Vigna, and Y. Chen, "Protecting web-based single sign-on protocols against relying party impersonation attacks through a dedicated bi-directional authenticated secure channel," in Research in Attacks, Intrusions and Defenses. Springer, 2014.

[5] "The Moz Top 500", https://moz.com/top500.