Survey on Security Framework for Single Sign On in cloud for SaaS application

[1]Punit Teraiya,[2]Mr. Girish Khilari
[1]IT Systems & Network Security,
[1]Gujarat Technological University, Ahmedabad, India

Abstract **- Single Sign on in cloud eliminates to sign in again and again unlike simple cloud. So it demands more and more now a days not only for multinational companies but it is also being used by small and medium enterprises. As single sign on maintains user's credentials centrally the security must be provided to secure credentials. As with increasing use of single sign on the attacks are also increasing like identity theft, replay attack, DOS attack. So this paper proposes a security framework for single sign on in cloud to prevent them against security attacks.**

IndexTerms **- Single Sign On, DDOS attack**

I. INTRODUCTION [3][4]

Single sign-on (SSO) is a session /user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

SSO is not suited for systems requiring guaranteed access, as the loss of log-in credentials results into denial of access to all systems. Ideally, SSO is used with other authentication techniques, such as smart cards and one-time password tokens.

II. ADVANTAGE

- Eliminates credential reauthentication and help desk requests; thus, improving productivity.
- Streamlines local and remote application and desktop workflow.
- Minimizes phishing.
- Improves compliance through a centralized database.
- Provides detailed user access reporting.

III. DDOS ATTACK

It is one type of attack which makes resource unavailable to the users by making many requests to that users.

Relation between DDOS attack and Single Sign On

In Single Sign On , if attacker makes multiple requests to the single sign on server which grants request to access multiple services then that server is unavailable to those users and not able to access the services. So as we know in Single Sign on , credentials are centrally maintained so if DDOS attack occurs then whole applications or services will unavailable to the users.

IV. SINGLE SIGN ON PROCESS

- The first step is logging into the main service (Facebook or Google, for instance).
- 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.
- An OTP (One-time password) token is returned.
- 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.

V. EXISTING SYSTEMS FOR SINGLE SIGN ON

1. Single Sign on for Cloud[1]

In this system the Single Sign on is done using trusted third party. Trusted third party check the authentication of the user.

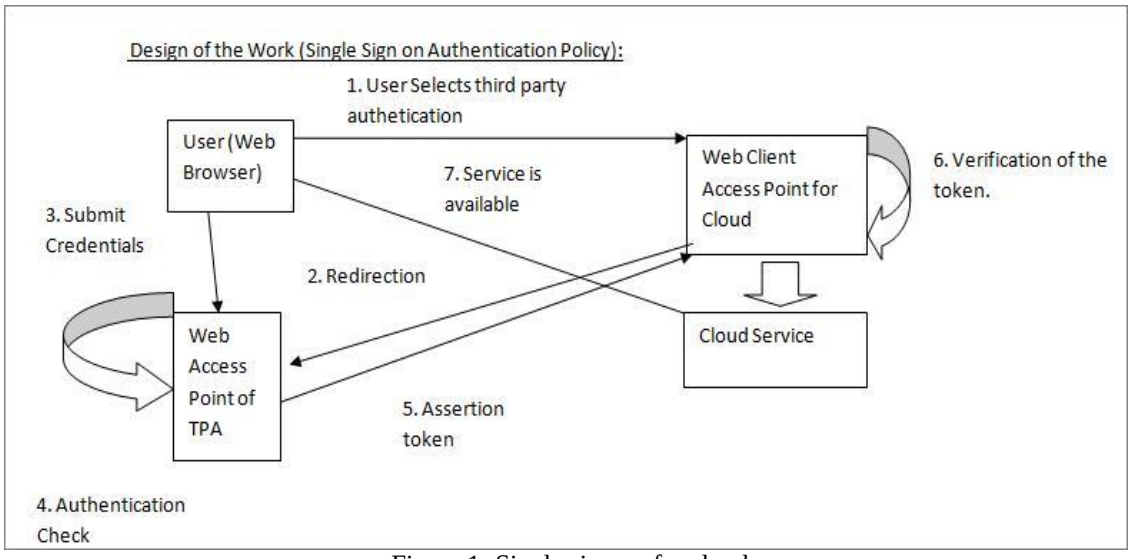

Figure 1- Single sign on for cloud

Algorithm

- A user interface will be shown that which has the option of creating and managing the virtual machines. Create a simple cloud portal which acts as service provider.
- User comes to portal login page and there is an option of sign in with the trusted identity provider.
- Based on the available standards the identity provider implements any one of the standards for authentication of the users.
- As and when user clicks the identity provider the identity provider site will be opened to enter the user credentials.
- User enters the user name and password, the credentials are verified and the site will redirect to the user interface which is shown at step 1.
- Maintain the database for audit of the user (user operations) so that the accountability also can be shown.

The cloud service is available to the user.

2. Single Sign on using two different servers.[2]

In this system there are two servers used for single sign on process. one is for password storage and second is for keys storage.

Algorithm

A. Storing Usernames and Passwords

1. User installs PMA as an extension in his browser.
2. By using PMA and singing on to this extension, user can access to SSOSA for storing his various usernames and passwords.
3. SSOSA generates keys according to AES-256 and encrypts given usernames and passwords.
4. After the encryption process, encrypted data are stored on PCS and keys are stored on KCS.

B. Accessing to Various SaaS Applications

1. User accesses to SSOSA by signing on PMA.
2. User requests to access on a specific cloud-based SaaS application from SSOSA.
3. SSOSA gets encrypted username and password from PCS and related keys from KCS.
4. Username and password are decrypted and sent to the requested SaaS application for signing on process.
5. After confirmation process, data are transferred from the SaaS application to SSOCS and after that transferred to the user browser.

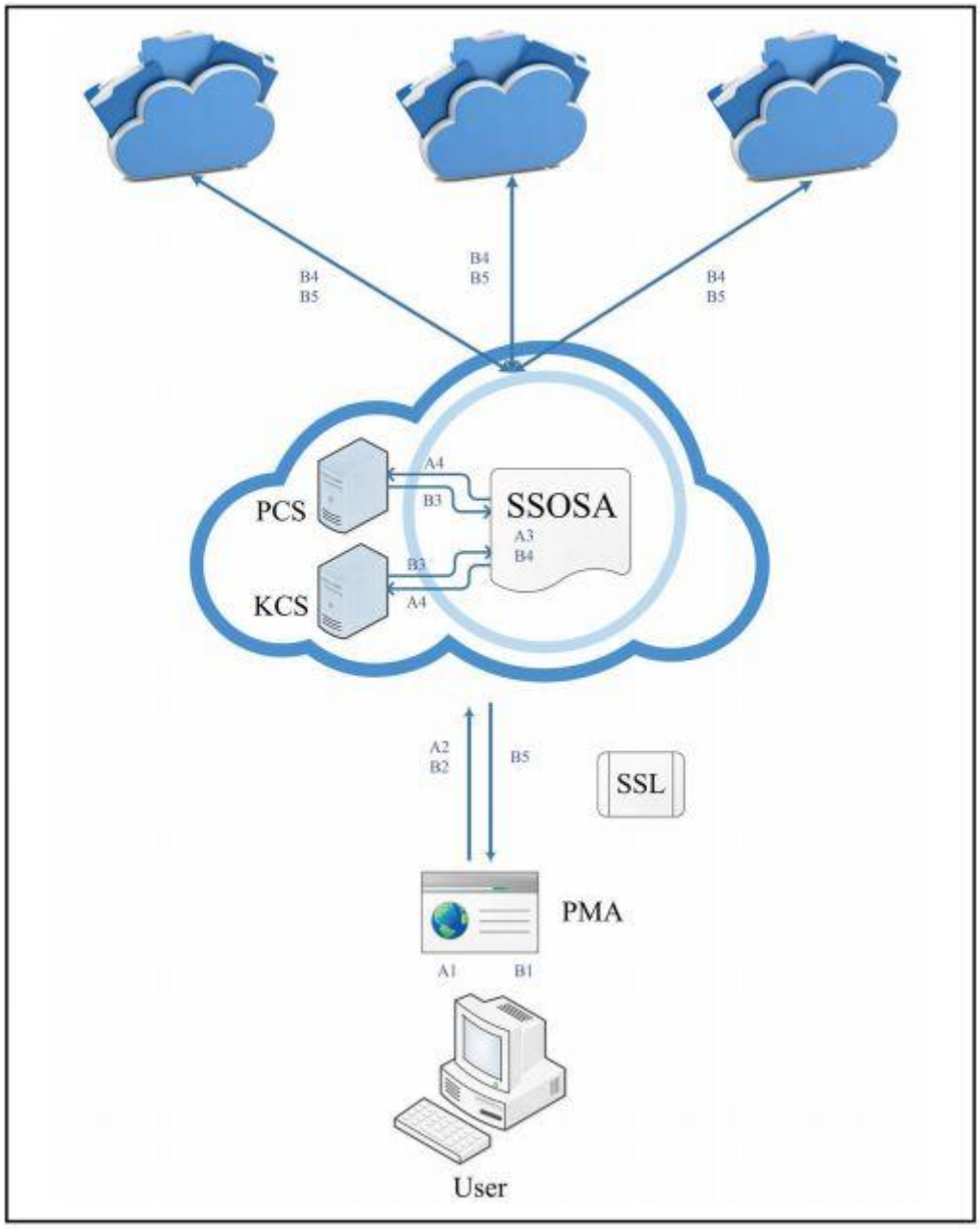

Figure 2- Single sign on using two different servers

Problems identified in the existing Systems.

- There will be a chance of DDOS attack in this model.
- There will be still chance of Man in the middle attack and replay attack.
- Not suitable for enterprise lan system.

VI. CONCLUSION

We have already studied some existing systems on single sign on. But as per above there is a chance of DDOS attack on that systems. So now i want to propose solution for single sign on which will help to solve problem of DDOS attack.

VII. ACKNOWLEDGEMENT

I would like to thank to all who supported me and guided me throughout the survey. I am very thankful to them. It was impossible to complete this without them.

REFERENCES

[1] Pratap Murukutla, K.C.shet, "Single Sign On for Cloud", Phagwara, pp. 176-179, 2012 International conference in computing science, Sep 2012

[2] Faraz Fatemi Moghaddam, Omidreza karimi , "Applying a Single Sign On algorithm Based on cloud computing concepts for SaaS Applications", Kuala Lumpur, pp. 335-339, 11th IEEE International Conference on Communications, Nov 2013

[3] Introduction to Cloud Computing available at www.priv.gc.ca/resource/fsfi/02_05_d_51_cc_e.pdf

[4] Introduction to SingleSign on , available at http://www.techopedia.com/definition/4106/single-sign-on-sso