CROSS CLOUD SINGLE SIGN ON (SSO) USING TOKENS

Priyanka Patil[1], Snehal S. Talokar[2], Vishakha Gonnade[3], Vaishali Bhagat[4]

[1, 2, 3]*Student, Computer Science and Engineering, SRMCEW, Maharashtra, India*
[4]*Lecturer, Information Technology, SRMCEW, Maharashtra, India*

Abstract

The cloud computing service provider ensures the security of their services by username/password schemes. Such type of scheme may be suitable for small personalized services but not for the large scale organizations where employees may require to login for more than one application related to various clouds. This paper identifies the issues of multiple logins and presents how multiple applications of various clouds are accessed by single login process securely. Single Sign-On is the mechanism where a user only need to authenticate him/her self once, then has the ability to access other protected resources without having to re-authenticate. Our objective is to design the single sign on architecture for more than one cloud's applications. Due to that client log in only one time at time and automatically user login in remaining cloud applications and assess successful same process is for log out only user logout once then user logout properly from the all of the cloud applications. The login audits are done for the security purpose and its controlling by admin panel. Cloud service providers also neither need to support redundant registration process for new accounts of applications nor dealing with enormous databases for same user of multiple applications and managing multiple authentication credentials is annoying for users and as well as for authentication system. In other words, Single sign-on (SSO) is the mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords.

Keywords: *Cloud Computing, Password Synchronization, Refreshing Mechanism, Session ID, Tokens.*

----------***----------

1. INTRODUCTION

Cloud computing is known as On-Demand computing and one of the latest emerging topics in IT industry. The cloud computing provide the services over the internet. The services include applications, system hardware, collection of resources on request etc.

Cloud classification is done on their usage mode, if cloud is available for the general users on pay basis according to their usage basis then it is called public cloud. If the customer develops their own applications and run on their own infrastructure then it is called private cloud. Integration of these two clouds is called hybrid cloud.

Community cloud shares infrastructure between several organizations from a specific community with common concerns whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud but more than a private cloud.

The current scenario of web applications forces user to remember the user credentials which make trouble to remembering large number of identities and associated password for the applications. In cloud computing the similar problem faced by the user. This document gives the information about the implementation of Single Sign On (SSO) in cross cloud arrangement.

The following section contains the survey related to the growth of cloud, security aspect, cloud is the first priority to the vendors, revenue report, future and current usage, state of cloud to the IT users and popularity survey of cloud computing.

1.1 Cloud Growth

The survey conducted by International Data Corporation (IDC) shows the strength of cloud computing to be implemented in IT industry and gives the potential inspiration to CSP. The Table 1 shows the cloud growth from year 2008 to 2012[1].

Table -1: Cloud Growth

Year	2008	2012	Growth
Cloud IT spending	$ 16 B	$42 B	27%
Total IT spending	$383 B	$ 494 B	7%
Total-cloud spend	$367 B	$ 452 B	4%

1.2 Cloud Security Survey

The following figure indicates that security as first rank according to IT executives. This information is also collected from two hundred six three IT professional by asking different question related to the cloud, and many of the executives are worried about security perspective of cloud. The Fig. 2.1 shows the survey on security [2].

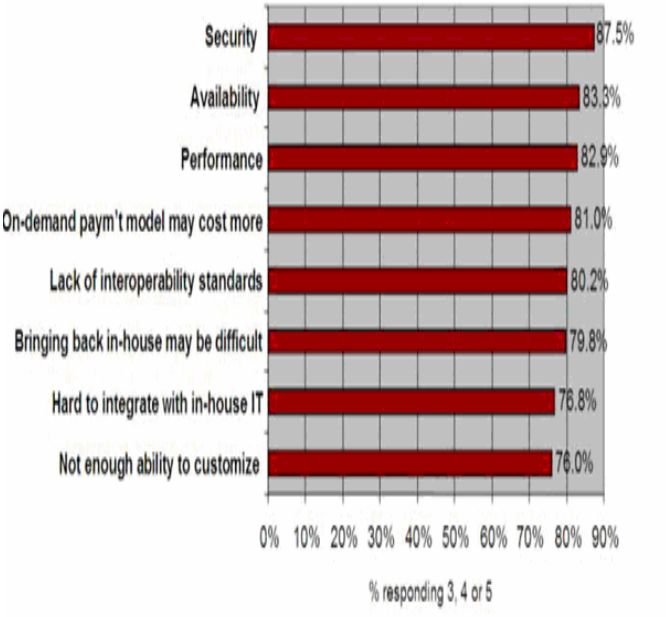

Fig -1: Cloud security survey

1.3 Objective

The aim of our research is to suggest a design of the single sign on web application in cross cloud manner. Due to that client log in only once, at the time of opening first application and automatically user get login in remaining applications and access successful without re-authentication process which makes user free from remembering user credentials.

2. EXISTING SYSTEM

Currently most common authentication approached used by the cloud service provider is user credentials (i.e. username and password) which requires each cloud service provider host its own and separate user management system. The main problem with this system is that for accessing services of various cloud service providers user have to register first and secondly user have to authenticate for each services. Another problem with the existing system is those users have to manage individual username/password pair for each cloud service provider which becomes impractical to expect from user to remember different user credentials for each applications.

3. PASSWORD SYNCRONIZATION

The password synchronization is the process of changing each password for different applications to the same value, so that the user always enters the same password. Once you implement password synchronization technique, users will enter the same password when they login to any of the synchronized systems, such as to their network, finance system, e-mail, calendar or the mainframe.

In other words the password synchronisation is the implementation of same password for each and every applications or system. But using the same password is the weakest policy for the security of system [4] where in SSO only one password is used as similar to password synchronisation but we can ensure the security by using the strong policy.

Another important point is that in password synchronisation [5] user still have to login in each application or system. In single sign on user needs to login once for the primary authentication only then user become authorised to access the all available applications.

Following is the comparative table of password synchronization and single sign on.

Table -2: Comparison of Password Synchronisation and Single Sign On

Parameters	Password Synchronization	Single Sign-on
Process	It is very simple process user change all passwords of application to the same password.	User needs to sign in only one application using single username and passwords. Specific server does the process of authentication for remaining applications.
Login Times	User needs to login each and every time, to get access to applications.	User needs to login only once.
Manage Credential Data	Only management of password required.	Specific mechanism is required for the client such as refreshing and validation of tokens.
Password Policy	For all applications same password is the weakest policy.	One strong password is better than password synchronization.

4. PROPOSED SYSTEM

In our proposed work the architecture of Single Sign On is suggested in cross cloud manner. An admin cloud is used to maintain the login sessions and generating the identifiers for the each application's accessing process. The user credentials are used to form the tokens. The tokens are the encrypted form of the user credentials and the physical address (machine key) of the user machine.

The tokens are used under the supervision of admin who checks the validation of the request send by the user. The admin works as an access manager. Initially users have to send the user credentials for the first time login process. Admin gives token as authorization to get access for the remaining applications.

The tokens generated by the admin clouds contain session information about the authorised user. Session is a data structure in the access manager memory that contains information about an authorised user. The admin cloud is responsible for the generation of session identifiers which are responsible for time dependent behaviours of users.

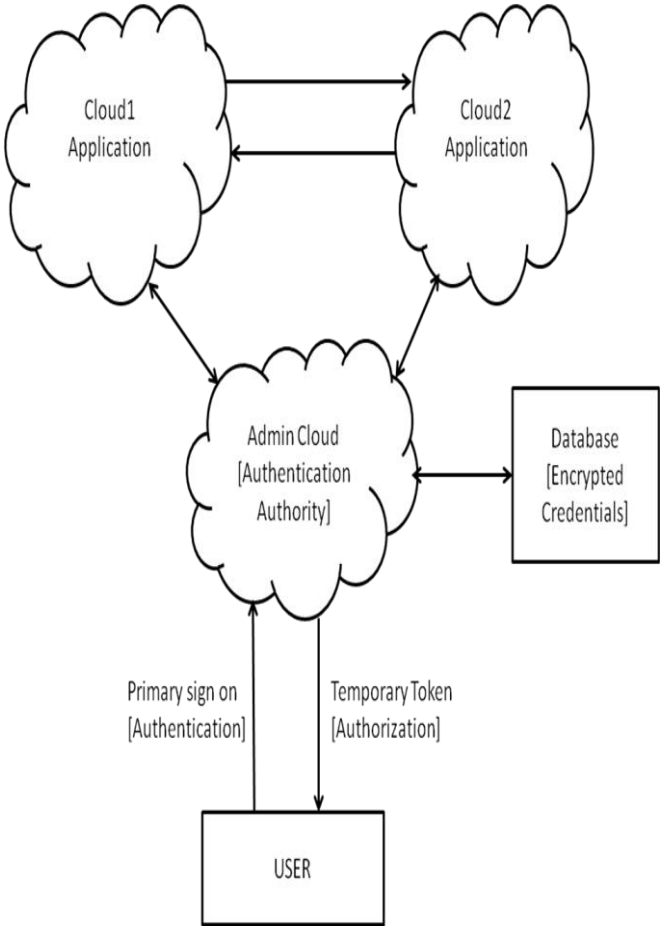

Fig -2: Scenario of cross cloud single sign on

A security problem occurs in the above scenario is that if user is not active at the application, another user tries to get access for another application then admin generate a request to user asking for the user credentials. The request generation is refreshing mechanism.

To sign out user just only need to click on sign out logo which make user to free from the sign out process of individual applications and destroys all the tokens. The destruction of tokens stops the use of history recalling from the user side and inhibit the intruder to use the tokens [3].

5. WORKING

The working of single sign on is performed in the following manner and illustrated in the figure 3.

1. The user first authenticate for the first application accessing procedure
2. The authenticated user request another protected application from another cloud.
3. As the request does not include an app-token, the application server constructs a request-token which is encrypted by a session key shared between the applications cloud and the admin cloud. The user is redirected to the admin cloud along with the request-token.

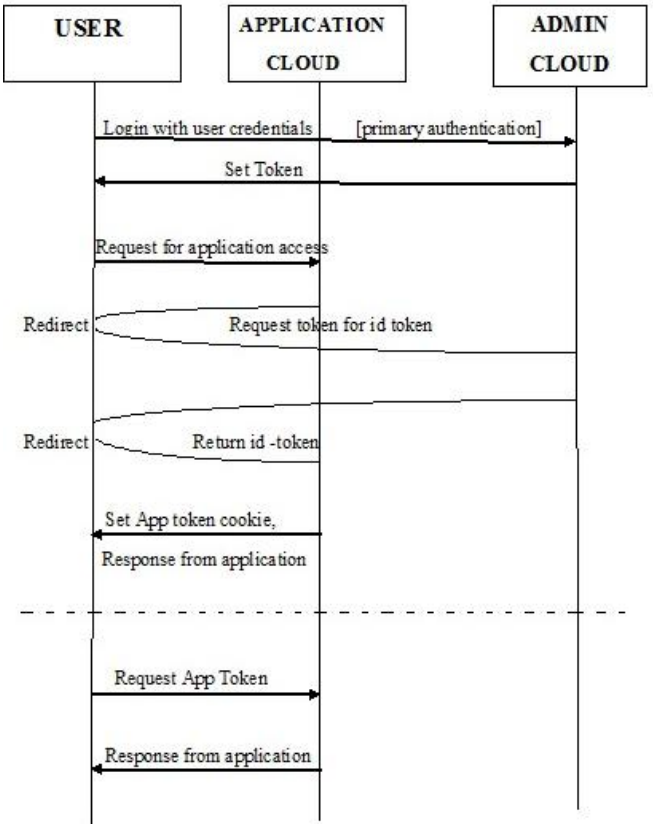

Fig -3: Working of single sign on

4. The admin cloud decrypt the request-token using the session key and detects the user has a valid token. It constructs an id-token and then returns URL, which will contain the response-token, as well as the requested-token.
5. The user is redirected to the original resource, along with the id-token.
6. The application cloud checks the id-token, rewrites the id-token into an app-token, and creates an app-token to be placed into a cookie for future requests.
7. User's browser saves the app-token cookie; the application serves the original request to the user.
8. Logging out of an application involves deleting all the session cookies associated with this application on the server.

6. BENEFITS

The implementation of cross cloud single sign on system improves the productivity of employee with less time users spend logging into so many applications and it also reduces the workload of the helpdesks for recovering the forgotten passwords. Employee productivity is dramatically improved, with less time users spend logging into multiple applications and recovering the forgotten passwords.

Another benefit of this system is that it increases the system security potentially by the user to choose a single complex and more secure password instead of using multiple simple and insecure passwords. SSO effectively reduces the password-related workload to the helpdesk and lowers the costs associated with managing passwords across multiple distributed applications.

7. CONCLUSIONS

In cloud computing, Software as a Service application uses the username/password scheme for the authentication purpose. The implementation of private admin cloud with common database for multiple applications of various clouds can improve the security and remove the password problem.

The proposed system can also be helpful for all cloud service provider to get the benefits of secure cross cloud single sign on and the e-government sector where data sensitivity is very high, cross cloud SSO helps government employee and users to handle data of various departments like health, finance, payment etc.

It is possible to implement the SSO concept which increase the security level of users who manages passwords manually. It also enables the user to use more secure passwords

REFERENCES

[1]. Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010. ICFN ' 10.pp 23, 22-24 Jan 2010.

[2]. Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.

[3]. "Kerberos: The Definitive Guide", Jason Garman

[4]. Kessler "Passwords - Strengths and Weaknesses", Internet and Networking Security, Auerbach, 1997.

[5]. M-tech Information Company, "Definition of Password Synchronization", 2005 http://mtechit.com/concepts/password_synchronization.html

BIOGRAPHIES

Priyanka Patil has received the Diploma in the Computer Science And Engineering from R.G.T.U., Bhopal [M.P.] in 2011 and is pursuing B.E Degree in C.S.E. from S.R.M.C.E.W,Nagpur, Maharashtra INDIA. Her field of interest is Computer Networking & Security.

Snehal S. Talokar, is pursuing B.E Degree in C.S.E. from S.R.M.C.E.W, Nagpur, Maharashtra India. Her field of interest is VB.Net.

Vishakha Gonnade, is pursuing B.E Degree in C.S.E. from S.R.M.C.E.W, Nagpur, Maharashtra India. Her field of interest is Cloud Computing.

Vaishali Bhagat has received the BE Degree in Information Technology from RTMNU, Maharashtra, India in 2008 & pursuing M. Tech in CSE from RTMNU. Since 2010, she is working in the department of IT as a lecturer in SRMCEW, Nagpur, and Maharashtra, India.