Arvind D Meniya, Harkishan B Jethva / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 1,Jan-Feb 2012, pp.891-895

Single-Sign-On (SSO) across open cloud computing federation

***Arvind D Meniya, ** Harikrishna B Jethva**

*(Department of Information Technology, S S Eng. College, Bhavnagar, Gujarat, India)
** (Department of Computer Engineering, L D Eng. College, Ahmedabad, Gujarat, India)

Abstract—Cloud Computing is a concept which serves the computing resources, like Hardware Infrastructure, platform, software application as a Service. Client just need to get connect with the service to use all the computing resources. Cloud users no need to deploy the resources at their site because resources are available at the provider's side and they provide it and charged on usage basis. This paper focuses on the concept of Single-Sign-On (SSO) across all the open cloud to use their computing resources in single or shared manner. We also explore the scenario of interoperability standards between different clouds. This will accelerate consumer specific efficient cloud resource sharing mechanism.

***Key Words*— cloud interoperability, Single-Sign-On (SSO), Cryptographic attack, Service Oriented Architecture (SOA), Open standard for cloud**

I. INTRODUCTION

Traditional business applications have always been very complicated and expensive. The amount and variety of hardware and software required to run them are frightening. You need a whole team to install, configure, test, run, secure and update them. When you multiply these efforts across dozens and hundreds of application, it's easy to see why the biggest companies with best IT departments are not getting the applications they need. Small and medium sized organization doesn't take any chances on this procedure. So what is the better way to eliminate these types of headaches? The answer is "Cloud Computing".

The term cloud computing is a marketing term of technologies that relies between the service provider and client on the internet. Service provider provides computation, software, data access and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Basic environment of cloud computing is shown in below fig.

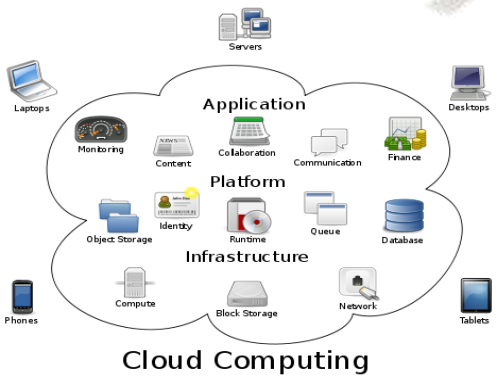

Fig. Traditional Cloud Computing Environment

The idea of the cloud computing can be easily understand by the example of Satellite TV where end-user watch different TV channels without knowing any complexity and understand the component devices or infrastructure required to provide the service.

Cloud computing services are broadly divided into three categories: **Infrastructure-as-a-Service (IaaS)**, where hardware related services are provided using the principle of cloud computing. Second **Platform-as-a-Service (PaaS),** which provides the infrastructure needed to run the application on the internet. And finally **Software-as-a-Service (SaaS),** which are on-demand end user software applications like Google App.

Traditional cloud computing can be divided into four deployment models: In **Public Cloud,** computing infrastructure is hosted at vendor's side. In **Private cloud,** computing architecture is dedicated to the customer and is not shared with any other organizations. **Hybrid Cloud,** which is the combination of public and private cloud. **Community cloud,** in which infrastructure is shared between the organizations of the same community.

Today many companies provide their cloud computing environment to its client, such as Google, Amazon, yahoo etc. If a client wants to use the Google Apps services such as Gmail, he/she need to sign in for the authentication. If an authentication is successful, client can use the service provided by the Google Apps. If a client wants to use another service of the Google Apps, then he/she doesn't need to sign in again, He/she will authorize automatically by the same cloud environment. So this is the authentication process that permits a single user to enter one name and password to use multiple applications. This is the concept of **"Single-Sign-On (SSO)".**

The process of the single-sign-on can be easily work in a single cloud computing environment, but what happens while a single user wants to access different applications from the different cloud computing environment? So user has to enter username and a password for each and every application from different cloud environment. This is the first way by which a single user can access different application from different cloud environment. This will generate the question that is there any functionality or concept is available so that user can access the different application by only single sign in?

This paper mainly focus on the problem just described above and a solution to overcome this problem by making an open cloud computing federation which contains the management of every cloud register in it. This open cloud computing federation will also allow the concept of the single-sign-on in different cloud which is registered in the federation. We will briefly discuss all this mechanism in this paper.

In section I, the basic introduction of the cloud computing is discussed. We will discuss the working of Traditional Cloud computing II. In Section III, we will discuss the concept and working procedure of Single-Sign-On and the issues in traditional cloud computing. Section IV will discuss give the highlight about the issues in traditional cloud computing environment and section V contains the solution of issues discusses in section IV. Section VI contains the security issues which can be effect on developed federation using single-sign-on. Finally, we give the conclusion of this paper in section VII.

II. WORKING OF CLOUD COMPUTING

In traditional enterprise computing, IT departments forecast demand for applications and capacity and invest time and money to develop those resources in-house or purchase them from others and operate them in-house.

As we have discussed about the basic about the cloud computing in section I, we can say that the cloud computing is a paradigm shift from the distribute computing where an organization uses the resources as services. This is a sort of "utility computing" where you pay-as-you-go like electricity bill. Cloud providers are the companies which manage large datacenters and can expertly manage this datacenters. Cloud users may be a single user or an entire organization which uses services from providers. Cloud users need not to deploy the computing resources at their site. These resources are available at the cloud providers on utility basis and charged on uses basis.

Cloud providers specialize in particular applications and services, and this expertise allows them to efficiently manage upgrades and maintenance, backups, disaster recovery, and failover functions. As a result, consumers of cloud services may see increased reliability, even as costs decline due to economies of scale and other production factors.

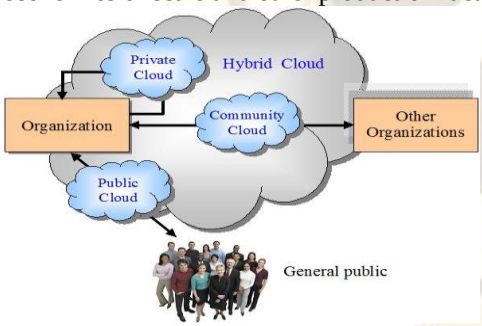

Fig. General scenario of traditional cloud provider

We are taking an example of one cloud service provider that creates the world's largest cloud based infrastructure to understand the working of cloud computing mechanism, that is: **Google.**

Google provides the Google Apps Engine that lets you run web applications on Google's infrastructure. App Engine applications are easy to build, maintain, and scale as your traffic and data storage needs grow. Users just have to create an account in Google and that is the use of Public cloud of Google. User creates his/her own account and mange it, so user establishes his private cloud environment where he can use different services provided by Google. Public cloud is used by the user in his private cloud that creates the Hybrid cloud.

Google Apps now allows free hosting of your e-mail server (with your own domain name), up to 7.3 GB of storage per free user account **(IaaS)**, and free Google Talk, Google Calendar, Google Docs (for creating and sharing documents, spreadsheets and presentations, collaboration in real-time right inside a Web browser window), Google Sites (for easily creating and sharing a group Web site) and Start Page (**SaaS**), and so forth.

Google cloud services can be run in any system from anywhere without any consideration of which platform system provide, which OS provide with internet connection. This thing provides the **PaaS** concept of cloud by Google to its user.

III. SINGLE SIGN ON (SSO)

As IT systems proliferate to support business processes, users and system administrators are faced with an increasingly complicated interface to accomplish their job functions. Users typically have to sign-on to multiple systems, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information. System administrators are faced with managing user accounts within each of the multiple systems to be accessed in a co-ordinated manner in order to maintain the integrity of security policy enforcement.

Such a wide range of systems brings with it a vast amount of username / pass-word pairs to remember. The credentials in many cases are given as a secret word at the startup of an application and since humans are tempted to forget things, these credentials are noted down on reminder stickers or other unsecure media which can be accessible to anyone.

So there is a need to remove this functionality that the user has to enter user name and password for each and every service he wants to use. The concept of Single-Sign-On (SSO) removes this functionality and provides a better way to give the authentication to user without multiple sign-in process to use different services. Simple scenario of SSO between different domains is shown in the following fig.

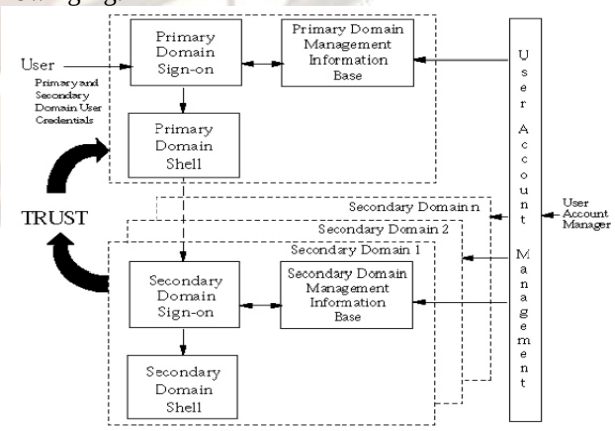

Fig. simple scenario of Single-Sign-On

We can define the Single-Sign-On (SSO) as a user authentication process that permits a user to enter one name and password in order to access multiple services. The information supplied by the user as part of the primary domain sign in procedure may be used in support

of secondary domain sign in procedure in different ways, such as directly, indirectly, temporary, or immediately.

IV. ISSUES IN TRADITION CLOUD COMPUTING ENVIRONMENT

In today's technology environment, many cloud providers are available, such as Google, Microsoft, Amazon and users have a choice of selecting a best cloud environment which satisfies his requirement. Every cloud environment provides the different services to its users at the same time using single sign on. Every cloud provider provides the different services to its authenticate user, so the main thing is that every user has to first subscribe or register to a respected cloud environment and then the user can access the services provides by that cloud. This is the procedure for every cloud provider to authenticate user and give the privileges to access its services. This is the scenario for every cloud provider.

Now issue is generated that what happen if a same user wants to access the different services provides by the different cloud provider? For example, if a user is using the Google docs service from Google and user have to maintain the database using another service which is provide by the other cloud provider say Oracle cloud. So how user can use both the services from the different cloud provider? The simple solution for this issue is that user has to first subscribe in the entire cloud provider environment and then the user can access the services from different cloud provider.

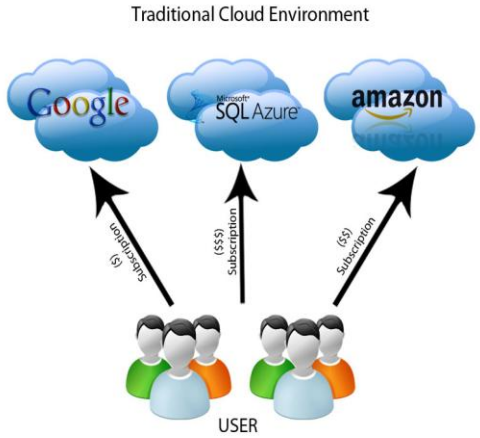

Fig. Traditional Cloud Computing Environment

In above scenario we explain the traditional cloud computing working that every cloud provider is using. The second approach for the above issue can be resolve by creating one federation for the different cloud providers and by using the concept of Single-Sign-On. With the help of SSO, we can use the different services provides by the same cloud provider, but not use the different services provides by the different cloud provider.

V. SOLUTION FOR THE TRADITION CLOUD COMPUTING ISSUE

The above discussed issue can be solved by creating one federation of traditional cloud providers which will provide the different services from the different cloud providers. With the help of Single Sign-in process, a single user can access all the services which are provided by different cloud provider that are member of this federation.

The solution of the traditional cloud computing environment can be resolve by making a universal open cloud federation. The given solution can be view as given below.

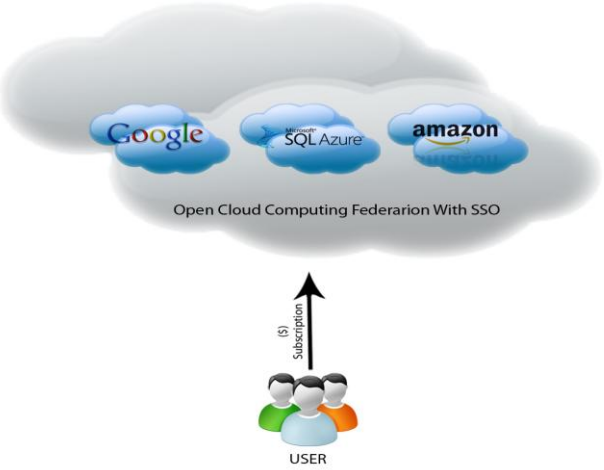

Fig. Every cloud provider members of Open Cloud Computing federation and user can use different services provides by this federation.

As shown in above figure, we are taking an example of most famous cloud provider of recent time that is **Google**, **Microsoft SQL Azure** and **Amazon**. If these three cloud providers are a member of open cloud federation, then they provide all the services to the user who registered in this open cloud computing federation. As we have discussed the issue of traditional cloud environment in section IV, here the issue can be solved using the concept of open cloud computing federation.

The main part of this open cloud federation is providing SSO between the user and different cloud providers which are the authorized members in this federation. Instead of subscribe in different cloud, user just have to subscribe in this open cloud federation. After successful subscription, user can use the services from different cloud by interoperability between clouds.

So if user wants to take an advantage of the Google's web application framework and to develop their application, and also take an advantage of Microsoft's cloud based intensive data storage service then user just need to probe these two services. To connect these services user need open standard specified by the respective cloud provider.

The open cloud computing federation provides the platform for probing services of cloud provider and follows the open standards specifies by the respected cloud provider.

VI. SECURITY ISSUES RELATED TO OPEN CLOUD COMPUTING FEDERATION

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used.

This open cloud computing federation provides the great concept for sharing services from different cloud providers by just a single sign in process to user. User is not aware about how cloud services are provided, But this concept arise some vulnerabilities which are as follow.

A. Data Privacy

Every cloud provider which are members of this federation, have to compromise their data with the service of other cloud provider. So this is violation of the clouds privacy.

B. Misuse of Data

Because there is interoperability between cloud of this federation, data of one cloud can be easily used by another cloud. So there is possibility to misuse the data or changes in original data.

C. Standardization

It is hard to achieve the standardization that open cloud computing federation will fulfill each and every open standard of different cloud provider.

D. Hacker's Attack

Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

E. Denial of Service (DoS) Attack:

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009. We are creating a federation of different cloud provider, so this is consider as a major security issue in open cloud computing federation.

F. Side channel Attack:

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. We are providing a different cloud provider at a single place. So, if users will success for one cloud compromises, they can achieve all the data from different cloud.

G. Authentication Attack:

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Once user has been authenticating, he can use all the data from the cloud.

H. Man-in-the-middle cryptographic Attack:

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications. This attack can violate the working and the sharing of services to single user.

I. Data Classification system in cloud

This type of security issue mainly generates the question of users data classified in cloud. The main question user should concern with this issue is: Is data classified? How one user's data is separated from other user? Encryption should also be concern while data is in rest and in transit.

J. SLA (Service Level Agreement) Terms:

The SLA services as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

K. Long Term Viability of Cloud Provider:

How long has the cloud provider been in business and what is their track record. If they go out of business, what happens to your data? Will your data be returned, and if so, in what format? As an example, in 2007, online storage service MediaMax went out of business following a system administration error that deleted active customer data. The failed company left behind unhappy users and focused concerns on the reliability of cloud computing.

L. Security breach in Cloud Provider:

If there is any security incident creates, how can user get the support from the cloud provider? Many cloud provider claim that services provides by them are free from hackers, but cloud based services are a most target to the hackers.

M. Functionality of all clouds is not identical:

The different models for cloud service delivery (IaaS, PaaS, SaaS) have different requirements of the customer when it comes to security. The less control you have the greater you must rely on the security practices of the provider. Understanding where the lines are drawn and who is responsible for what is vital before moving *anything* of value to a cloud.

These are some major security issues the cloud developers must have to concern while developing an open cloud computing federation.

VII. CONCLUSION

Cloud computing is the most popular notion in IT today; by reviewing from the traditional cloud computing environment of business, we can say "Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry." I would like to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing". While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud.

Our vision relates to making an efficient and more specific open cloud computing federation that removes the complexity of cloud user in traditional cloud environment. By implementing this type of federation, there will be a universal way to provides different cloud services at one place and user does not need to sign-in for different cloud because of introducing the Single-Sign-On to the federation and probing between clouds.

Our vision not only to focus on good side of this federation, we also have to focus on other side of this solution, that is Security issues arises while implementing this type of federation. And also considers the problem that how a federation will manage if a new issue arises.

REFERENCES

[1] *Armbrust, M., Fox, A., Griffith, R. et al.* Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[2] How to Secure Cloud Computing. http://searchsecurity.techtarget.com/magOnline/0,sid14_gci1349550,00.html

[3] Google Docs Glitch Exposes Private Files. http://www.pcworld.com/article/160927/google_docs_glitch_exposes_private_files.html

[4] Security issues with Google Docs. http://peekay.org/2009/03/26/security-issues-with-google-docs/

[5] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[6] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. http://blogs.idc.com/ie/?p=210

[7] Privacy in the Clouds: Risks to Privacy and confidentiality from Cloud Computing. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[8] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[9] What is cloud computing? http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[10] Introduction to cloud security http://www.esecurityplanet.com/trends/article.php/3930401/Top-5-Cloud-Computing-Security-Concerns.htm

[11] Secure multiparty computation for cloud computing paradigm by *Durgesh Kumar Mishra* http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=5701921&openedRefinements%3D*%26filter%3DAND%28NOT%284283010803%29%29%26searchField%3DSearch+All%26queryText%3Dcloud+computing

[12] Design and auditing of cloud computing security by *Gowrigolla, B.; Sivaji, S.; Masillamani, M.R.; Dept of Comput. Sci. & Eng., Hindustan Inst. of Technol. & Sci., Chennai, India* http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=5715676&openedRefinements%3D*%26filter%3DAND%28NOT%284283010803%29%29%26pageNumber%3D2%26searchField%3DSearch+All%26queryText%3Dcloud+computing

[13] Identity federation in a Hybrid cloud computing environment solution guide http://www.techrepublic.com/whitepapers/identity-federation-in-a-hybrid-cloud-computing-environment-solution-guide/2385477

[14] Cloud federation and inter cloud http://www.buyya.com/papers/InterCloud2010.pdf

[15] Single-Sign-On concept in VMware http://www.readwriteweb.com/cloud/2011/05/vmware-launches-single-sign-on.php

[16] *Jan De Clercq*, "Single Sign-on Architectures", Proceedings of Infrastructure
Security: International Conference, InfraSec 2002, Bristol, UK, pg 40-58, October 1-3, 2002.

[17] Ely, Adam, "Get Serious About Cloud Security", 2008.

[18] *Junjie Peng, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang, Qing Li*, "Comparison of Several Cloud Computing Platforms", School of computer science & High performance computing center Shanghai University Shanghai, 200072 P.R. China.