ISSN 2047-3338

Enhanced Secure Model for Single Sign-On Across Open Cloud Federation

Asif Iqbal, Haroon Ur Rashid and Muazzum Khattak

***Abstract*– Cloud computing enables users to get their resources on pay per-use basis using internet. There are many advantages of it but security is the main concern too. One powerful user-name password scheme shall far better than dozen ordinary ones. Remembering so many schemes is very difficult and Single Sign-On (SSO) is a way to solve this problem. This paper focuses on and extends the concept of SSO, to avail the services of not only Home cloud-Service-Provider (HSP), but also of Foreign cloud-Service-Provider (FSP), using credentials stored on the HSP site. A scenario is explored along with algorithm that will show this concept works to make users more efficient, by utilizing the services of HSP and different FSPs. This paper is an effort to remove the problems in Open Cloud Computing Federation that were mostly pointed out by Arvind D. Meniya et al. [3] through a new idea.**

***Index Terms*– Cloud Computing, Cloud Service Providers, Open Cloud Computing Federation, Single Sign On and Home Cloud Service Providers**

I. INTRODUCTION

THE term cloud or "the cloud" is closely related to "the Internet", as it is a type of Internet-based computing and different services such as servers, storage and applications are provided to public users or an organization's computers through the internet [14]. There is no single definition of cloud computing on which everyone agrees [19]. According to NIST "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" [20], [16]. The cloud model has five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service), four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud) and three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)) [21].

In October 2007, Cloud computing got popularity [4]. It enables its users to reduce cost of hardware deployment, software licenses and system maintenance [8]. Cloud computing is a very attractive area for public users and especially for business organizations. Cloud provides a large pool of virtualized resources to its users, on a pay per use bases. It means users / organizations can utilize the amount of resources according to their need. Cloud services are stored on data centers and users access them through browsers or any other service. User can connect to these services from anywhere and at any time and can use applications that are provided by the cloud providers. These services are in the form of storage, computation, access to data and applications. To get the optimum utilization of resources, are dynamically reconfigured to adjust to a variable load (scale) [5].

Virtualization is the basic concept behind the success of Cloud computing [6], [18]. Virtualization lets you [11]:

- Enables a single computer to run multiple operating systems and applications
- Consolidates resources like hardware to get enough productivity from less number of servers
- Provides 50 per cent savings or more on overall IT costs of the organization.
- New cloud applications are more quickly and easily managed, maintained, and deployed.

There are some issues related to cloud computing and due to these issues consumers are reluctant to adopt cloud computing. Security is the biggest issue with many users or organizations for cloud computing as mentioned by Vijay G.R [16]. SSO can play an important role to improve security of cloud computing. One powerful password is far better than dozen of weak passwords. If a user wants to get the services of different service providers, then he/she can access them by using each service provider's user user-name and password. It will be very difficult for any user to remember these user-names and passwords of all CSPs to access their services. So the solution is SSO, by maintaining a centralized Third party Auditor (TPA) as mentioned in [3] for checking users authentication. What will happen if this TPA fails and removal of the issues / problems that where mentioned in [3]

Asif Iqbal, PhD Scholar University of Malakand, Pakistan
Haroon Ur Rashid, CECOS University, KPK, Pakistan
Muazzum Khattak, Assistant Professor, NUST, Islamabad, Pakistan

are of very important nature. This makes my research problem domain.

Problem Domain: This paper aim is to focus on the following two issues:

- How to remove problems mentioned by Arvind D. Meniya et al [3]?
- What will happen in case of centralized TPA failure regarding security, trust and privacy for cloud service providers and users in case of OCCF environment?

The rest of paper is designed as: the related work will be discussed in the next section. Section III is related to SSO basics. In section IV the proposed model will be discussed with Scenario, algorithm and flowchart. Section V will discuss conclusion and future work.

II. RELATED WORK

Some of the important papers will be presented in this section that proved to be very important / helpful for this research work.

Arvind D. Meniya et al [3] have presented a model for Open Cloud Computing Federation (OCCF). In that model they presented centralized registry for users to use all resources of CSPs. Here the concept looks to be theoretical. The authors have presented their idea through scenario and mentioned some strength and weaknesses in OCCF of a very important nature.

"High Security and Privacy in Cloud Computing Paradigm through Single Sign-On", was proposed by Muhammad Munwar Iqbal et al. A method for single sign-on implementation had been presented for heterogeneous cloud federation in their paper and also explained how their model works to provide better security for using cloud services [7].

As already mentioned security issues are one of the key issues in cloud computing. The same is addressed in [8] by Danish Jamil et al. and also proposed some countermeasures for resolving issues like XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks on theoretical bases.

Without proper standards it would be very difficult to gain full advantages of clouds in federation. This concern was also discussed by Guilherme Sperb Machado et al. [12]. They presented "proprietary features"; (that the cloud owner can change their services if they wish to), and "cloud core capabilities", (features cannot be changed in the federation of clouds) for making better cloud federation and these two to be the base for standardization. This standardization of federation is not exhaustive and only theoretical work.

In cloud data is stored in the encrypted form. But what is about it when data is going to be transferred from user system to the cloud. Fadadu Chirag et al. [13] discusses this problem and provided solution for it by sending file form client's computer in encrypted form to cloud. There was neither a practical implementation in this paper as well.

"Single Sign-On for Cloud", proposed by Pratap Murukutla, K.C. Shet [15]. It provides a way to use services of different cloud service providers through single sign-on. They proposed their model with algorithm and also tested their work. It provides information regarding what alternatives of Single Sign-On (SSO), having defacto standards.

III. SINGLE SIGN ON

Single Sign On which is shortly represented by SSO and it a process by which we can use one system login for many applications [9]. It has 3 defacto standards SAML, OpenId and Open authorization to provide the Single Sign on mechanisms. OpenId and SAML are the standards for authentication while Oauth provides authorization and pseudo authentication [15]. Benefits of SSO include [1]:

- Reducing headache of trying to remember many user names and passwords combinations for a user
- Reducing the amount of time spent on re-entering user name and passwords for the same identity
- Less number of help desk calls about passwords

In traditional cloud computing environment every cloud service provider provides services to its authenticated users for fulfilling their needs, the user will provide his user-name and password for authentication and after being considered as an authenticated user, they will be granted required resources on basis of their registration with that particular cloud service provider for example Amazon. The same user then has to repeat the same process to avail services of another cloud service provider, such as Google and so on. It is also common that different service providers have different sign in scheme and it makes the job of user and system administrator more difficult. When the user is dealing with so many user names and passwords, they can easily be forgotten or their password can be taken by someone else, if the user writes it down. The user is putting themselves or the organization at risk. The traditional cloud computing environment is shown in Fig. 1.
Traditional cloud computing is a time consuming process as the user has to repeat this process when wants to use services of different CSP. So there is a need to develop such a paradigm that allows the user to just sign on once and use the resources of different cloud service providers. This idea helps to develop a new idea of Open Cloud Computing Federation using SSO. Arvind D. Meniya et al. [3] tried to solve this issue by maintaining a centralized registry i.e., third party auditor as shown in Fig. 2. They also mentioned many problems in this regard shown in Table 1.

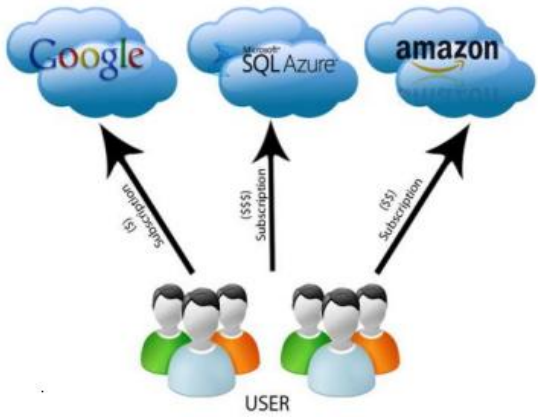

Fig. 1: Traditional Cloud Computing

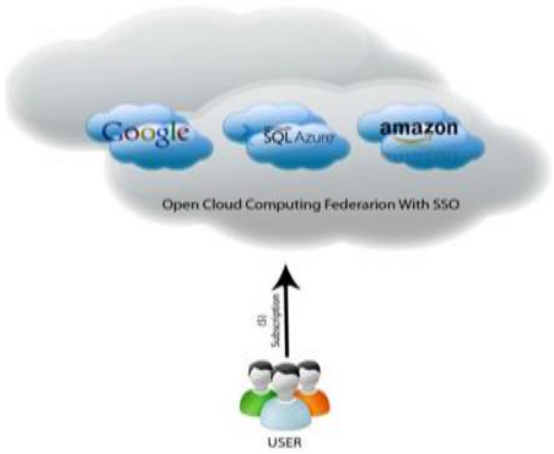

Fig. 2: Every cloud provider members of Open Cloud Computing Federation and user can use different service providers by this federation [1].

IV. PROPOSED MODEL

Assumption: Cloud Service Providers have a contract to provide their services to other cloud service providers on the basis of per use and payment to the owner of service. To solve problems in OCCF, this paper will propose a new idea, where the services of foreign cloud providers (e.g., Google, SQL Azure etc) will be available to home cloud service provider (e.g. Amazon) through a link that will exist between them, on the basis a of contract as mentioned in the assumption. In the same way the services of this home cloud provider will be available as foreign cloud service providers in other cloud service providers (e.g., Google, SQL Azure etc). The link would be used for communication between home and foreign clouds e.g. services request on the behalf of the user from HSP to FSP, to keep check on usage of services. It is also important that both HSP and FSP will keep records of usage of the services, so according to the agreement the payment will made to the deserving party. The diagrammatic representation of my proposed model is shown in Fig. 3.

Here users of any HSP are still able to access all services of any FSP, through a single user-name and password. Here only one user-name and password would be enough for user, to gain all services of any provider, though there is the possibility of keeping more than one user-name & password,

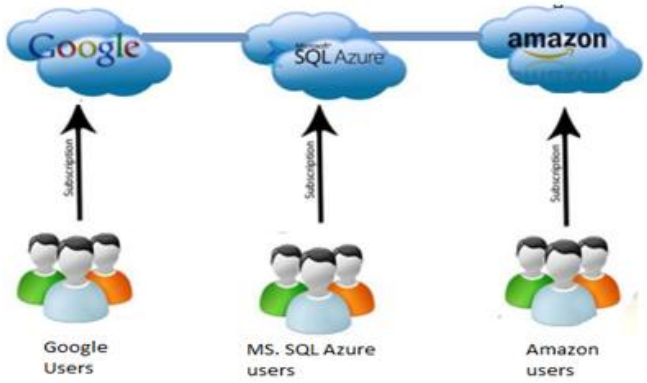

Fig. 3: Users of one cloud service provider is using the service of other cloud provider's services through SSO.

without any sound reason behind it. Registered Group of users will most probably retain users with the same HSP, because they are getting services from all cloud service providers. That is the reason that every user will most probably have one ID. The new users can join any cloud service provider as a Home Cloud Service Provider for that particular user. If a user wishes to use services of any FSP that are not available with HSP, then HSP will forward the request of the user to that particular FSP and the FSP will provide that service to that particular user on the basis of agreement.

How this model will work is shown in the following Fig 4. User Authentication Authorization Module (UAAM) checks if the user is registered to HSP or not. It checks the credit of user for accessing services. It performs these two jobs by looking at records of a user in a database. There is another module i.e., SMM related to the services that are to be provided to the users from HSP and FSP databases. It will observe the nature of request either the service request is for HSP or FSP and accordingly it will provide service from HSP or FSP. In case of FSP service, it will forward the request of the user to FSP and accordingly the service will be provided from FSP.

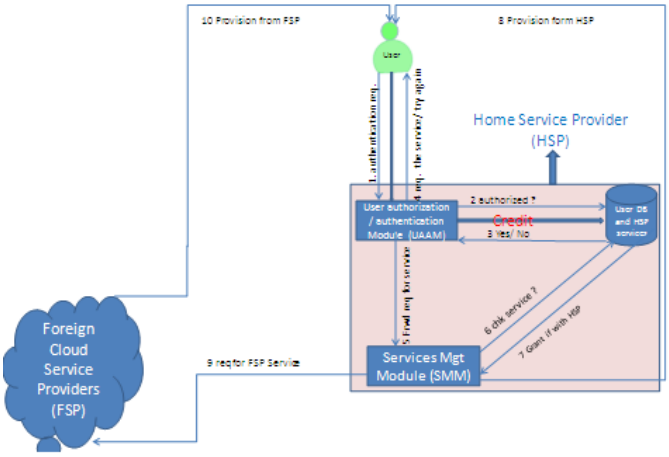

Fig. 4: Scenario of proposed model

A) Algorithm Implementation and flow chart of Proposed Model

The algorithm for the proposed model is:

1. Enter User Name and Password.
2. if (Not authentic user) then
3. print " try again" (2 times more i.e., goto step 1 or more than 3 attempts goto 9)
4. else
5. if(Not credit?) then
6. print " can't get paid services"
7. else
8. provide service from HSP or FSP
9. finish

The flowchart for the proposed system is given in Fig. 5.

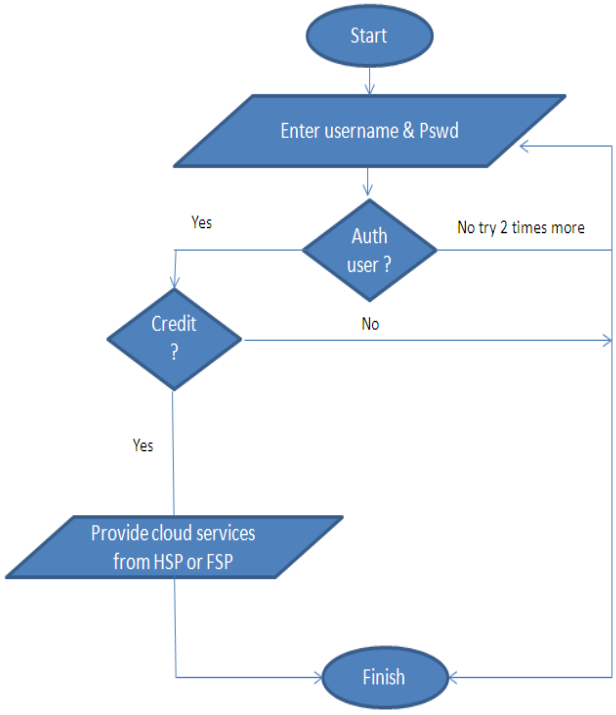

Fig. 5: Flow Chart of proposed model

B) Solution for the Problems in Open Cloud Computing Federation issue

As this research work is based on two questions. Now let us focus on the first question.

How to remove problems mentioned by Arvind D Meniya et al. [3]**?:** Brief list of problems in open cloud computing and this research work answer is given in the Table 1.

Table I: Overview of problems in OCCF and proposed model response

Problems	Open Cloud Computing Federation	Proposed solution of this research
Data Privacy	No	Yes
Misuse of Data	No	Yes
Standardization	No	Yes
Hacker's Attack	No	Yes
Denial of Service (DoS) Attack	No	Yes
Side channel Attack	No	No
Authentication Attack	No	No
Man-in-the-middle cryptographic Attack	No	No
Data Classification system in cloud	No	No
SLA (Service Level Agreement) Terms	No	No
Long Term Viability of Cloud Provider	No	No
Security breach in Cloud Provider	No	No
Functionality of all clouds is not identical	No	No

Now let us see how these issues can be resolved, mentioned in the Table 1.

Data Privacy: As there is no sharing of user accounts or credentials between different cloud providers in this model the privacy of user credentials would be handled in far better way as compared to OCCF. Every CSP may keep its own TPA rather than just a centralized TPA as mentioned in [3] for all users of all CSPs.

Misuse of Data: As the credentials of users of particular cloud will remain with the same cloud, here the chance of misuses are minimum as compared to OCCF.

Standardization: The base for the solution of this problem is provided in [12].

Hacker's Attack: Since, each home cloud provider is responsible for protecting his own services and user credentials, then number of attacks will be divided as compared to OCCF and the risk would be less if the number of attacks per cloud is minimum as well as in case of side channel attack.

Suppose we have 'N' clouds and attacks are 'x'.

Then the Number of attacks per cloud will be N/x, as compared to N attacks on unified credentials as in OCCF.

Denial of Service (DoS) Attack: As the number of users would be less, and due to better management in each home cloud provider, the chances of DoS attacks are lessened.

Now let us move to Question 2.

What will happen in case of centralized TPA failure regarding security, trust and privacy for cloud service providers and users in case of OCCF environment?: As in Open Cloud Computing Federation, the credentials of users will be placed in a single location with third party Auditor; this produces concern in users mind about their data. It will further increase the issues of privacy, trust and security. Users will have to think about the storage of their credentials on third party data centers, because their credentials were only with certain cloud provider and now it is available to all cloud service providers. Also HSP will also be worried about services and own users credentials. So it is a two faceted problem i.e., first the worries of users about their credentials in OCCF, second the worries of HSPs about their user credentials and services in OCCF.

So to get higher trust level and other related problems (security etc) it will be better that every CSP will store its user's credentials with own local TPA, rather than storing all of user's credentials of all CSPs in single TPA (as in OCCF). The level of trust of users will be higher in this model as compared to OCCF. The providers trust level will be also high with this approach as compared to if providers place user's credentials on federated accounts manager as in OCCF.

Apart from the above Management of fewer users is easier in comparison to OCCF, where there will be many cloud service providers users at one location. This research model is a kind of divide and rule based strategy as compared to centralized structure of OCCF. So System Administrator work is easy here compared to the previous approach. Things will be handled here in a smooth way.

There is another issue which is "what will happen if centralized registry fails some way in Open Cloud Computing Federation and fails to authenticate its authorized users or any

other destruction happens". In proposed model, if a HSP local TPA fails it would only be limited to that particular HSP. All other Cloud providers will be able to continue their services in a normal way.

V. CONCLUSIONS AND FUTURE WORK

Cloud computing has got tremendous attention attentions of users and researchers in the last few years. It is due to the great benefits that it provides to not only individuals but to organizations, corporations and small businesses as well. By 2014 the revenue and market size of cloud computing will reach to USD 149B and compound annual growth rate of 20 [20]. Therefore, I will suggest to developers to develop software working in cloud environment because in future a lot of work is still to be done. We will also advise companies to put some part of their business on cloud, so they can get establish their name in the market, before a complete transfer over. The purpose of this research is to remove problems in OCCF, through a new concept based on SSO. It will make the job of users more efficient, easier, and more secure. The proposed work has not been tested practically. Our next goal is to implement the proposed design.

ACKNOWLEDGMENT

These are not formal words; they are from the depth of heart. I am very thankful to Dr. Muazzum Khattak, for providing true guidance. Also I am very thankful to my friends for their help and especially to my family members who encouraged me a lot to do research work.

REFERENCES

[1] Single Sign On, http://en.wikipedia.org/wiki/Single_sign-on#Common_Single_Sign-On_Configurations, accessed on 07-14-2013

[2] http://www.opengroup.org/security/sso/sso_intro.htm, accessed on 01-17-2013, accessed on 01-17-2013

[3] Arvind D Meniya, Harikrishna B Jethva, "Single-Sign-On (SSO) across open cloud computing federation", IJERA ISSN: 2248-9622, Vol. 2, Issue 1,Jan-Feb 2012, pp.891-895

[4] Sara Qaisar and Kausar Fiaz Khawaja, "cloud computing: network/security threats and countermeasures", on Interdisciplinary Journal of Contemporary Research in Business (IJVRB) , Vol 3, No 9

[5] Pankaj Arora, Rubal Chaudhry dhawan, Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service", Vol. 2, Issue 1, January 2012 ISSN: 2277 128X , Available online at: www.ijarcsse.com

[6] Tutorial: by Professor Huaglory Tianfield, "Identify Federation and Access Control in Cloud Computing", Dept. of School of Engineering and Built Environment Glasgow Caledonian University, United Kingdom, available at www.ieee.com, accessed on 06-04-2013.

[7] Muhammad Munwar Iqbal, Muhammad Salman Bashir, Yasir Saleem, Muhamamd Farhan, Amjad Farooq, Abad Ali Shah, "High Security and Privacy in Cloud Computing Paradigm through Single Sign On", available at http://www.sciencepub.net/researcher

[8] Danish Jamil, Hassan Zaki, "Security issues in cloud computing and countermeasures", Vol. 3 No. 4, International Journal of Engineering Science and Technology (IJEST), April 2011

[9] Single Sign On, http://www.comparethecloud.net/cloud-computing/software-as-a-service/single-sign-on/, accessed on 07-14-2013.

[10] https://wiki.cloudsecurityalliance.org/guidance/index.php?title=Cloud_Computing_Architectural_Framework&oldid=18, accessed on 01-21-2013

[11] Virtualization basics, http://www.vmware.com/virtualization/what-is-virtualization.html, accessed on 07-14-2013

[12] Guilherme Sperb Machado, David Hausheer, Burkhard, "Considerations on the Interoperability of and between Cloud Computing Standards", Stiller Communication Systems Group CSG, Department of Informatics IFI, University of Zürich UZH Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

[13] Fadadu Chirag, Shrikanth Venkatesh, Trivedi Harshal, "Cloud Security Using Authentication And File Base Encryption", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012, ISSN: 2278-0181

[14] Cloud Computing, http://www.webopedia.com/TERM/C/cloud_ computing.html, accessed on 07-14-13.

[15] Pratap Murukutla, K.C. Shet, "Single Sign On For Cloud", 2012 International Conference on Computing Sciences, National Institute of Technology,Karnataka

[16] Vijay.G.R, Dr.A.Rama Mohan Reddy, "Security Issue Analysis in Cloud Computing Environment ", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January - February 2013, pp.854-857.

[17] White paper by ThinkGird, http://www.thinkgrid.com/docs/computing-whitepaper.pdf, accessed on 17-02-2013.

[18] Loganayagi B. and S. Sujatha, "Secure Cloud Computing Services with ECPS", European Journal of Scientific Research, ISSN 1450-216X, Vol. 91, No. 1, Nov. 2012, pp.119-131, http://www.europeanjournalofscientificresearch.com

[19] Deepti Sahu, Shipra Sharma, Vandana Dubey, Alpika Tripathi, "Cloud Computing in Mobile Applications", International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012, ISSN 2250-3153, www.ijsrp.org

[20] Deyan Chen and Hang Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering. http://www.nist.gov/itl/cloud/, accessed on 14-02-2014.