I. J. Computer Network and Information Security, **2015, 6, 50-58**
Published Online May 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.06.06

Single Sign-On in Cloud Federation using CloudSim

Manoj V. Thomas, Anand Dhole, K. Chandrasekaran
Department of Computer Science and Engineering, National Institute of Technology Karnataka
Surathkal, Karnataka, India-575025
Email: manojkurissinkal@gmail.com, dhole.anand@gmail.com, kchnitk@gmail.com

Abstract—Single Sign-On (SSO) is an authentication mechanism in which a Cloud Service Consumer (CSC) needs to be authenticated only once while accessing various services from multiple service providers, or when accessing multiple services from the same service provider. In the case of Cloud Federation, the consumers can get services from various Cloud Service Providers (CSPs) who are members of the federation, and SSO can be used to verify the legitimate users without requiring them to get authenticated with each service provider separately. CloudSim is a popular tool used for simulating various cloud computing scenarios. As of now, the simulator lacks effective user authentication and authorization methods with it. In this paper, we discuss the design and implementation of SSO mechanism in the Cloud Federation scenario using the CloudSim toolkit. We have used the Fully Hashed Menezes-Qu-Vanstone (FHMQV) protocol for the key exchange and the Symmetric Key Encryption technique AES-128 for encrypting the identity tokens. We give the workflow model for the proposed approach of SSO in the Cloud Federation and also, the execution time taken in the simulation for various Single Sign-On scenarios where the number of SSO required varies are also shown.

Index Terms—Authentication, Authorization, Single Sign-On, Cloud Federation, Fully Hashed Menezes-Qu-Vanstone, Advance Encryption Standard, CloudSim.

I. Introduction

Currently, the Cloud Computing domain offers different cloud services such as the public, private and the hybrid clouds. This Cloud Computing environment provides service consumers various benefits such as the elasticity in using the resources, high availability, reduced maintenance costs and also the ability to pay as per their usage. These benefits have increased the acceptance of the Cloud services over time. Cloud Computing has brought a whole new set of services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) etc. which are made available to the users through the internet. However, there is also the downside associated with the use of the Cloud Computing model such as security concerns of the data stored in the cloud, ownership of the data, vendor lock-in due to the lack of global standards and protocols for inter-operability and communication [1]. Nowadays, Cloud Federation is an emerging technology to meet the highly dynamic resource requirements of the cloud consumers.

In Cloud Computing or Services Computing, users access various resources or services after verification of their identity by the service provider. Access control deals with verifying the access rights of users towards different resources in the system. Verification of the identity and the access privileges of the service consumers is utmost important in Cloud Computing or Services Computing, before they are allowed to access the various resources or services hosted by the Service Providers. The aim of an access control system is to protect the system resources against unauthorized or illegal access by the users. A secure and effective access control system facilitates resource sharing also. An effective access control system keeps the confidentiality, integrity and availability of the resources. An access control mechanism includes the processes of identification, authentication and the authorization. The identification process includes associating an identity with the users of the system and the authentication process verifies the identity of the users. The authorization process follows the authentication process and it determines the access rights of various users towards different resources in the system. Since different users have varying access rights associated with the resources in the system, effective access control mechanism is required to maintain the security of the resources.

In open service-oriented systems, in many cases, the service providers and the service consumers are not known to each other beforehand. Since they do not have a pre-established trust value between them, the authentication of the users is to be carried out by the service providers in order to verify their access privileges. Trust establishment between consumers, Service Providers and Identity Providers also assumes very high importance in the current scenario. As the development of the internet is very fast, there are increasing demands for the cooperation of distributed, heterogeneous, and autonomous organizations, emphasizing the need for the development of an efficient access control model. In open distributed systems, secure authentication and authorization processes are required before access privileges are granted to the users.

A. Cloud Federation

Cloud Federation is an association of different Cloud Service Providers. In the standard Cloud Computing model, a client gets the required services from a single Cloud Service Provider or data centre, and this approach has several challenges associated with it. Due to some reasons, if a CSP cannot handle the service requests initiated from the cloud customers, it can leave several customers who depend on that service provider, without access to the required resources and services. Also, this approach of depending on a single cloud data centre, at times makes it difficult to ensure the adequate responsiveness and QoS to the clients. In reality, the Cloud Service Providers have a finite amount of resources with them. Also, it cannot lose an important customer because of the lack of available resources at the moment and thereby not being able to cater to the needs of that customer. To overcome these limitations, CSPs got together as a federation. For many service providers, in order to meet the dynamic and unpredictable user requirements, cooperation with other service providers is an option. This cooperation can be utilized to access resources and services from other partners in the federation to deliver the required QoS to the customers. The CSPs in the federation can share the cloud infrastructure between them in order to have better resource utilization and improved QoS to the cloud consumers. Thus, the primary reasons for the formation of Cloud Federation are better resource utilization and the increased revenues for the CSPs, and the availability of reliable cloud services with no vendor lock-in for the cloud consumers.

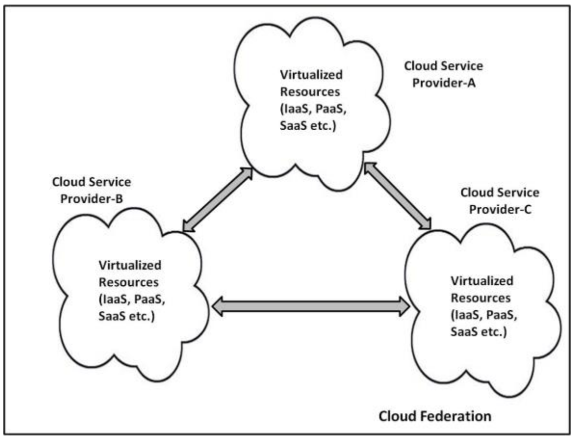
Virtualized Resources (IaaS, PaaS, SaaS etc.)
Cloud Service Provider-A
Cloud Service Provider-B
Virtualized Resources (IaaS, PaaS, SaaS etc.)
Cloud Service Provider-C
Virtualized Resources (IaaS, PaaS, SaaS etc.)
Cloud Federation

Fig. 1. Overview of the Cloud Federation

The overview of the Cloud Federation is shown in the Fig. 1. As described in the figure, Cloud Federation helps to have a collection or pool of resources from different CSPs, and this aggregation of resources can take place at different service levels of the Cloud Computing stack such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) levels to have a pool of programs (code), data, platform, compute, storage and network resources which could be utilized by the cloud users across the globe. Thus, Cloud Federation enables a CSP to have a single large pool of homogeneous or heterogeneous computing resources (for eg. Virtual Machines (VMs) which are federated from different CSPs). There are different types of Cloud Federation [2]. It could be categorized into horizontal as well as vertical federations. Horizontal Federation refers to the aggregation of resources among the Cloud Service Providers at a particular service delivery model such as IaaS, PaaS or SaaS, whereas the Vertical Federation refers to the association of CSPs where one type of service model of a CSP uses services from other CSPs to form another service model. For e.g., the PaaS service of a CSP uses IaaS services from other CSPs in the federation.

Hence, the motivating factors for the adoption of Cloud Federation paradigm are the enhanced collaboration between the various Cloud Service Providers and the improved Quality of Service delivered to the cloud consumers. The collaboration ensures the support in terms of information and resource sharing among the partners in the Cloud Federation environment. The Quality of Service includes factors such as availability, uptime, interoperability and response time of the services delivered by the various Cloud Service Providers.

B. Single Sign-On (SSO)

As there are different services available in the cloud environment, if all the variety of services have their own authentication mechanism, the various cloud users will have to log in and verify their credentials each and every time they use a different set of services, even though the services are from the same Cloud Service Provider. This gives rise to the multiple credentials problem. To overcome this problem, we make use of the Single Sign-On (SSO) mechanism in the authentication process.

Single Sign-On (SSO) is a mechanism used for authentication in which a service consumer is required to be authenticated only once while accessing various services from multiple service providers, or when accessing multiple services from the same service provider. The process of SSO involves the association between the following entities: Cloud Service Consumer (CSC), Relying Party or Cloud Service Provider (CSP) and the Identity Provider (IdP). The CSP and the IdP have mutual trust established between them. That is, IdP offers Identity Management functions to the CSP. Before accessing the services from the CSP, the Cloud Service Consumer has to get authenticated as a valid user from the IdP. Since the CSP and IdP are part of the association, and they have mutual trust with each other, the user is allowed to access the services from the CSP after successful authentication. Hence, the Identity Federation supports Single Sign-On as the users are able to access multiple services from the same or different CSPs using the identity token issued by the Identity Provider. Because of this association, the service providers can concentrate more on their core services, since the identity management operations are taken care of by the Identity Providers.

C. SSO in Cloud Federation

Even though the cloud computing paradigm promises to offer infinite resources, in reality, the resources with each and every Cloud Service Provider are finite. Sometimes, there could be requests from the cloud users for rapid increase in the usage of their computing, memory or network resources due to reasons such as failure of a server or data centre, or to meet the sudden request made by their own clients. In this case, when the Cloud Service Provider runs out of resources, the service provider can get the required services from partners in the Cloud Federation, if the CSP is a part of a federation. This scenario underlines the urgent requirement for the proper identity management in the Cloud Federation. Federated Identity Management approach (like Single Sign-On authentication) is required for the current cloud federation scenario. The users in a cloud federation don't need to use separate credentials for each Cloud Service Provider or service they subscribe to; instead, they can have the identity tokens issued by the Identity Provider (Ping Identity, Symplified etc.). They can submit the security tokens (normally SAML assertions) issued by the Identity Provider, to the service providers in the cloud federation. This approach is both efficient and secure, and relieves the users of the multiple credentials problem when accessing services from multiple CSPs.

Thus, in the Single Sign-On (SSO) mechanism in Cloud Federation, a user needs to verify his credentials and get authenticated himself only once during an active session of accessing cloud services. The cloud users are benefitted in such a way that they will be able to access all the related services that are offered by the single CSP or multiple CSPs seamlessly without the need of providing the identity credentials again and again for accessing the services. It also helps in increasing the productivity of the users as well as the developers by reducing the number of times a user must login, also reducing the number of credentials one has to remember. The overall view of the SSO in Cloud Federation is shown in the Fig. 2.

D. Motivation

In order to have a reliable and scalable architecture for the Cloud Federation which is in its inception stages, many issues still remain to be solved. For achieving secure and effective collaboration between heterogeneous cloud partners, issues related to the Federated Identity Management (FIM) need to be solved as a primary step, in order to maintain the confidentiality, integrity and the availability of the information or resources in the Cloud Federation environment.

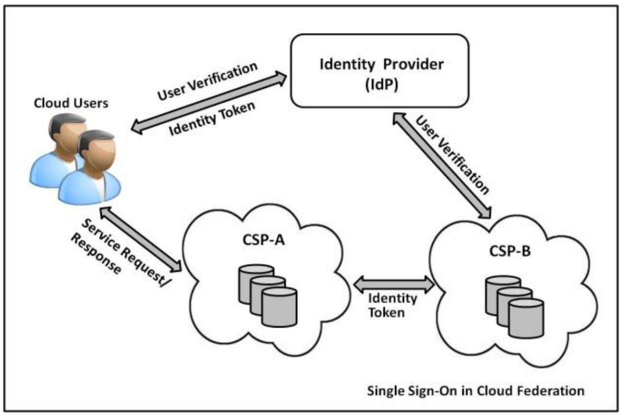

Fig. 2. Overview of the Single Sign-On (SSO) in Cloud Federation

CloudSim is a generalized simulation framework which helps in modeling and simulating large cloud infrastructure on a single computing node as proposed by Rajkumar Buyya et al. [3]. It has features which can be extended to model the Cloud Federation used for studying the Cloudbursts. Even though various scheduling and provisioning policies can be designed using the CloudSim, as of now, the simulator lacks effective user authentication and authorization methods with it. Hence, in this work, we focus on implementing the SSO authentication of cloud users in the Cloud Federation environment using the CloudSim toolkit. We discuss the design and implementation of the SSO mechanism, providing the services such as confidentiality, integrity and non-repudiation of the identity information.

Several important factors come into play when forming a Cloud Federation, such as SLA negotiation, trust establishment between the Cloud Providers etc. Since our work focuses on the SSO approach in an existing federation, these topics are out of the scope of our paper. In this work, our scope of the federation is limited to the IaaS level and we deal with the resource requests for VMs in order to show the SSO approach adopted.

The rest of this paper is organized into the following sections. The Section II presents the literature survey related to our work. The Section III explains the approach of SSO in the Cloud Federation as implemented in this work. The Section IV explains the workflow model of the SSO in this paper. Experimental setup, results and analysis are shown in the Section V, and finally, the Section VI draws the conclusions and the future works.

II. Related Works

Many works related to the identity management and the Single Sign-On in cloud computing domain have been published, and the relevant papers are discussed in this section. In [4], the issue of identity management in the cloud computing scenario is discussed. They also show the privacy issues associated with cloud computing. The paper gives a review of the existing approaches in identity management in cloud computing. In this work, loss of user control, lack of trust between various entities and the multitenancy issues are considered as the major problems in the cloud computing model.

Fugkeaw et al. [5] have presented an SSO model based on Multi-Agent System (MAS) and strong authentication based on PKI. Multi-Agent System is a technique in which a group of systems solves the problem by working together which would not have been solved, had the systems worked independently. However, this mechanism could be improved with respect to the access control and security checks during the transmission of messages. User authorization is also not considered as part of this work. Fugkeaw et al. [6] have extended their previous work in order to utilize the services of distributed Role Based Access Control (dRBAC) model. Zwattendorfer et al. [7] made the use of STORK (Secure Identity Across Borders Linked) framework for an interoperability between electronic IDs (eIDs) of various nations within Europe for

SSO. But the scope of this framework is limited only to the nations having electronic IDs, and hence it is not globally scalable.

Guilin et al. [8] present a security analysis of various Single Sign-On mechanisms in the distributed networks. They have identified various flaws such as impersonation of a user, impersonation of a Service Provider etc. during the authentication process. They have also proposed a secure scheme by using RSA-based signatures. David Argles et al. [9] provide a different approach for secure Single Sign-On mechanism in which they have used QR codes for achieving the Single Sign-On. Since many Single Sign-On approaches aren't secure against real-time attacks, this paper presents an anti-phishing Single Sign-On solution which is resistant against active attacks and phishing attacks. Major assumption made in this paper is that all the users have smart phones with camera feature for the scanning of QR codes.

Celesti et al. [10] have implemented a three-phase mechanism for cross-cloud Single Sign-On authentication. The three phases discussed in this paper are Discovery, Match-Making and Authentication. They have focused mainly on authentication in their work and tried to solve the issue by defining their own Security Assertions Markup Language (SAML) profile. They also extended their work in [11] by developing a CLoud Enabled Virtual EnviRonment (CLEVER). Also, in this work they have only focused on a single Identity Provider rather than having multiple Identity Providers. Chin-Chen Chang et al. [12] present a secure Single Sign-On mechanism for computers which are distributed over the network where the devices in the network may be mobile. For access control, this paper uses unitary tokens based on secure hash functions, nonce values and public key encryption techniques.

Basics of the authentication process have been explained in [13] discussing Single Factor Authentication, Two-Factor Authentication and Multi Factor Authentication based on three factors such as something you know (passwords, PINs etc.), something you have (tokens, smart cards etc.) and something you are (DNA, fingerprints etc.). It discusses the common authentication techniques such as password based authentication, biometric based authentication and also a combination of these techniques. National Institute of Standards and Technology (NIST) [14] have mentioned the thorough guidelines or recommendations for protecting the confidentiality of Personally Identifiable Information (PII). Recently, the authors in the network security domain have adopted MAS for network security. Kumar et al. [15] have proposed the MAS based network security for authentication and authorization. They have implemented an Adaptive Agent Architecture based on MAS. Chang et al. [16] discuss the various issues for authentication and access control such as ensuring security of the user's data. Secure authentication for mobile users is discussed in [17] using Consolidated Authentication Models (CAM).

Nowadays, many of the systems on the internet are still using the password-based authentication or Password Authentication Scheme (PAS). It is still the most accepted mechanism in many cases for distinguishing the legitimate users from the malicious or illegitimate ones. Therefore, lots of research is still going on in this area for providing secure and dynamic authentication schemes. Chang et al. [18] have identified the flaws in the Quadratic Residue approach and Lin et al. [19] have tried to enhance the security of the Optimal Strong Authentication Password protocol which was earlier vulnerable to stolen-verifier attack. Our approach adopted in this paper is able to resist this attack because we have used FHMQV which is resistant against impersonation and Man-in-the-Middle (MITM) attacks, even if session keys are leaked. Leung et al. [20] present various security flaws in the authentication scheme using smart cards such as the off-line password guessing attacks, impersonation attacks, the intruder-in-the-middle attacks and the denial-of-service attacks.

In [21], the authors propose the architecture for Federated Identity Management in a scenario similar to the Inter-Cloud environment. The work focuses on information or resource sharing across the cloud service models such as SaaS, PaaS and IaaS. The cloud federation is aimed more at vertical level, in which various SaaS providers and underlying PaaS/IaaS providers can collaborate or federate to form the heterogeneous Cloud federation. This work does not focus on the federation at the horizontal level such as between various Infrastructure providers.

The work in [22] discusses the inter-cloud security considerations. In [23], the authors propose an authentication mechanism for inter-cloud environments using SAML profile over XMPP. The architecture discussed in this work is based on the internet scale. The work shown in [24] discusses a Federated Identity Management approach using Hierarchical Identity-Based Cryptography. This mechanism makes collaboration possible within a Hybrid Cloud, which is a combination of private and public clouds. The work focuses on the Private Key Generator (PKG) hierarchical model. This model assumes a root PKG for managing the entire Hybrid Cloud. The root PKG generates private keys for PKGs of the member Clouds associated with the hybrid cloud. Before applying this model to the inter-cloud scenario, issues regarding the control of the root PKG should be solved.

A robust remote authentication scheme is presented in [25]. But, its major drawbacks are higher computation and communication costs and also its inability to prevent the insider attacks. In order to overcome the problems of guessing attacks in the authentication schemes, Lee et al. [26] have proposed an authentication scheme which uses one-way hash functions. We have also used hashing for a similar purpose in our work. Chen et al. [27] propose an approach for secure and dynamic PAS scheme which solves the issue of authentication failures dynamically by using the theory of quadratic residue. But, this paper does not deal with secure communication between the entities which we have handled in our work. Ren et al. [28] also proposed a dynamic approach for PAS. It uses One-Time Passwords (OTP) unlike traditional static passwords. This OTP is used for authentication along with the user's private identity information and also considering the current authenticating time. Major benefits of this work are its resistance to various real time attacks in the network such as the MITM, replay attacks etc. At the same time, the method adopted is still vulnerable to types of phishing attacks which aren’t possible in our approach.

Before we adopt new technology and practices in the Cloud Computing environment, it is highly necessary to model, simulate and study the new technologies for evaluating their performance and also to assess their security features. As mentioned earlier, one of the popular tools used for modeling, simulation and experimentation of cloud computing services is the CloudSim. The layered architecture of CloudSim is shown in the Fig. 3 [3]. But, as per our knowledge, authentication and authorization with Single Sign-On (SSO) has not been addressed in the CloudSim toolkit. As security is absolutely necessary in today’s world with every new technology, we propose our SSO mechanism in the Cloud Federation, in order to aid the research community in simulating the Cloud Computing services with the required security features. Hence, in our work, we have integrated the SSO authentication and the authorization processes in the Cloud Federation environment using the CloudSim.

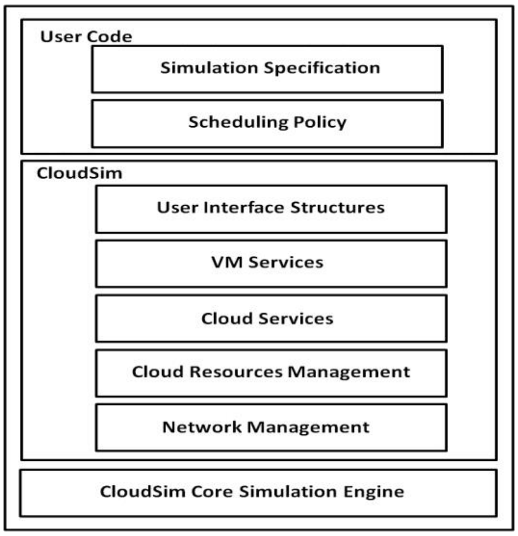

Fig. 3. Layered CloudSim Architecture [3]

III. SSO In Cloud Federation Using Cloudsim

Single Sign-On (SSO) approaches can be categorized based on different parameters such as how and where the mechanism is used, the type of credentials used for authentication etc. [29]. For example, the ter ”where” defines the domains in which the SSO is applied to access the services such as the intranet, extranet or the internet. The parameter ”how” defines whether the architecture of the Single Sign-On mechanism is simple or complex. In the complex architecture, it deals with multiple Identity Providers for supporting the identity of the users. In this case, each user can have multiple set of credentials. The ”credentials” used for authentication can be of different types such as ”tokens” or ”certificates”. In our simulation, we have implemented the SSO mechanism where multiple Identity Providers are used for the management and administration of user accounts, and also the users can have accounts with different Identity Providers at the same time. In our work, the credential used for SSO mechanism in the Cloud Federation scenario is the ”token”.

The overall flow of the Single Sign-On approach implemented in our work is as shown in the Fig. 4. In the figure, in order to access the cloud services in the federation, the cloud user submits the credentials and also the details of the Identity Provider (IdP) supported by the CSP. The CSP verifies the identity token by contacting the IdP mentioned (provided that this IdP is trusted by the CSP considered). Upon successful authentication, the user request is processed to verify the access request of the user. If the verification of the authorization is successful, the local resources are allocated to the user. If the local resources are insufficient to meet the client’s request, this CSP contacts other CSPs in the federation for the allocation of the required resources. Upon receiving the resource request along with the corresponding identity token, the other CSPs in the federation verify the identity of the user by contacting the corresponding IdP. In this case, the user does not need to enter the identity credentials each time he gets resources from the cloud partners in the federation. The identity credentials are submitted only once to the first CSP alone, while making the access request. Thus, the proposed model has the following main components: 1) Cloud User 2) Cloud Service Provider (CSP) and 3) Identity Provider (IdP). In this experiment, whenever a cloud user wants to use the services from any of the Cloud Service Providers, he requires the following three processes.

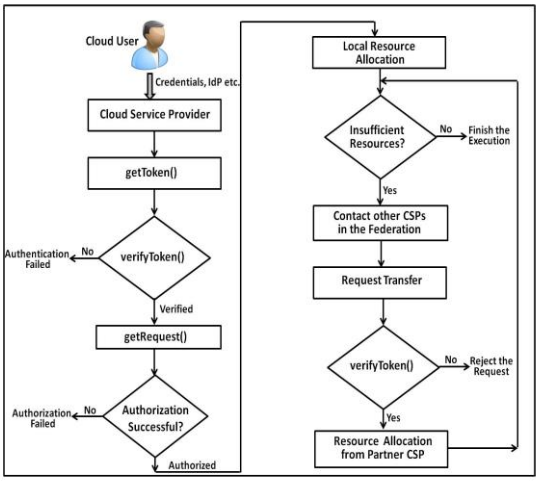

Fig. 4. Overall flow of the SSO in the Cloud Federation

A. Registration of the User with the Identity Provider (IdP)

In order to use the cloud services from the federation, the user has to register with any one of the supported Identity Providers for getting the identity token associated with him. This token is further used for authentication and authorization in the Single Sign-On (SSO) module. The flow diagram of this process is shown in the Fig. 5. As shown in the figure, in this process, the user provides his credentials such as the preferred username and password to the selected Identity Provider. The user's registration request is then redirected to that particular Identity Provider. On receipt of this request, the Identity Provider checks for duplicate and invalid entries such as username, credentials etc. Upon verification, if the Identity Provider finds that the particular user is new and valid, it calls the issueToken() method and generates a token for that user, and also stores the generated token in the database for subsequent verification.

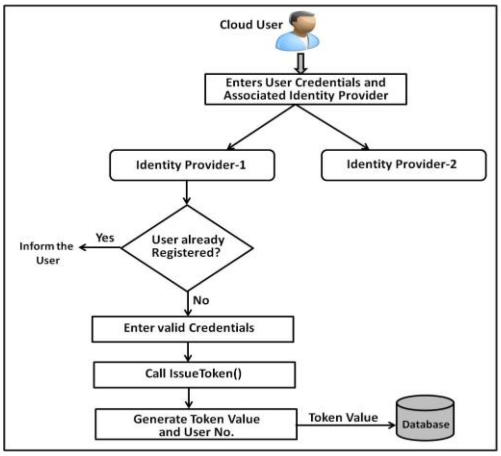

Fig. 5. User Registration with the IdP in the Cloud Federation

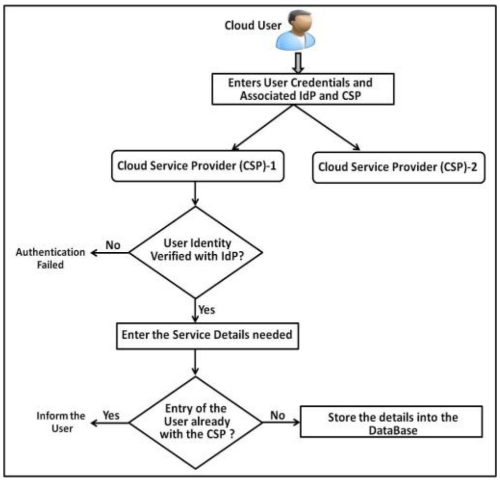
Cloud User
Enters User Credentials and Associated IdP and CSP
Cloud Service Provider (CSP)-1
Cloud Service Provider (CSP)-2
User Identity Verified with IdP?
No
Authentication Failed
Yes
Enter the Service Details needed
Entry of the User already with the CSP ?
Yes
Inform the User
No
Store the details into the DataBase

Fig. 6. User Registration with the CSP in the Cloud Federation

B. *Registration of the User with the Cloud Service Provider (CSP)*

For availing the services from any CSP in the federation, a user has to register with the corresponding Cloud Service Provider. This step is equivalent to negotiating an SLA with the CSP regarding the various QoS attributes of the service delivery. In our simulated experiment, the users negotiate the number and type of virtual machines, and also the access rights associated with the VMs. The flow diagram of this process is shown in the Fig. 6. As shown in the figure, whenever the user requests for some service from a Cloud Service Provider, it must be verified that the user is registered with any one of the Identity Providers trusted by the CSP, such that the particular Identity Provider provides services to the Cloud Service Provider from which the user has requested service. On successful verification, the user enters the resource request details such as the number of virtual machines, type of virtual machines, access rights associated etc. Now, the user access request is verified with the *UserRights* table of the concerned CSP to ensure the validity of the entry, and then the details are entered into the database.

C. *Requesting services from the CSP*

After the above mentioned two steps, the user can submit his request to the Cloud Service Provider for availing the services. The flow diagram of the processing of the user's request is shown in the Fig. 7. As shown in the figure, whenever the user submits the details of the user credentials and Identity Provider to the Cloud Service Provider selected, while making the access request for the allocation of virtual machines, the identity of the user is verified by the CSP by contacting the corresponding Identity Provider. This step is necessary to provide the authentication of the user. Upon successful authentication, the user's request for virtual machines and other access rights are validated from the CSP's database, and depending upon the access rights allowed, the user's access request is either accepted or rejected. After the successful authentication and authorization, execution of the user's request starts. In case the CSP does not have enough resources to meet the resource request of the cloud user, the CSP in the federation requests resources from other CSPs and satisfies the user's request as shown in the Fig. 3. In our implementation, in this case, once the user is authenticated at a particular CSP, the access token from the CSP is transferred to other CSPs in the federation for accessing the cloud resources in the federation. That means, the same user is not required to submit the identity credentials again and again for accessing services from various CSPs in the federation.

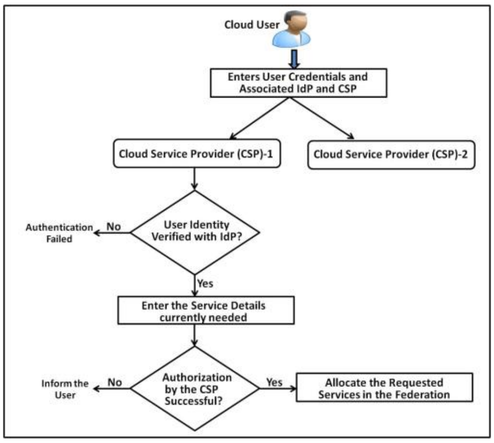
Cloud User
Enters User Credentials and Associated IdP and CSP
Cloud Service Provider (CSP)-1
Cloud Service Provider (CSP)-2
User Identity Verified with IdP?
No
Authentication Failed
Yes
Enter the Service Details currently needed
Authorization by the CSP Successful?
No
Inform the User
Yes
Allocate the Requested Services in the Federation

Fig. 7. Processing the Resource Request in the Cloud Federation

IV. Workflow Model Of The Single Sign-On Approach

The sequence of steps involved in the workflow of the implementation of SSO in the Cloud Federation is shown in the Fig. 8. In this figure, we have shown only two CSPs in the Cloud Federation. As shown in the figure, the various steps involved are:

1) The Cloud User wants to access the service hosted by the CSP-1, and submits the identity credentials to the CSP-1.
2) The CSP-1 contacts the associated Identity Provider (IdP) for the authentication of the user.
3) The CSP-1 gets the result of user verification from the IdP.
4) The user submits the service request for accessing the resources from the CSP-1.
5) User authorization is performed by the CSP-1 to decide whether to accept or reject the request.
6) The local resources (if available at the CSP-1) are allocated to the user.
7) The CSP-1 contacts the other CSP(s) in the federation (CSP-2), if the local resources are not sufficient to satisfy the user's request.

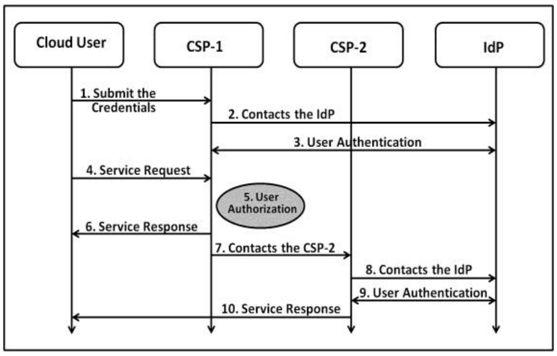

Fig. 8. Workflow model of the SSO in the Cloud Federation

8) The CSP-2 contacts the IdP for the authentication of the user.
9) The CSP-2 gets the result of user verification from the IdP.
10) The CSP-2 allocates the resources (if available) to the user after authorization.

V. Experimental Results

The primary objective of our experiment is to design and implement the functionality of the Single Sign-On and the authorization modules, and also to verify that they are working correctly in the Cloud Federation environment simulated using the CloudSim toolkit. Our test scenario consists of a number of Cloud Service Providers and multiple Identity Providers. The cloud users can have multiple accounts with different Identity Providers, and the Cloud Service Providers may use the services of one or more Identity Providers.

A. Experimental Setup

We have carried out the simulation experiments on a system with Intel (R) Core (TM) i7-3770, CPU 3.40 GHz, 8.00 GB RAM and 32-bit Operating System (Ubuntu 14.04). Softwares used for the implementation include CloudSim-3.0.3, Eclipse IDE version 3.8, MySQL Workbench Community (GPL) for Linux/Unix version 6.0.8 and Java version 1.7.0_55.

For implementing the SSO module and the Authorization module, we have used the Java programming language. We have used MySQL database to store the data related to the various users of the CSPs. Each Cloud Service Provider (CSP) has a table for storing the user's access rights which shows the access rights associated with a particular registered user, and this information is used during the authorization phase of dealing with the access request. Each Identity Provider (IdP) stores the user related data and the user credentials in the corresponding Identity Provider table. We also have a table in the database showing the mapping of which CSP uses the services of which Identity Provider.

In our implementation, for securing the data in transit such as during the transfer of the identity tokens of the cloud users between CSPs and also between CSP and IdP, we have used the Symmetric Key Encryption technique using Advanced Encryption Standard, AES-128. Also, we have used Fully Hashed Menezes-Qu-Vanstone (FHMQV) key sharing protocol for key exchange between the entities in the simulation. AES is a protocol mentioned in the set of standard protocols for security by the National Institute of Standards and Technology (NIST) [30] and the FHMQV protocol has its root in Diffie-Hellman (DH) protocol. The FHMQV protocol defines the Full Exponential Challenge Response (FXCR) and Full Dual exponential Challenge Response (FDCR) schemes which preserve the performance of the (H)MQV protocol, in addition to providing resistance against various attacks such as the impersonation attack, man-in-the-middle attack etc.

B. Results and Analysis

In order to test our approach, we have implemented the Cloud Federation scenario with 25 CSPs with each CSP having two heterogeneous hosts associated with them. The user makes the resource request to any CSP in the federation, and we have tested the access request in such a way that the access request made by the user cannot be met by a single CSP alone. In the federation set up simulated, if a CSP alone cannot handle the access request, the access request is transferred to other CSPs in the federation as we have already discussed.

The Fig. 9 shows the number of SSO involved in the simulation and the corresponding execution time associated with the user request. In the figure, we have shown the maximum number of SSO associated with a single access request of a user in the federation as 20. From the figure, it is seen that the average execution time taken for 20 SSO operations associated with the user request, involving 20 CSPs in the Cloud Federation is 2679 milliseconds, as observed in our simulation. Without SSO, as the number of times a user's request is transferred from one service provider to another increases, the number of logins he needs to perform also increases, thus increasing the response time for the access request. If we assume that, on an average, two seconds are required by a Cloud user to enter the username and the password at a CSP, then as the number of CSPs in the federation increases, the number of logins needed also increases and hence, the total time needed for user verification will be much higher than the time taken for the corresponding authentication using the SSO approach. Hence, this shows that the SSO approach reduces the average user response time considerably, besides providing the required security features. Also, by using the Single Sign-On mechanism, it reduces the load of the cloud users and developers in dealing with multiple credentials while accessing services from various CSPs in the federation.

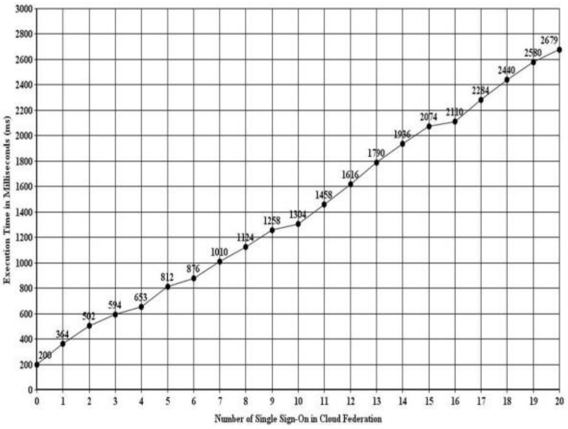

Fig. 9. Execution Time with SSO in the Cloud Federation

VI. Conclusion And Future Work

In this paper, we have implemented Single Sign-On in the Cloud Federation scenario using the CloudSim toolkit, considering multiple Identity Providers and Cloud Service Providers. We have also considered the security aspects of the data transferred between the various entities in the cloud federation during the SSO mechanism. The simulation results show that the SSO approach is highly beneficial while accessing multiple services from CSPs in the Cloud Federation, as it reduces the execution time of the user request for resources in the Cloud Federation. In this work, the processing of the request of the cloud users is done in a sequential manner by the CSPs in the federation. As a future work, we plan to include the parallel processing of the user requests by analyzing the resource requirements and the capacities of other Cloud Service Providers in the federation dynamically, and executing the requests in parallel incorporating the SSO approach.

References

[1] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang and Karim Djemame, “Security Risks and their Management in Cloud Computing”, in 4th IEEE International Conference on Cloud Computing Technology and Science, 2012, pp. 121-128.

[2] David Bermbach, Tobias Kurze and Stefan Tai, “Cloud Federation: Effects of Federated Compute Resources on Quality of Service and Cost”, in IEEE International Conference on Cloud Engineering, 2013, pp. 31-37.

[3] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C’esar A. F. De Rose and Rajkumar Buyya, “CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms”, Software-Practice & Experience 41 (2010) pp. 23-50.

[4] Kumar Gunjan, G. Sahoo and R. K. Tiwari, *”Identity Management in Cloud Computing-A Review”*, International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, Vol.1, Issue 4, June-2012, pp. 1-5.

[5] Somchart Fugkeaw, Piyawit Manpanpanich and Sekpon Juntapremjitt, “A Robust Single Sign-On Model based on Multi-Agent System and PKI”, in 6th International Conference on Networking, 2007, pp. 101-101.

[6] Somchart Fugkeaw, Piyawit Manpanpanich and Sekpon Juntapremjitt, “An SSO-capable Distributed RBAC Model with High Availability across Administrative Domain”, in 22nd International Conference on Advanced Information Networking and Applications - Workshops, 2008, pp. 121-126.

[7] Bernd Zwattendorfer and Arne Tauber, “Secure Cross-Cloud Single Sign-On (SSO) using eIDs”, in 7th International Conference for Internet Technology and Secured Transactions, 2012, pp. 150-155.

[8] Guilin Wang, Jiangshan Yu, and Qi Xie, *“Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks”*, IEEE Transactions on Industrial Informatics 9 (2013) 294-302.

[9] Syamantak Mukhopadhyay and David Argles, *“An Anti-Phishing mechanism for Single Sign-On based on QR-Code”*, in International Conference on Information Society (i-Society), 2011, pp. 505-508.

[10] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, *“Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication”*, in Second International Conference on Advances in Future Internet, 2010, pp. 94-101.

[11] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, *“Federation Establishment between CLEVER Clouds through a SAML SSO Authentication Profile”*, International Journal on Advances in Internet Technology 4 (2011) pp. 14-27.

[12] Chin-Chen Chang and Chia-Yin Lee, *“A Secure Single Sign-On Mechanism for Distributed Computer Networks”*, IEEE Transactions on Industrial Electronics 59 (2012) pp. 629-637.

[13] Sabi Goriawala, *“Authentication and Access Control: Selecting the Appropriate Authentication Method for Your Organization”*, SmartSignIn (www.smartsignin.com), 2013.

[14] Erika McCallister, Tim Grance and Karen Scarfone, *“Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”*, in NIST Special Publication 800-122, National Technical Information Service, Springfield, VA, May 1985.

[15] Sanjeev Kumar and Philip R. Cohen, *“Towards a Fault-Tolerant Multi-Agent System Architecture”*, in Proc. of Autonomous Agent, 2000, pp.459-466.

[16] Hyokyung Chang and Euiin Choi, *“User Authentication in Cloud Computing”*, in 2nd International conference on Ubiquitous Computing and Multimedia Applications, 2011, pp. 338-342.

[17] Jaejung Kim and Seng-phil Hong, *“A Consolidated Authentication Model in Cloud Computing Environments”*, International Journal of Multimedia and Ubiquitous Engineering 7 (2012) pp. 151-160.

[18] C. C. Chang and Y. F. Chang, *“Yet Another Attack on a Password Authentication System”*, in Proc. of 18th Inter

national Conference on Advanced Information Networking and Application, 2004, pp. 170-173.

[19] C. W. Lin, J. J. Shen and M. S. Hwang, *“Security enhancement for Optimal Strong-Password Authentication Protocol”*, Operating system Review 37(2) (2003) pp. 7-12.

[20] K. C. Leung, L. M. Cheng, A. S. Fong and C. K. Chen, *“Cryptanalysis of a remote user authentication scheme using smart cards*, IEEE Trans. Consumer Electronic 49 (2003) pp. 1243-1245.

[21] M Stihler, A O Santin, A L Marcon and J da Silva Fraga, “*Integral Federated Identity Management for Cloud Computing*”, In 5th International Conference on New Technologies, Mobility and Security (NTMS) Proceedings, 2012, pp. 1–5.

[22] D Bernstein and D Vij, “*Intercloud Security Considerations*”, In Second IEEE International Conference on Cloud Computing Technology and Science (CloudCom) Proceedings, 2010, pp. 537–544.

[23] D Bernstein and D Vij, “*Intercloud Directory and Exchange Protocol Detail using XMPP and RDF*”, In 6th IEEE World Congress on Services (SERVICES-1) Proceedings, 2010, pp. 431–438.

[24] L Yan, C Rong and G Zhao, “*Strengthen Cloud Computing Security with Federal Identity Management using Hierarchical Identity-based Cryptography*”, In Cloud Computing, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 5931 (2009), pp. 167–177.

[25] C. Fan, Y. Chan and Z. Zhang, *“Robust Remote Authentication with Smart Cards”*, Computers and Security 24 (2005) pp. 619-628.

[26] C. C. Lee, L. H. Li and M. S. Hwang, *“A Remote User Authentication Scheme Using Hash Functions”*, ACM Operating Systems Review 36 (2002) pp. 23-29.

[27] C. Y. Chen and C. Y. Gun, *“A Fair and Dynamic Password Authentication System”*, in 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011, pp. 4505-4509.

[28] Xuguang Ren and Xin-Wen Wu, *“A Novel Dynamic User Authentication Scheme”*, in International Symposium on Communications and Information Technologies (ISCIT), 2012, pp. 713-717.

[29] V. Radha and D. Hitha Reddy, *“A Survey on Single Sign-On Techniques”*, in 2nd International Conference on Computer, Communication, Control and Information Technology (C3IT-2012) on February 25 - 26, 2012, pp. 134-139.

[30] National Institute of Standards and Technology, An agency of U.S. Department of Commerce [Online]. Available: *http://www.nist.gov/.*

Authors’ Profiles

Manoj V. Thomas is currently pursuing Ph.D in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India. He obtained his Bachelor of Technology from RIT, Kottyam, Kerala and Master of Technology from NITK, Surathkal with First Rank and Gold Medal. He has more than 10 years of teaching experience and he is a Life Member of Computer Society of India. His areas of interests include Computer Networks, Cloud Computing and Cloud Security.

Anand Dhole is currently pursuing M.Tech in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India. He obtained his Bachelor of Technology from SGGSIET, Nanded, Maharashtra. He has 2 years of Industry experience and his areas of interests include Database Management and Cloud Security.

K. ChandraSekaran is currently Professor in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, having 26 years of experience. He has more than 120 research papers published in various reputed International journals, conferences which include IEEE, ACM, Springer etc. He has received best paper awards and best teacher awards. He serves as a member of various reputed societies, including IEEE (Senior member), ACM (Senior Member), CSI, ISTE and Association of British Scholars (ABS). He is also a member in IEEE Computer Society’s Cloud Computing STC (Special Technical Community). His areas of interest include Computer Networks, Distributed Computing (includes Cloud Computing and Security) and Business Computing and Information Systems Management.

How to cite this paper: Manoj V. Thomas, Anand Dhole, K. Chandrasekaran,"Single Sign-On in Cloud Federation using CloudSim", IJCNIS, vol.7, no.6, pp.50-58, 2015.DOI: 10.5815/ijcnis.2015.06.06