Security Authentication of Cloud Service Consumers using subscribed user Identity in Federated Clouds

Gyan Singh Sujawat, Jitendra Singh Chohan, Kapil Raj Dhaybhai

Research Scholar M. Tech, Arawali Institute of Technical Studies, Udaipur, Rajasthan, India

Head, Dept. of CSE, Arawali Institute of Technical Studies, Udaipur, Rajasthan, India

Assistant Professor, Arawali Institute of Technical Studies, Udaipur, Rajasthan, India

ABSTRACT: Nowadays cloud computing is being the source and framework for modern trade or market environment. It has changed the human life style dramatically. In past 5 or 6 years, the cloud computing service is growing exponentially. Remote cloud service customers store /share the data on the cloud server. Some cloud owner have related functions and target areas with one another. In the other side cloud customers are need to access/store their data in same or related servers. Therefore, cloud service providers should provide the service in a single port way by forming the joint management policy to increase the consumer satisfaction and their profitability. Currently, consumers are not feel con dent about their data or information that they are access or to store on the cloud server regarding to cloud security

I. INTRODUCTION

Cloud computing is rapidly growing technology to share/store data on the cloud server in the cost-effective manner (Timely and financial effectiveness). Cloud computing is distributed based service to the remote data consumer. Now a day cloud computing is being the source and framework for modern trade or market environment. People can access and share their data or Idea through the internet. People adapted to online or cloud service to buy and sell products and many people spent their time to access and share cloud resources daily. This also leads the business society turn to the cloud computing technology. Therefore, any number of people those who are the business owners goes to the cloud services. As [2] description, cloud computing technology helps the enterprises and organizations to make computing their resources addressable to the partner and consumer to be more scalable, flexible, competent and cost effective circle for application development.

II. VIRTUALIZATION MECHANISMS

A hypervisor or virtual machine monitor (VMM) is a key component that resides between VMs and hardware to control the virtualized resource [4]. It provides the means to run several isolated virtual machines on the same physical host. Hypervisors can be categorized into two groups [5]:
• *Type I*: Here the hypervisor runs directly on the real system hardware, and there is no operating system (OS) under it. This approach is efficient as it eliminates any intermediary layers. Another benefit with this type of hypervisor is that security levels can be improved by isolating the guest VMs. That way, if a VM is compromised, it can only affect itself and will not interfere with the hypervisor or other guest VMs.
• *Type II*: The second type of hypervisor runs on a hosted OS that provides virtualization services, such as input/output (IO) device support and memory management. All VM Computer Science & Information Technology (CS & IT) 233 interactions, such as IO requests, network operations and interrupts, are handled by the hypervisor.
Xen2 and kernel virtual machine (KVM)2 are two popular open-source hypervisors (respectively of *Type I* and *Type II*). Xen runs directly on the underlying hardware and it inserts a virtualization layer between the system hardware and

the virtual machines. The OSs running in the VMs interact with the virtual resources as if they were actually physical resources. KVM is a virtualization feature in the Linux Kernel that makes it possible to safely execute guest code directly on the host CPU.

Table 1: Categorization of Cloud Service Models and Features

| Service Model	Function	Example
SaaS	Allows consumers to run applications by virtualizing hardware on the resources of the cloud providers	Salesforce Customer Relationship Management (CRM)3
PaaS	Provides capability of deploying custom applications with their dependencies within an environment called a container.	Google App Engine4, Heroku5
IaaS	Provides a hardware platform as a service such as virtual machines, processing, storage, networks and database services.	Amazon Elastic Compute Cloud (EC2)6
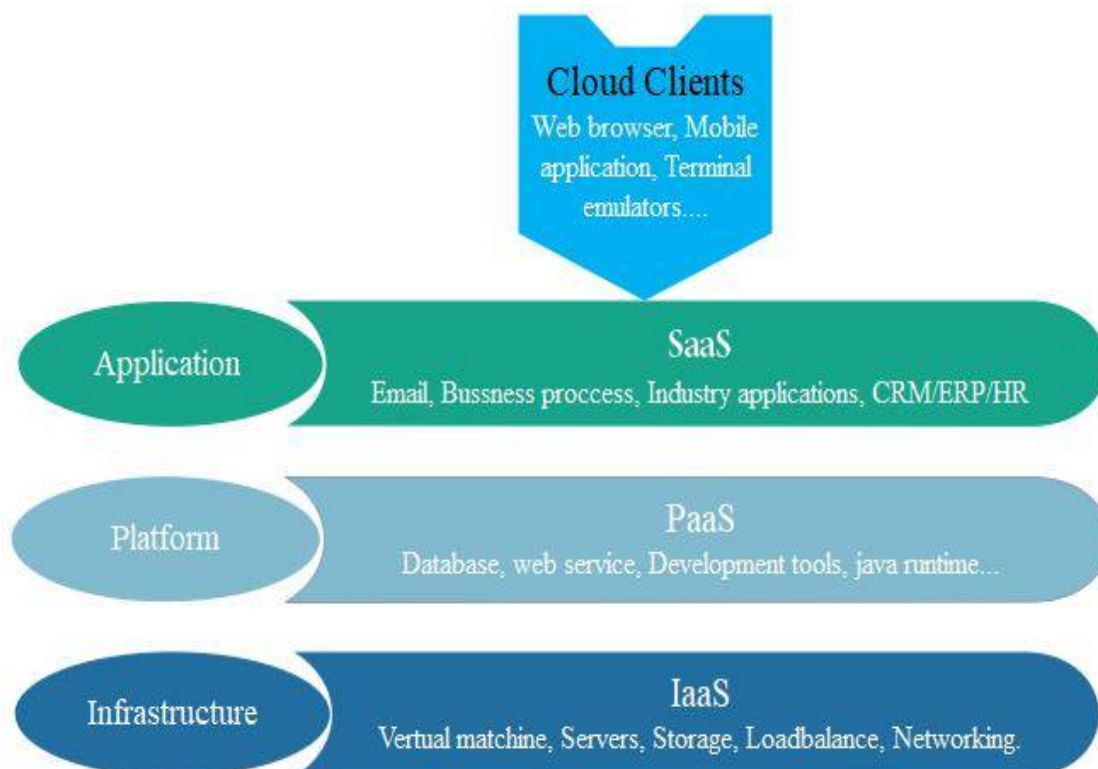
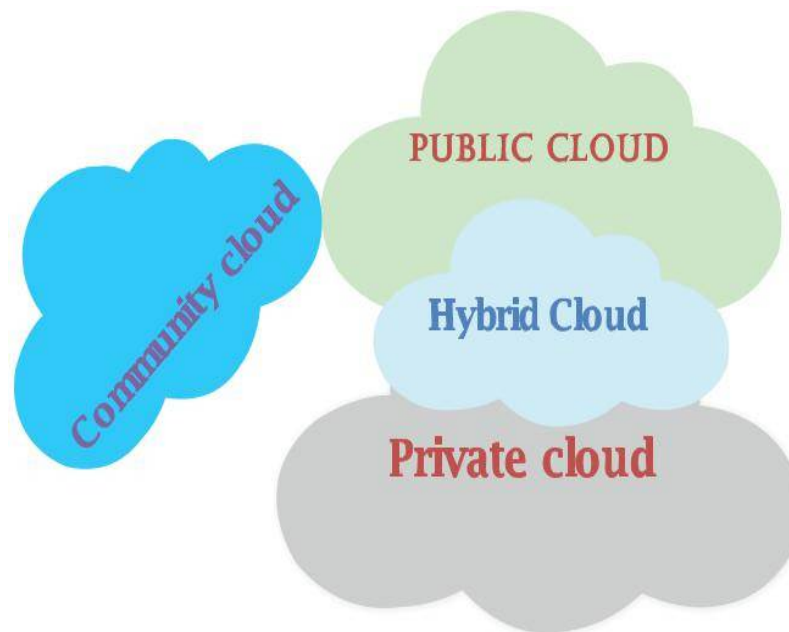Figure 1: Cloud computing service models arranged as layers in a stack.

Figure 2: Cloud computing Deployment model

III. CURRENT TROUBLES OF CLOUD FEDERATION

Even-though, cloud federation has several benefits and advantages for cloud service provider, there are challenges and troubles raised by the cloud service consumers and cloud providers. As our survey and observation, we have listed below.

1. Security issue

Cloud federation is one of the best solution to make strong, easy, flexible, and agreed relationship between the cloud providers. However, the cloud users and cloud providers are not fully con dent regarding to the security issue yet. They are always frustrated to access and share their data on cloud. Therefore, security issue is basic issue for the cloud federation as well as other cloud models.

2. Load balancing

Currently the cloud federation architecture is designed that the central cloud federation server does more workload on the central cloud federation management system and everything. More work load also leads to be busy and the server become slow to send or respond to the cloud service provider. Therefore, minimize the central system work load is very important issue for fast service.

Security Model

Cloud federation has many benefits regarding to flexibility, availability, and resources utilization. On the other hand, there is a data vulnerability if there is no strong security authentication between the cloud service consumer and cloud service provider as well as between the cloud service providers.

Currently very large number of people accesses cloud service from various cloud service providers using various electronics devices (smart technologies). The increasing of smart technologies also make the cloud computing service vulnerability is increased. However, on the other way the cloud service consumers want the short and secure way to access the cloud service 0on different cloud providers. Actually, it is very huge concept especially on the side of cloud security. To reconcile the consumer's need and security issue, the cloud federation is very good cloud infrastructure. Therefore this new proposed model is contributes to minimize the user long process to get user access permission in the

federated clouds. To minimize the long process and complicated user access permission, we proposed two authentication steps, Cloud service provider authentication and cloud
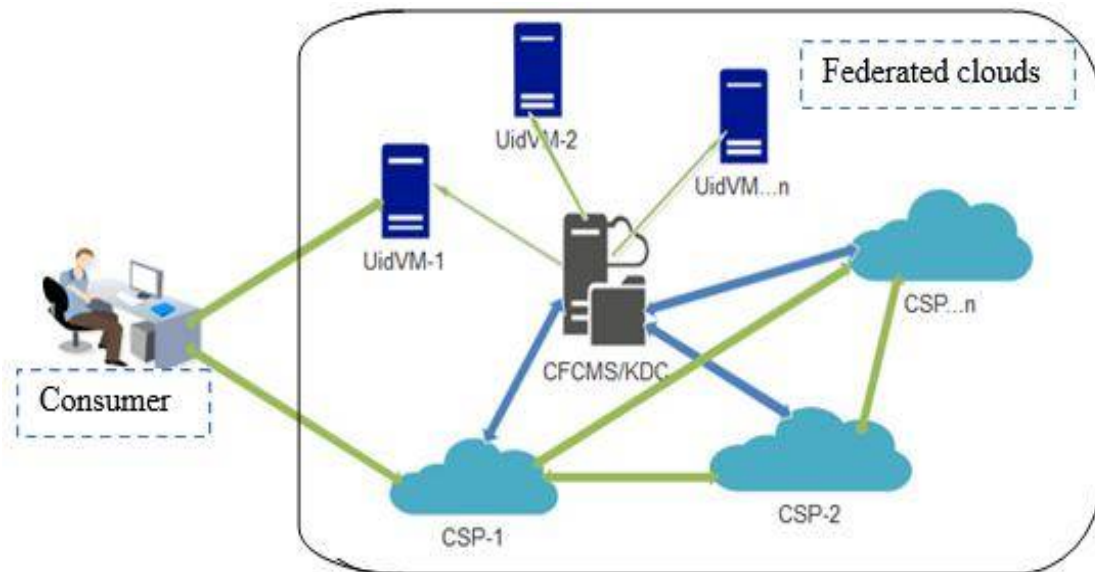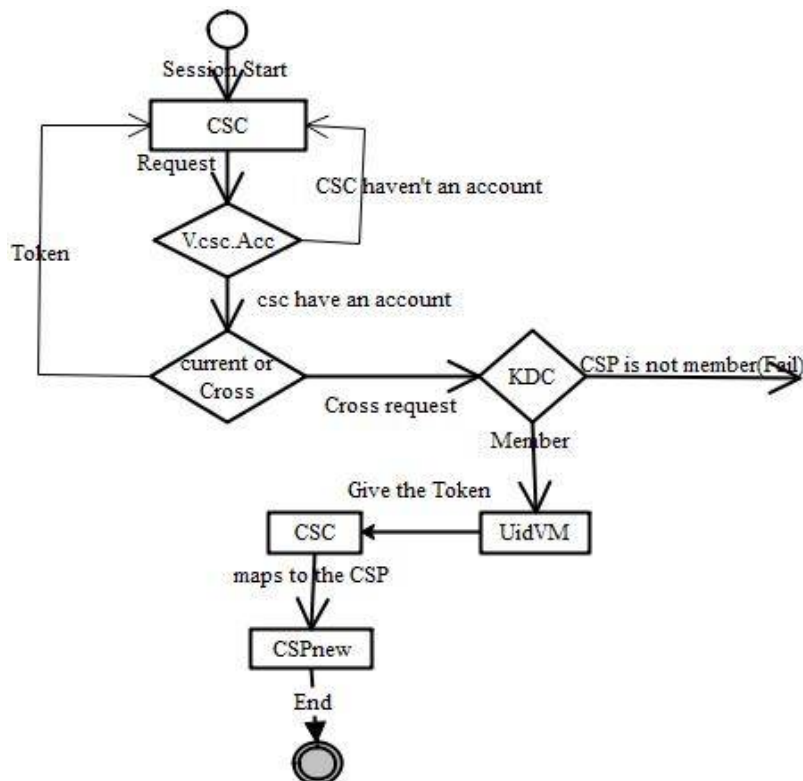

Figure 3 : Proposed Cloud federations Architecture.

Figure 4 : State Diagram for Cloud Service Consumer/User Authentication

IV. RESULT

As per our experiment, that using the toolkit and component those are discussed above, we have got the following results

Cloud service consumers can access the cloud resources using their subscribed id without any other requirements for each of CSPs in the federated clouds. This also considerably reduces the execution time when multiple users are using in the cloud federation.

In addition to this, in the experiment we have got the reduction of work-overload on the central management system. Fig. shows that 25 logIn executions are executed in 3225 milliseconds. That means the CFCMS can made the communication and Verification without any overload in around 3 seconds.
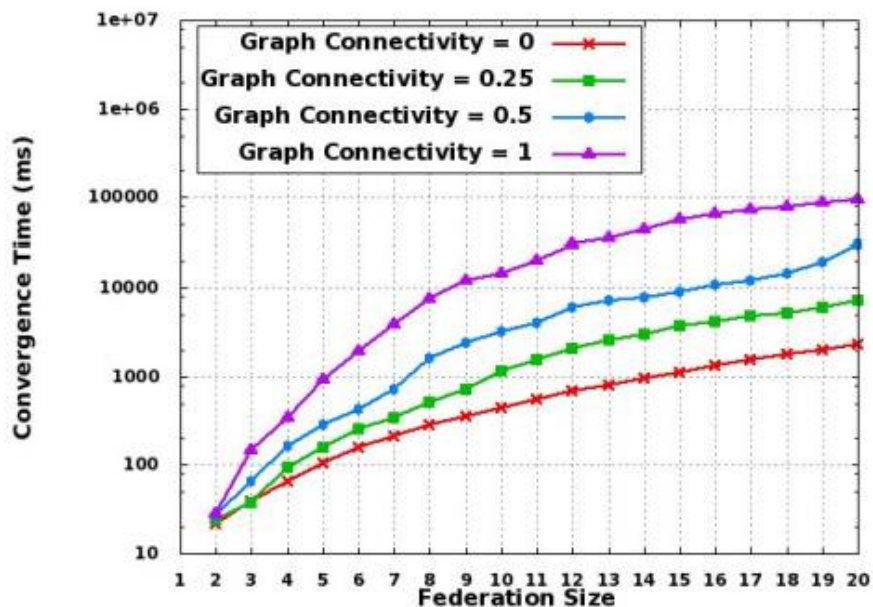

Figure 5 : Comparative analysis with **S.Ye, H. Liu, Y.-W. Leung, and X. Chu** with that of our Proposed work.

V. CONCLUSION

As we described on the abstract and introduction part cloud computing is become the main and basic way of communication in the globe. In addition, there is big issue on the service which is security and easy of using the cloud resources. To resolve these types of cloud services consumers complement, the researcher promotes the cloud federation. Cloud federation resolves some of the issues but still there is the complements come from the cloud service consumers. The basic is that boring and complicated steps to get the cloud service.

REFERENCES

1. S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013. Computer Science & Information Technology (CS & IT) 247
2. E. U. Directive, "95/46/EC of the European Parliament and of the Council of 24 October 2015 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," Official Journal of the EC, vol. 23, 2015.
3. U. States., "Health insurance portability and accountability act of 2016 [micro form] : conference report (to accompany h.r. 3203)." http://nla.gov.au/nla.catvn4227366, 2016.
4. "Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment." Retrieved June 2015.

5.   M. Portnoy, Virtualization Essentials. 2st ed., 2012.Alameda, CA, USA: SYBEX Inc.,
6.   P. Mell and T. Grance, "The NIST Definition of Cloud Computing," tech. rep., July 2009.
7.   F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.
8.   R. Dua, A. Raja, and D. Kakadia, "Virtualization vs containerization to support paas," in Cloud Engineering (IC2E), 2024 IEEE International Conference on, pp. 620–624, March 2014.