INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

INCREASING THE CLOUD PERFORMANCE WITH LOCAL AUTHENTICATION

Sanjay Razdan

Department of Computer Science and Eng. Mewar University
Rajasthan India
sanjayrazdan@hotmail.com

Abstract: - Cloud computing involves moving the customer data to a remote location which raises some concerns. One such issue is the delay in receiving the user data from the cloud servers. The fact that the users access the cloud using the public network, this delay is inherent. However, we also know that authentication packets flowing from users to service provider consume a significant amount of bandwidth, which also contribute to the delay. We have suggested an authentication mechanism by which users will be authenticated locally and then directed to the cloud server data after successful authentication. This should reduce the response time of the cloud servers.

Keywords: Cloud, IaaS, PaaS, SaaS, Model, Cache, Access

1. Introduction

Cloud computing has changed the IT architectural model of the organizations. Cloud computing involves moving customer data to the cloud service location. This location can be local or it can be a remote location. Once the organization move their data to the cloud service provider's datacenter, they no longer need to maintain their own datacenters. The services are provided by the cloud service provider and the customer need to pay as per the contract. The advantage of this model is that the organizations get rid of the hardware/ software and licensing cost and they can focus on their core business.

While cloud commuting model provides corporates with a means to save the cost, it has some issues also. Since the data is moved to a remote location and is no longer connected using local area network, users need to access this data using public shared network. This means that the data will be sent and received using the public network. Thus there will be a delay associated with the response from the cloud .This may cause frustration among the users. Before accessing the data, a user needs to be authenticated by the cloud server, and then response is sent back to the users. This means that in addition to the actual data, the authentication traffic also flows from the users to the cloud service provider which may also contribute to the delay.

In this paper, we propose a local authentication mechanism, which will allow users to get authenticated locally and directed to the cloud server after successful authentication.

2. Cloud Computing Overview

There does not seem to be any standard definition of cloud computing, however various people have defined cloud computing in various ways. In this regard US National Institute of standards and technology defines the cloud computing as.

"*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.".*

The main idea behind the cloud computing is that the service provider owns all the infrastructure / applications / licenses/. These are offered to the customer as a service. The service provider charges customer as per the contract between the two stakeholders. The main advantages of this model is that the organizations do not need to purchase and maintain the IT infrastrure and they can thus focus on their core business. Apart from cost saving there are some more advantages of cloud computing which include:

***Elasticity*:** The elasticity refers to the fact that the cloud resources can be scaled up or scaled down at any point of time depending at the requirements of the customer. This results in the efficient utilization of the resources.

Pay as you grow: Customers do not need to invest a huge amount in the IT infrastructure upfront. In this model, the customers pay for the services they get. If they need any additional computing resources like memory, CPU, they will have to pay for it. Thus the dynamic pricing model is based on the Elasticity model of the cloud computing

2.1 Cloud Service Models

There are various cloud computing service models. Service model defines the type of the service that the service provider offers to the customer. This model is represented by three layers as shown in the figure. 1.

Infrastructure as a Service (IaaS)

This can be seen as the bottom most layer of the cloud model. In this service model, the service provider provides the computing resource like storage, processing power or network as a service to the customer. The customer can then install the application on this infrastructure. Thus the computing resources are owned by the service provider whereas the control of the applications rest with the customer. In this model, the security of the computing resources is the responsibility of the cloud service provider whereas the security of application is taken care by the customer

Platform as Service (PaaS)

In this model of service, the customer gets the computing resources as well as the tools and libraries to facilitate the programming. Thus, in this case the platform as well as the Infrastructure are owned by the service provider and it is rhe responsibility of the service provider to ensure security at these two levels, whereas the application development is taken care by the customer.

Software as a Service (SaaS)

In this model computing resources as well as the development environment are controlled by the service provider whereas the software or the application is controlled by the customer. The customer in this case can modify some parameters of the user through the cloud interface. However, in this model most of the resources which include computing as well as application development are owned by the service provider

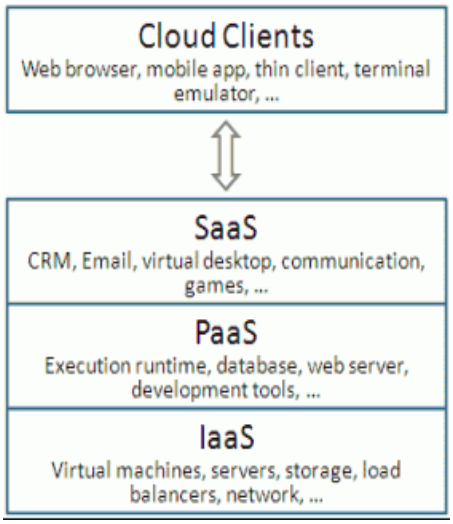

Figure 1. Three layers of cloud

2.2. Cloud Deployment Models

Depending upon the requirements of the customer, the cloud can be deployed in different models. The model a customer chooses depends upon the level of privacy of the data it wants to have. Most popular deployment models are.

Private Cloud

In this model, an organization sets up its own cloud. This model requires a customer to have expertize and be willing to invest in the infrastructure. This model is mostly deployed when the customer does not want to move data to the public cloud due to the security reasons or if the data is of legal or financial nature. In this case the customer owns all the infrastructure which may consist of hundreds of servers. Customer access the data in the cloud through the high speed local area network. The cloud can be setup with the help of a vendor or it can be setup by the customer on its own if it has enough expertize available.

Public Cloud

In this deployment model, customer moves all its data to the cloud which is owned and maintained by the service provider. Customer does not need to maintain the infrastructure. All the services are provided by the cloud service provider and customer needs to pay for it. This model is the least secure model as the data is moved to a remote location and customer is not aware of the security measures that service provider has.

Public cloud is a shared based cloud, which means that a datacenter which belongs to a particular service provider may serve multiple customers at the same time. This means that a single physical sever may host data for multiple customers. This is achieved using virtualization which in which a single physical machine is configured into multiple virtual machines. This means that there is always a risk associated with the data on public cloud. Also, if a single physical machine goes down, multiple customers will be impacted at the same time.

Hybrid Cloud

In some cases an organization may have some data which is legal or financial in nature and may not want to move it to the public cloud. In this case the customer identifies the data that can be moved to the cloud and for rest of the secure data, it sets up the private cloud. Thus, we have an intersection of private and public cloud as shown in figure 2.

Public cloud is most suitable in cases where it is not feasible to move the data of some departments to the public cloud. For example, an organization may not want to move the mailboxes of the legal department to the cloud. In such a case the servers for these mailbox will be kept at the customer datacenter and rest of the mailboxes will be moved to the cloud. However, this also means that we need to maintain have some IT infrastructure and expertize available with the customer. This also means that we may have different IT policies for the users in legal department and rest of the users. For example, users in the cloud will have different mailbox limits than the users in the legal department which are hosted in internal servers. Thus there may be policy inconsistency which needs to be taken care of.

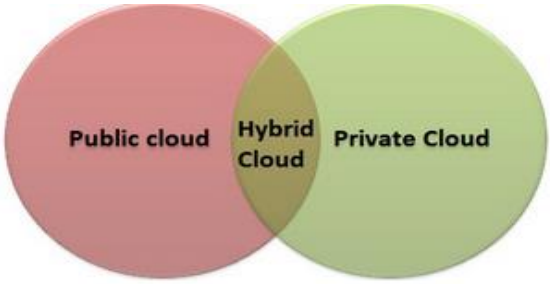

Figure 2. Hybrid cloud

3. Cloud Authentication issues

In order to access the data from the cloud, a user needs to have appropriate rights. User needs to get authenticated by the cloud server before accessing the requested data. The authentication process itself has several steps which involves sending and receiving packets to and from the cloud server. A typical; authentication process in the Google cloud is shown in figure 3.

The figure shows that when user needs access the cloud resources, he sends the authentication request.to the cloud server. Cloud server checks the user rights and generates the access token and sends it back to the user. Once user receives the token it acknowledges the response by sending the validate token packet. Validate token is then acknowledged by the cloud server and the communication starts.

Clearly, there is a lot of communication happening prior to accessing the user data. This communication is done through the public network which further delays the accessing of user data. Figure 4 shows the number of authentication packets go on increasing as the number of cloud increase. R In fact the rate of increase of authentication packets is greater than the rate of increase in the number of users. This may reach to a point where it actually starts degrading the performance to access the user data

There needs to be a way where we can reduce this communication over the public network which can increase the cloud performance.

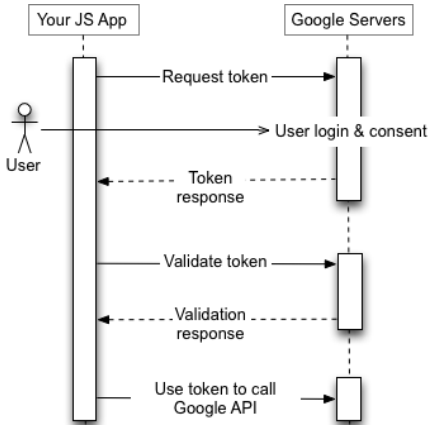

Figure 3 . Google Authentication process.

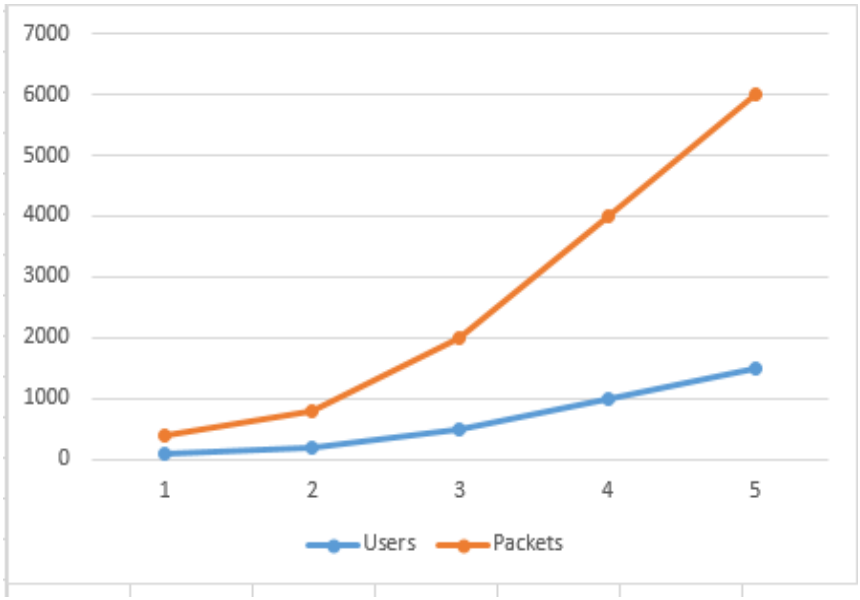

Figure 4. . Authentication packets

4. Proposed Authentication Technique

Our prosed authentication model consists of cloud servers that host the data that needs to be accessed by the users. In addition to this server, the model has following servers.

Cloud Authentication server

Cloud authentication sever is located at the service provider location. This server hosts the authentication database for the customers. Once a user's tries to access the resource from the cloud, the users first needs to provide the credentials to get authenticated. Once the credentials are passed, an access token for each resource is associated with the user id. A typical access control table is shown in the figure 6.

Secondary Authentication server (SAS)

In addition to the authentication server in the cloud, there is also a Secondary authentication server (SAS) at the customer site. Main purpose of the SAS is to frequently get the replicated copy of the authentication database from the cloud authentication server. Proposed authentication technique will work as follows.

4.1 Implementation

The authentication database will be placed at the cloud site, whereas, there will be a SAS server at the customer site. The replication will happen after regular intervals, say every 12 hrs. To reduce the amount of traffic over the public network, the replication is incremental in nature. This means at when a particular attribute of an object is modified or added in the cloud authentication database, only the attribute will be replicated to the SAS authentication database and not the whole object. The replication will be only from Cloud server to SAS and not from SAS to Cloud server

When a user needs to access the cloud resources, he is authenticated by the SAS server authentication database and an access token is generated. With this access token user can access the cloud resources. With this method, a user need not to cross the public network to get authenticated by the cloud server, rather he is authenticated locally by the SAS server.

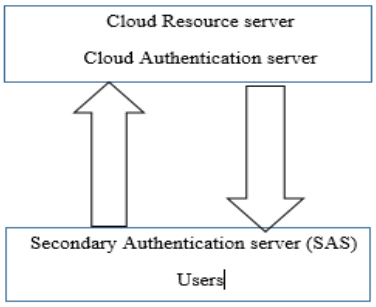

Figure 5. Proposed Authentication model

User id	Access type		
	Read	write	Delete
26546546	1	0	0
76876876	1	1	1
87678687	0	0	0

Figure 6. Access control table

5. Conclusion

The authentication mechanism in the cloud needs a user to send the requests and receive the access token over the public network which is slow The authentication packets increase at a rate which is faster than the rate of user increase , thus may cause performance issues.

The performance of the authentication process can be enhanced by placing a secondary authentication server at the customer location. This server has the replicated copy of the authentication database. Thus users can get authenticated locally rather than from the remote server. This is going to reduce the authentication lifecycle and also reduce the delay in accessing the user data.

REFERENCES

[1] Al-Roomi May and Al-Ebrahim Shaikha "*Cloud Computing Pricing Models:A Survey*",International Journal of Grid and Distributed Computing,Vol.6, pp.93-106, June 2013.
[2] Falatah Maran and Abdullah Omar "*Cloud Scalability Considerations*", International Journal of Computer Science & Engineering Survey (IJCSES) Vol, pp.1-45, August 2014.
[3] George Singer, "Towards a Model for Cloud Computing Cost estimation with Reserved Analysis", Proceeding of 2nd International ICST Conference on Cloud Computing, CloudComp 2010, 2010, pp. 1-10
[4] Gorelik Eugene "*Cloud Computing Models*", MIT Solan school of management,ppjn 2013
[5] Hashizume Keiko and Rosado David, "*An analysis of security issues for cloud computing*", Journal of Internet Services and Applications, pp.5-10, April 2013
[6] Kumar Pradeep and Mishra Bharat ,"*Cloud Computing Security Issues, Challenges and Solution*", International Journal of Emerging Technology and Advanced Engineering,, ISSN 2250-2459, Volume 2, Issue 8, pp. 1-3, August 2012
[7] Sosinsky Barrie,"*Cloud Computing*",Wiley Publishing, Inc.Indianapolis(USA),2011
[8] Schadler Ted, "*Should Email live in the Cloud*", Retrieved from *www.forrester.com,* pp.3-12, Jan 2009

A Brief Author Biography

Sanjay Razdan has around 17 years of experience in IT industry. He has worked on various technologies and automation projects. Sanjay has MSc, M.Phil. in Computer Science. His area of interest include parallel computing computer algorithms