CLOUD COMPUTING RESEARCH AND SECURITY ISSUES COMPARATIVE STUDY OF DIFFERENT PLATFORMS

Dhruv Mangal

Abstract

Cloud computing, a rapidly developing information technology has aroused the concern of the whole world. Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid. Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the powerful computing capacity to end users' hands. This article introduces the background and service model of cloud computing. This article also introduces the existing issues in cloud computing such as security, privacy, reliability and so on. Proposition of solution for these issues has been provided also.

Keywords – cloud computing; security; privacy; issue

I. INTRODUCTION

Cloud computing is not a total new concept; it is originated from the earlier large-scale distributed computing technology. However, it will be a subversion technology and cloud computing will be the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, will be widely used in the near future. The core concept of cloud computing is reducing the processing burden on the user's terminal by constantly improving the handling ability of the "cloud", eventually need to invest in building and managing the data centers.

II. WHAT IS CLOUD COMPUTING

A. Definition

"Cloud" is a virtualized pool of computing resources. It can:

- Manage a variety of different workloads, including the batch of back-end operations and user-oriented interactive applications.
- Rapidly deploy and increase workload by speedy providing physical machines or virtual machines.
- Support for redundancy, self-healing and highly scalable programming model, so that workload can be recovered from a variety of inevitable hardware/software failure.
- Real-time monitor resources usage, rebalance the allocation of resources when needed.

B. Service Model

- Software-as-a-Service (SaaS): Software as a service is software that is deployed over the internet and/or is deployed to run behind a firewall in your local or a network or personal computer. This is a "pay-as-you-go" model and was initially widely deployed for salesforce automation and Customer Relationship Management (CRM).
- Platform-as-a-Service (PaaS): Platform as a service, another SAAS, this kind of cloud computing provide development environment as a service. You can use the middleman's equipment to develop your own program and deliver it to the users through Internet and servers.

- Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service.
- Hardware-as-a-Service (HaaS): According to Nicholas Carr, "the idea of buying IT hardware or even an entire data center as a pay-as-you-go subscription service that scales up or down to meet your needs. But, as a result of rapid advances in hardware virtualization, IT automation, and usage metering and pricing, I think the concept of hardware-as-a-service, let's call it HaaS, and may at last be ready for prime time." This model is advantageous to the enterprise users, since they do not need to invest in building and managing data centers.

C. Deployment Model

- Public Cloud: In public clouds, multiple customers share the computing resources provided by a single service provider, Customers can quickly access these resources, and only pay for the operating resources .Although the public cloud has compelling advantages, their existing the hidden danger of security, regulatory compliance and quality of service (QoS).
- Private Cloud: In the private cloud, computing resources are used and controlled by a private enterprise. It's generally deployed in the enterprise's data center and managed by internal personnel or service provider. The main advantage of this model is that the security, compliance and QoS are under the control of the enterprises.
- Hybrid Cloud: A third type can be hybrid cloud that is typical combination of public and private cloud. It enables the enterprise to running state-steady work loading the private cloud, and asking the public cloud for intensive computing resources when peak workload occurs, then return if no longer needed.
- Community Cloud: Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

III. CLOUD COMPUTING ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

A. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the user.

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones". On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

E. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

F. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

G. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring.

H. Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company."Ask potential providers how you would get your data back and if it would be in a format that you could import into are placement application," Gartner says.

I. Solution

To advance cloud computing, the community must take proactive measures to ensure security. The Berkeley paper’s solution is the data encryption. Before storing it at virtual location, encrypt the data with your own keys and make sure that a vendor is ready for security certifications and external audits. Identity management, access control, reporting of security incidents, personnel and physical layer management should be evaluated before you select a CSP. And you should minimize personal information sent to and stored in the cloud.CSP should maximize the user control and provide feedback. Organizations need to run applications and data transfer in their own private cloud and then transmute it into public cloud. While there are many legal issues exist in the cloud computing, Cloud Security Alliance should design relevant standards as quickly as possible.

IV. VARIOUS CLOUD COMPUTING PLATFORMS

A. ABICLOUD Cloud Computing Platform

Abicloud is a cloud computing platform developed by Abiquo, a company locates in Barcelona Spain that is mainly focused on the development of cloud platform. It can be used to build, integrate and manage public as well as private cloud in the homogeneous environments . Using Abicloud, user can easily and automatically deploy and manage the server, storage system, network, virtual devices and applications and so on. The main difference between Abicloud and other cloud computing platforms is its powerful web-based management function and its core encapsulation manner. Using the Abicloud, user can finish deploying a new service by just dragging a virtual machine with mouse. This is much easier and flexible than other cloud computing platforms that deploy new services through command lines.

According to Abicloud, there is no perfect cloud platform. For each user needs his own cloud infrastructures, and every cloud provider has his own management tools, say monitor, billing and so on, so generally it is very hard to deploy a cloud platform according to user's requirement. The best way to meet the requirement of users is to build public or private cloud with homogeneous cloud computing core and extensible infrastructures. Besides, the cloud platform should also have all kinds of interfaces that support the third parties products. With all these characteristics, providers can build the cloud computing platform of their own.

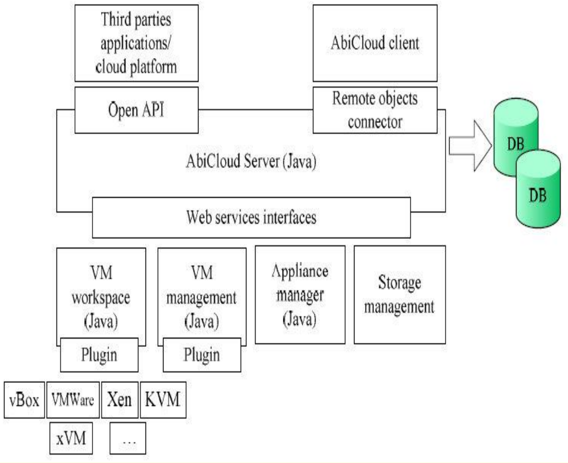


Figure 1 ABICLOUD Cloud Computing Platform

Abicloud can be used to deploy and implement private cloud as well as hybrid cloud according to the cloud providers' request and configuration. It can also manage EC2 according to the rules of protocol. Besides, apply the Abicloud, a whole cloud platform based on Abicloud can be packed and redeployed at any other Abicloud platform. This is much helpful for the transformation of the working environment and will make the cloud deployment process much easier and flexible. The architecture of Abicloud is illustrated in figure 1.

It can easily figure out that Abicloud is built based on Java, which sets it irrelevant to the platform and easy to transplant.

Actually, Abicloud can support many different virtual machine platforms which include vBox, VMWare, Xen, KVM and so on which make it very flexible.

B. EUCALYPTUS Cloud Computing Platform

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems) project began from California University Santa Barbara, and mainly was used to build open-source private cloud platform . Now it has been run by Eucalyptus system company. Eucalyptus is an open-source implementation of Amazon EC2 and compatible with business interfaces. It also implements virtualization depending on Linux and Xen as EC2 does.

Eucalyptus is an elastic computing structure that can be used to connect the users' programs to the useful systems, it is an open-source infrastructure using clusters or workstations implementation of elastic, utility, cloud computing and a popular computing standard based on service level protocol that permit users lease network for computing capability. Currently, Eucalyptus is compatible with EC2 from Amazon, and may support more other kinds of clients with minimum modification and extension. Figure 2 demonstrates the topology structure of Eucalyptus resources.

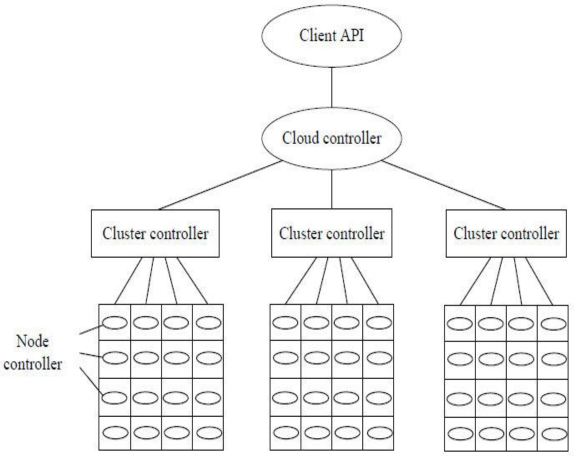


Figure 2 The Resource Topology Structure Of Eucalyptus

In figure 2, node controller is a component running on the physical resources, on which all kinds of entities of virtual machine can run. It answers for the startup, check, shut down and clear up of the virtual machines. Logic connected node controllers form a virtual cluster, all nodes belong to the same virtual cluster report to the cluster controller and are under the control and management of the cluster controller. Virtual cluster controller runs on the head node or server of the virtual cluster, is used to access private or public network. Cloud controller is the core of the manager of cloud platform, a component answering for global decision-making which is transplant to users. An Eucalyptus cloud has only one cloud controller. In Eucalyptus, client interface is the pass of communication and connection between the interior and the outside of Eucalyptus, through which users can access all kinds of resources on the cloud computing platform.

C. Nimbus Cloud Computing Platform

Nimbus is an open tool set, and also a cloud computing solution providing IaaS. Put forward based on scientific research in the early stage, Nimbus have supported many nonscientific research domain applications . It permits users lease remote resources and build the required computing environment through the deployment of virtual machines. Figure demonstrates the Nimbus cloud computing platform.

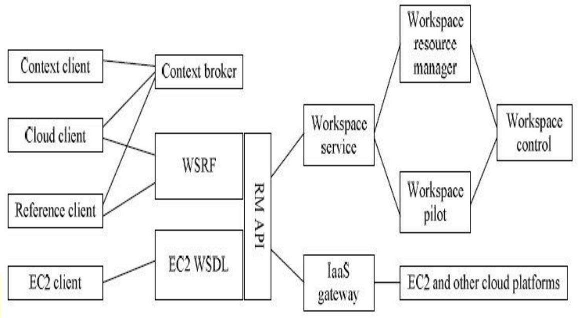


Figure 3 The Structure Of Nimbus Cloud Platform

Figure 3 shows that nimbus cloud computing platform includes many different components, say client, agent, resource manager and so on. Generally, all these functional components can be classified as three kinds. One kind is client-supported modules which are used to support all kinds of cloud clients. Context client module, cloud client module, reference client module and EC2 client module are all belong to this kind of component. The second kind of component is mainly service supported modules of cloud platform, providing all kinds of cloud services. It includes context agent module, web service resource framework module, EC2 WSDL module and remote interface module. The third kind of component is the background resource management modules which are mainly used to manage all kinds of physical resources on the cloud computing platform, including work service management module, IaaS gateway module, EC2 and other cloud platform support module, workspace pilot module, workspace resource management module and workspace controller. These components' functions are briefed as follows:

Workspace service module is an independent virtual machine manager and can access different kinds of remote protocol. It is irrelevant to the content running on the system while relevant to the Java application. The front of web service resource framework is the protocol before applications implemented between workspace and client. The front of EC2 is an implementation of Web Service Description Language (WSDL) from Amazon's elastic cloud computing platform, it permit users to develop EC2 not just nimbus cloud only. Cloud client module permit user run the requirement he want by very simple click operation. Reference client module tries to present the user all the characteristics of the front of WSRF in command line manner. This is a bit complex as it includes scripts of some specific applications. Object pilot is a program that tries to submit tasks to the local website resource manager to obtain virtual machine manager. Usually, the pilot module is an optional choice, and the service programs just manage the nodes deployed by the pilot program instead of running it. Remote management interface is a kind of interior interface. It permit implement the remote security protocol and independently process and manage operations.

Context agreement module answer for support client and coordinate manage the auto startup service of the large scale clusters. Besides, it also provides personal virtual machine services and can run both on nimbus cloud platform as well as EC2 through the backend service of EC2.

EC2 gateway can provide many functions, for example, running the public Amazon virtual machine image on the Amazon cloud platform, checking the status of homogeneous wireless sensor network, notice the user the public IP of virtual machine through the characteristics of resources when it is available and so on.

D. OpenNebula Cloud Computing Platform

OpenNebula is one of the key technologies of reservoir
plan and the flagship research project in virtualization
infrastructure and cloud computing of European Union. Like nimbus, OpenNebula is also an open source cloud service framework .It allows user deploy and manage virtual machines on physical resources and it can set user's data centers or clusters to flexible virtual infrastructure that can automatically adapt to the change of the service load. The main difference of OpenNebula and nimbus is that nimbus implements remote interface based on EC2 or WSRF through which user can process all security related issues, while OpenNebula does not.

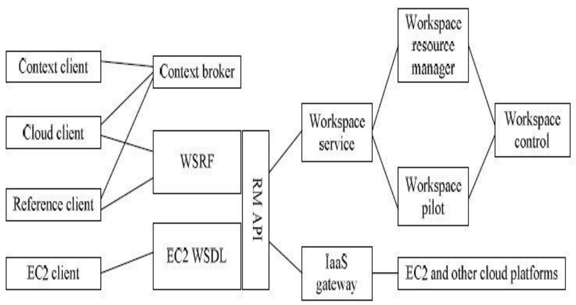


Figure 4 The Structure Of OpenNebula Cloud Platform

OpenNebula is also an open and flexible virtual infrastructure management tool, which can use to synchronize the storage, network and virtual techniques, and let users dynamically deploy services on the distributed infrastructure according to the allocation strategies at data center and remote cloud resources. Through the interior interfaces and OpenNebula data center environment, users can easily deploy any types of clouds. OpenNebula is mainly used to manage the data center of private cloud and infrastructure of clusters and it also support hybrid cloud to connect the local and public infrastructure. This is very useful to build high scalable cloud computing environment. Besides, OpenNebula also supports public cloud platform by providing interfaces and functions to virtual machines, storage and network management and so on. Through the control interfaces, users can access services provided by OpenNebula cloud computing platform. The structure of OpenNebula is illustrated in figure 4.

OpenNebula cloud computing platform has many advantages. Firstly, from the point of infrastructure management, it can dynamically adjust the scale of the infrastructure of the cloud platform by increasing the number of hosts and partition clusters to meet different requirements. Secondly, it can centralized manage all the virtually and physically distributed infrastructures and can create infrastructure with the heterogeneous resources at data center. This can guarantee use the resources more efficiently and can much reduce the number of the physical resources through the close integration of servers which further reduce the cost caused by space-saving, management, energy consumption, cooling and so on. What's more, integration of the local resources as well as remote ones can get rid of the extra cost to meet the peak requirements. From the point of infrastructure users, OpenNebula is scalable and can rapid response to user's requirements. From the point of system integrators, users can deploy any kind of cloud and integrate the visual data center and products or services in the management tools say cloud providers, virtual machine managers, virtual image managers, service managers, management tools and so on. As OpenNebula is an open source, flexible cloud with extensible interfaces, structure and components. This makes it suit be used in any kinds of data center.

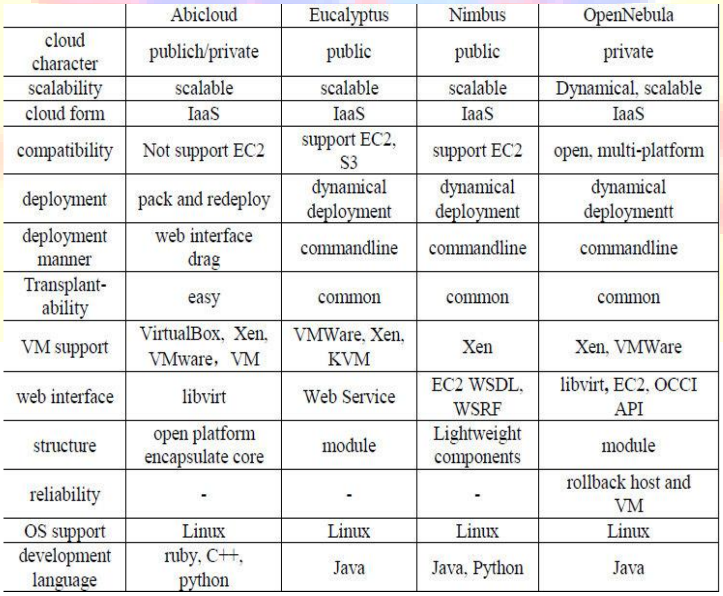
Compared with Eucalyptus, OpenNebula is more strength in the support of private cloud platform and dynamic management of the scalability of the virtual machines on clusters. To hybrid cloud, it provides on-demand access and elastic mechanisms as Amazon EC2 do.

V. COMPARISON OF CLOUD PLATFORMS

Currently, there are kinds of cloud computing platforms,
each has its own characteristics and advantages. To better understand these platforms, we analyze in detail and give a comparison from different implementation aspects. The characteristics and implementation of these platforms are summarized as table 1 shows.

From table 1, it can figure out that though the implementations of these cloud platforms are quite different, there are much common between them. For example, they are all scalable; all provide IaaS, all support dynamic deployment of the platform, all support Xen virtualization technology, and all support Linux operation system and the development of application with Java. However, there are also many differences, say their network interfaces, structure and reliability and so on. Generally, each cloud platform has its own advantages over others. For example, from the point of
cloud platform deployment, Abicloud stands out. As this cloud platform can be deployed with mouse under graphic user interfaces compared others with command line. This will be much simple to users and decrease the effort of the platform deployment. From the point of reliability, OpenNebula is more mature. For it has considered rollback and fault tolerance mechanisms in the cloud implementation while others do not.

Table 1 The Comparison Of Several Cloud Computing Platforms



	Abicloud	Eucalyptus	Nimbus	OpenNebula
cloud character	publich/private	public	public	private
scalability	scalable	scalable	scalable	Dynamical, scalable
cloud form	IaaS	IaaS	IaaS	IaaS
compatibility	Not support EC2	support EC2, S3	support EC2	open, multi-platform
deployment	pack and redeploy	dynamical deployment	dynamical deployment	dynamical deploymentt
deployment manner	web interface drag	commandline	commandline	commandline
Transplant-ability	easy	common	common	common
VM support	VirtualBox, Xen, VMware，VM	VMWare, Xen, KVM	Xen	Xen, VMWare
web interface	libvirt	Web Service	EC2 WSDL, WSRF	libvirt, EC2, OCCI API
structure	open platform encapsulate core	module	Lightweight components	module
reliability	-	-	-	rollback host and VM
OS support	Linux	Linux	Linux	Linux
development language	ruby, C++, python	Java	Java, Python	Java

VI. DIGITAL SIGNATURE WITH RSA ENCRYPTION ALGORITHM TO ENHANCE DATA SECURITY IN CLOUD

In Cloud computing, we have problem like security of data, files system, backups, network traffic, and host security. Here we are proposing a data security using encryption decryption with DES algorithm while we are transferring it over the network. .A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.

We proposed digital signature with RSA algorithm scheme to ensure the security of data in cloud. RSA is probably the most recognizable asymmetric algorithm. We include both digital signature scheme and public key cryptography to enhance the security of cloud computing. In Digital Signature, software will crunch down the data, document into just a few lines by a using “hashing algorithm". These few lines are called a message digest. Software then encrypts the message digest with his private key. Then it will produce digital signature .Software will Decrypt the digital signature into message digest with public key of sender’s and his/her own private key. We are using Digital signatures so that we are able to distribute software, financial transactions, over the network and in other cases where it is important to detect forgery and tampering.

A. Proposed Internal Working Steps Taken In Digital Signature With RSA Algorithm

Let us assume we have two enterprises A and B. An enterprise A have a public cloud with data, softwares and applications. .Company B wants a secure data from A's Cloud .We are here, trying to send a secure data to B by using Digital signature with RSA algorithm. We are taking some steps to implementing Digital signature with RSA encryption algorithm. Suppose Alice is an employee of an enterprise A and Bob is an employee of a company B.

Step1.Alice takes a document from cloud, which Bob wants.

Step2. The document will crunched into few lines by using some Hash function the hash value is referred as message digest. (Figure 5)

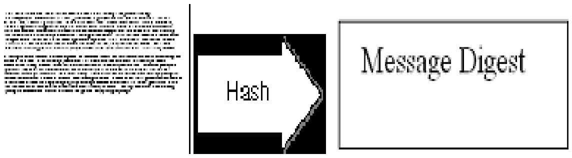


Figure 5 Document Crunched Into Message Digest.

Step 3. Alice software then encrypts the message digest with his private key. The result is the digital signature. (Figure 6)

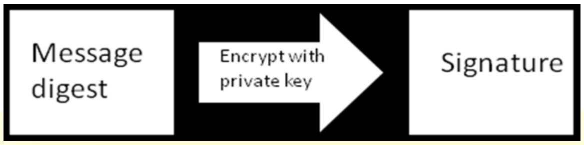


Figure 6 Encryption Of Message Digest Into Signature

Step 4. Using RSA Algorithm, Alice will encrypt digitally signed signature with Bob's public key and Bob will decrypt the cipher text to plain text with his private key and Alice public key for verification of signature (Figure7).

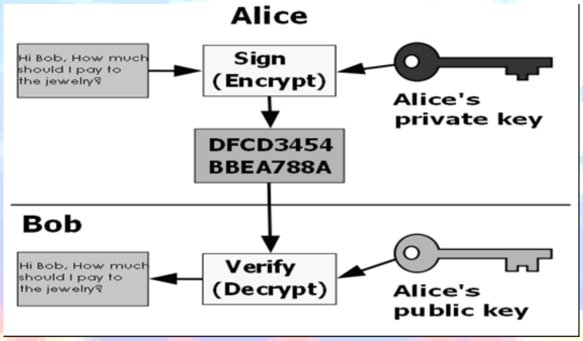


Figure 7 Encryption Of Digital Signature Into Cipher Text

B. Proposed Algorithm Taken For Implementing Digital Signature With RSA Algorithm

In this algorithm, n is known as the modulus. “e‟ is known as the encryption exponent. ‟ d‟ is known as the secret exponent or decryption exponent.

Step1. Key Generation Algorithm

1. Choose two distinct large random prime numbers p and q

2. Compute n = p q, where n is used as the modulus for both the public and private keys

3. Compute the totient: phi (n) = (p -1) (q-1)

4. Choose an integer e such that 1 < e < phi (n), and e and phi (n) share no factors other than 1, where e is released as the public key exponent

5. Compute d to satisfy the congruence relation d × e = 1 modulus phi (n); d is kept as the private key exponent

6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Step2. Digital signing

Sender A does the following:-

A) Creates a message digest of the information to be sent by using hash function.

Hash Function

1. Declare character “str“ of unsigned long type.

2. Declare and initialize hash of unsigned integer type

3. unsigned int hash = 0;

int q;

while (q = str+1)

hash =hash + q;

B) Represents this digest as an integer m between

0 and n-1

C) Uses her private key (n, d) to compute the signature,

s = md mod n.

D) Sends this signature s to the recipient, B.

Step3. Encryption

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).

2. Represents the plaintext message as a positive integer m

3. Computes the cipher text c = me mod n

4. Sends the cipher text c to B.

Step4. Decryption

Recipient B does the following:-

1. Uses his private key (n, d) to compute m = cd mod n.

2. Extracts the plaintext from the message representative m.

Step5. Signature verification Recipient B does the following:-

1. Uses sender A's public key (n, e) to compute integer

v = se mod n.

2. Extracts the message digest from this integer.

3. Independently computes the message digest of the information that has been signed.

4. If both message digests are identical, the signature is valid.

VII. MODELLING ON DIFFERENTIATED SERVICE JOB SCHEDULING SYSTEM IN CLOUD COMPUTING ENVIRONMENT

From a systemic viewpoint of a Cloud Computing environment, we can take a Cloud Computing environment as a very powerful server. This server will handle the CCU's jobs (See Figure 8). For each CCU may has different QoS requirement, usually, CCU's jobs have different priorities to be processed. So we can classify the jobs priorities into several classes.

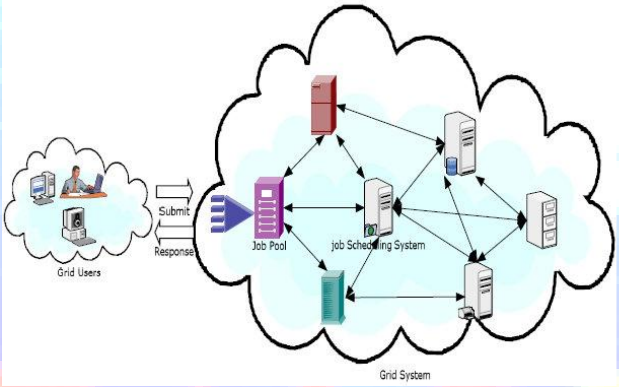


Figure 8 An Illustration for Cloud Job Scheduling.

In this model above, according to the CCU's jobs due time of finishing which is set by CCU, CCU's jobs are classified into N different classes by their different priorities. Each class i (i∈ [1, N]) is with a priority. The small number of i is the higher priority of the class is. Class 1 has the highest priority in the queue. We assumed that CCU's jobs in different classes with different priority. And they come to the server with a Poisson distribution at a certain rate, while the process time to each job by the server is in accord with a general distribution. Thus, we can build an M /G /1 queuing model with non-preemptive system (See Figure 9). The issue of job scheduling in the Cloud Computing environment is turned into a queue scheduling problem for M /G /1 with non-preemptive system. To measure the characteristics of CCU's jobs and CCSP's computing resources, we assume that CCU's jobs in the same class with priority are submitted to the Cloud according to Poisson distribution with rate λ_i , and job scheduling system in the Cloud will assign some resources in the Cloud to process each job with a general service time distribution of mean t_i and second moment t_i^2 .In each class with same priority, CCU's jobs are process by the order of its arrival (FIFO).

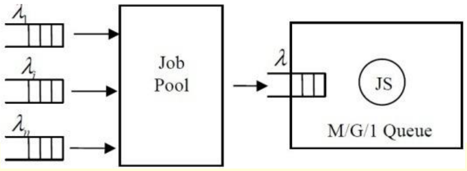


Figure 9 Queuing Model for Differential Cloud Computing Service

CONCLUSION AND FUTURE WORK

The algorithms and features discussed in this paper have been simulated and generated the satisfactory results. As cloud computing poses enormous opportunities for IT sector, the security, Job Scheduling, License Reusability, Fast Data Transfer are the important issue. Through this paper I tried to address some of the issues. But research is still on. Also it is important for the CCUs at various levels to understand the best cloud computing platform that can provide the most optimum requirement. The CCSP on the other hand have the task to provide the best services to the user and make the maximum profit. The research is still on to meet these two requirements of the cloud computing.

ACKNOWLEDGEMENT

The author would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCE

1. Implementing Digital Signature with RSA Algorithm to enhance the data security of cloud in cloud computing by Uma Somani, Kanika Lakhani, Manish Mundra.
2. Comparision of Several Cloud Computing Platforms by Junjie Peng, Xuejun Zhang, Zhou Lei, Bofang Zhang, Wu Zhang, Qing Li.
3. An optimistic differentiated service job scheduling system for cloud computing service users and providers by Luqun Li.