Volume 6, Issue 8, August 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Computing: Extended Distributed System

Shailza Kamal
Baba Hira Singh Bhattal Institute of Engineering & Technology,
Lehragaga, Punjab, India

Abstract: ***Cloud computing is the growing field in IT industry since 2007 proposed by IBM. Another company like Google, Amazon, and Microsoft provides further products to cloud computing. The cloud computing is the internet based computing that shared resources, information on demand. It provides the services like SaaS, IaaS and PaaS. The services and resources are shared by virtualization that run multiple operation applications on cloud computing. This discussion gives the survey on the challenges on security issues during cloud computing and describes some standards and protocols that presents how security can be managed.***

Keywords: service models, security issues, confidentiality, integrity, protocols.

I. INTRODUCTION

Cloud computing is Internet based computing, which share resources, software and information are provided to the computer and other devices on demand [3]. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources [9]. 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" to simplify the user's terminal to a simple input and output devices, and provides the services on demand.

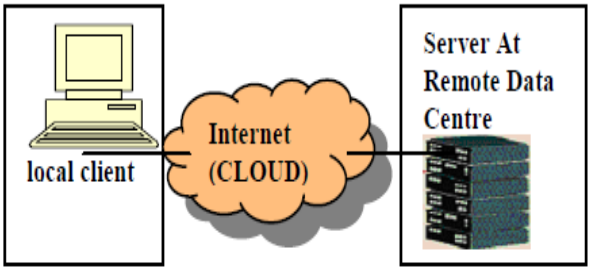

Fig. 1

The structure of cloud includes:
1. Service model
2. Deployment model

The architectural layer of cloud computing can be describe services being provided at any of the traditional layers from hardware to applications. Cloud service provider tends to offer services that can be grouped into three categories: *software as s service, platform as services, intrastate as a service.*

(a). Software as a Service:

Software as a service features a complete application offered on demand. Users prescribe software and it is license in order to install it on their hard disk and then use it, however cloud users do not required to purchase the software rather the payment will be based on pay-per-use model [5].

(b). Platform as a Service:

In this kind of cloud computing provide development environment as a service. We can use the middleman's equipment to development your own program and deliver it to the users through Internet and services [3].

(c). Infrastructure as a Service:

Infrastructure as service delivers a platform virtualization environment as service [3]. In IaaS vendors provide the infrastructure as a service where it is delivered in form of technology, data centers and IT services to the customer [5].

The following table shows the architectural view of cloud computing with example.

Table 1.

	Services	Providers
SaaS	• Support running multiple instances of it. • Develop software that is capable to run in the cloud.	• Google Docs • Mobile Me • Zoho
PaaS	• Platform which allows developer to create programs that can be run in the cloud. • Includes several applications services which allow easy deployment.	• Microsoft Azure • Force.com • Google App Engine.
IaaS	• Highly scaled and shared computing infrastructure accessible using internet browser. • Consists of Database, servers and storage	• Amazon S3 • Sun's Cloud Service

Virtualization:

The cloud computing incorporates virtualization, on demand deployment, internet delivery of services and open source software. Virtualization enables a dynamic datacenter where the servers provide a pool of resources that are harnessed as needed.

Many cloud computing systems vendors provide cloud infrastructures and platforms based on virtual machines. The virtual machine is the basic component to host these services. Fig. 3 shows this service provision architecture in detail. As shown in Fig. 2, hosted services reside on the virtual machine, which is combined with or shared from a set of CPUs, memory, storage on demand, and is regarded as services' infrastructures or platforms running on. Clearly, virtual machines have the capability in providing on demand services in terms of users' individual resource requirement for a large amount of users. In certain sense, users can use them as on-premises systems and can upgrade at any time they want to. On the other hand, a Cloud system vendor depends on the virtual machine to tie commodity personal computers or servers together and to provide a scalable, robust system. Thus, this virtual machine is always available to use.

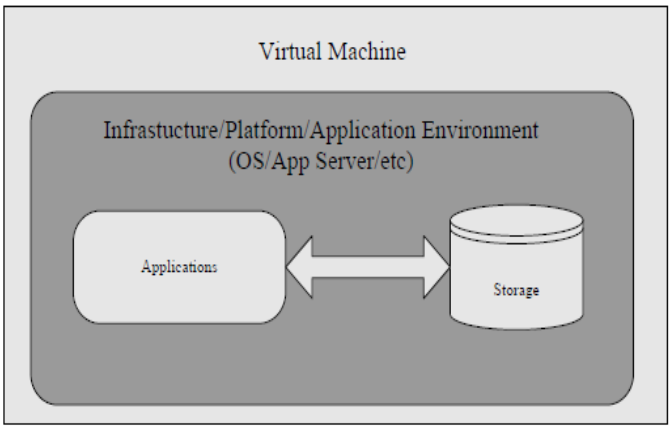

Fig .2

DEPLOYMENT MODELS:

There are three deployment models for cloud computing: public, private, and hybrid.

A. Public Cloud

The physical infrastructure is generally owned and managed by the service provider [14]. 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, there existing the hidden danger of security [3].

B. Private Cloud

The physical infrastructure is generally owned and managed by the service provider. 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 [3].

C. Hybrid Cloud

A third type can be hybrid cloud that is typical combination of public and private cloud.

- Major area of concern of my topic is to cover the following:

1. Various security issues and challenges
2. Security standards and protocols
3. Security management models

II. LITERATURE SURVEY

"On Technical Security Issue In Cloud Computing" the paper published in the 2009 IEEE conference they describe the cloud layers and access technology structure of the layered architecture. According to this paper to access these cloud services; two main technologies can be currently identified at that time. *Web services are* commonly used to provide access to IaaS service and *web browsers* are used to access SaaS applications in PaaS environment both approaches can be found.

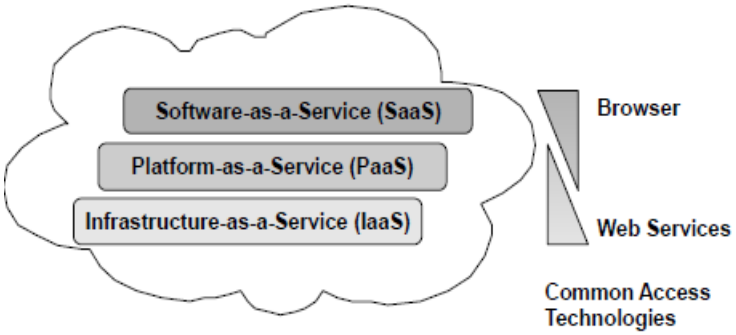

Fig. 3

There are two main foundations of this research that describe the main security are"

Web security: the most important specification addressing security for web services is WS- security, defining how to provide integrity, confidentiality and authentication for the cloud messages.

TLS: Transport Layer Security has been introduced, under its more common name "secure sockets layer SSL. It consists of two main parts: The *Record Layer encrypt/decrypt* TCP data streams using algorithms and keys negotiated in the *TLS Handshake* which is also used to authenticate the server client. TLS offers many different options for key agreement, encryptions and authentication of network peers.

The major cloud computing security issues at this paper describes the following:

1. Cloud Malware injection attack: A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system.

2. Flooding attacks: under the security consideration the this architecture of cloud system having some serious drawbacks i.s due to its on demand service application there is trouble of attackers are always ready. The corresponding threat is that of *flooding attacks*, which basically consist in an attacker sending a huge amount of nonsense requests to a certain service.

3. Metadata spoofing attack: the *metadata spoofing attack* aims at maliciously reengineering a Web Services' metadata descriptions [12].

So according to this paper the author describe that the base of the cloud computing due the internet based application and using open source applications are the web services and wed applications. The best way to protect the cloud is to firstly protect the wed services framework

According to J. Yang his research on the "Cloud Computing Security Issues" 2010 he describes the following main cloud computing security issues:

Security: According to some arguments that the where data is more secure in the cloud internally or provides the data outside venders? In the cloud system the data is distributed to various computers individually so the hackers can detect your personal data anytime and anywhere.

Privacy: the most of the task will be done on the virtual machine. The virtual computing technology, user's personal data may be scattered in various location. So the hidden information may be easily leak out by the users when they use to access cloud computing services.

Open standard: open standards are critical to the growth of cloud computing.

Long term viability: according to Gartner [12] you should be sure that your data put into the cloud will never be invalid even your cloud computing provider go broke.

According to the author the security issue may be controlled by, before storing the data into virtual machine the entire data should be encrypt with your own key and the user may be ready to use the data in cloud with secure certification and audits

Now the most importantly we will discuss the seven security issues by the Gartner's on the cloud computing.

1. Privileged user access: Get as much information as you can about the people who manage your data.

2. Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.

3. Data location: When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions,

4. Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest,"

5. Recovery: Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster

6. Long-term viability: According to Gartner[12] you should be sure that your data put into the cloud will never be invalid even your cloud computing provider go broke.

The biggest challenge in implementing successful cloud computing technologies is managing the security. The fig. 4 describes the cloud computing security requirements at each level to along with different services and deployment models.

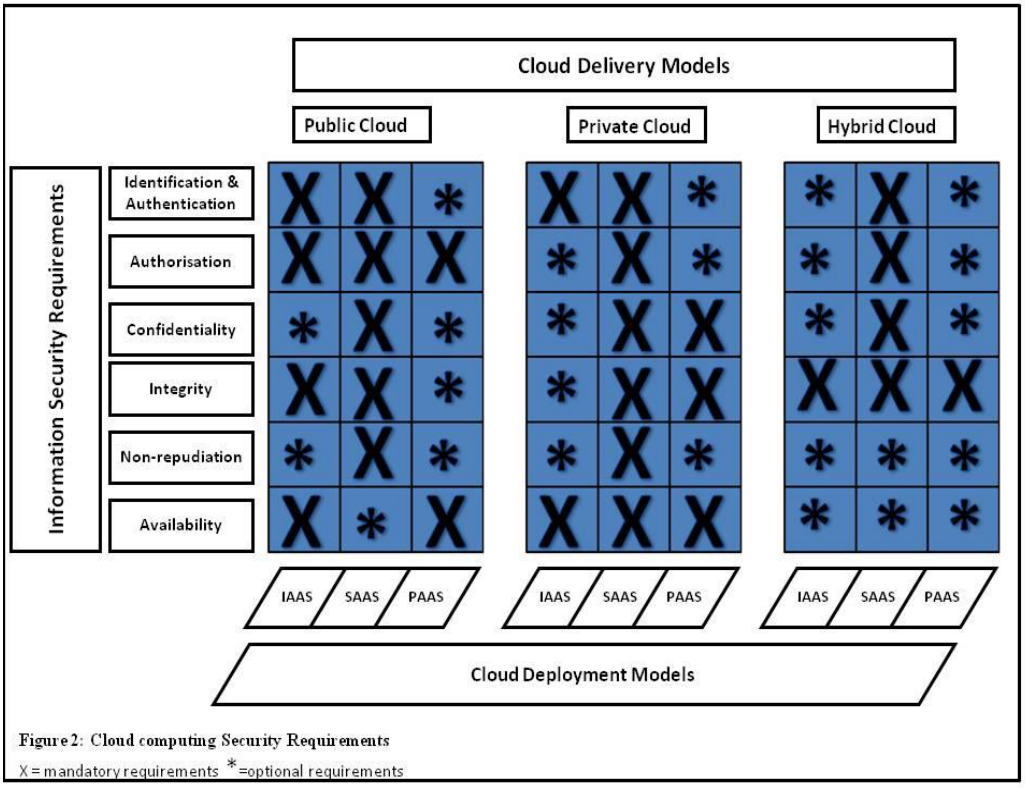

Fig. 4

From survey of the paper [5] the cloud security and privacy related data have been distributed to the basic three levels network level, host level, application level. At each level, it is required to security requirements to preserve data security in the cloud such as confidentiality, integrity and availability.

Confidentiality:

Ensuring that user data, which resides in the cloud, cannot be accessed by unauthorized party. This can be achieved through proper encryption techniques taking into consideration the type of encryption: symmetric or asymmetric encryption algorithms.

B Integrity:

This paper describes two approaches, which provides integrity, using message authentication code and digital signature. MAC is based on symmetric key to provide a check sum and DS depends on public key structure.

C Availability:

Another issue is availability of the data when it is requested via authorized users. The most powerful technique is prevention through avoiding threats affecting the availability of the service or data. It is very difficult to detect threats targeting the availability.

From the survey done by the international data corporation (IDC) of 263 executives they find out that the security ranked first as the greatest challenge or issue of cloud computing [9]. The reference to the international data corporation, is important because it highlights the shortfalls of cloud computing as well as user's security expectations in cloud computing.

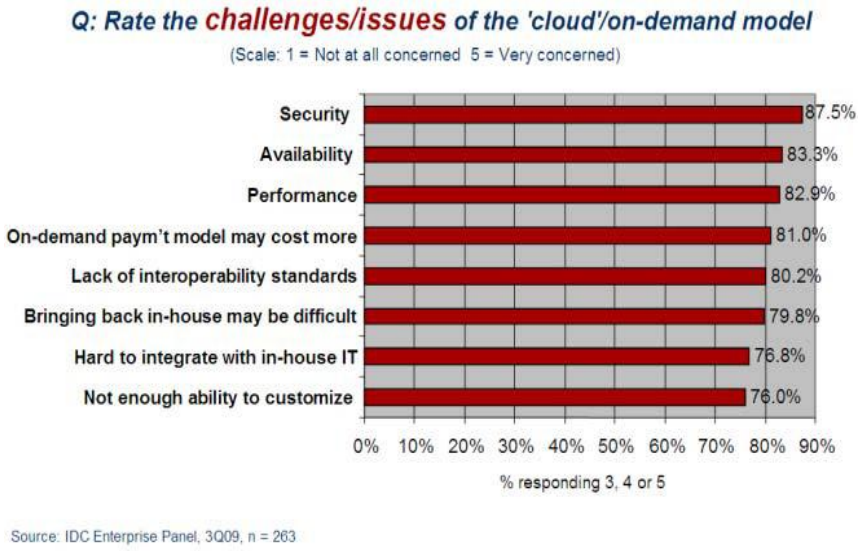

Fig. 5

III. DISCUSSIONS

On the discussion mode of the this paper I want to describe some cloud security management techniques and cloud computing tackling some protocols such as security assertions markup language (SAML) , open authentication protocols.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management (IAM) can be defined as a methods that provide an adequate level of protection for organization resources and data through rules and policies which are enforced on users via various techniques such as enforcing login password, assigning privileges to the users and provisioning user accounts. The IAM standard provides the great help in authentication, authorization and auditing for users who are accessing the cloud computing.

a) Authentication: Cloud computing authenticate involve verifying the identity of users or systems.

b) Authorization: once the authentication process succeeds, then the process of determining the privileges could be given to legitimate users.

c) Auditing: It is the process of reviewing and examining the authorization and authentication records in order to check, whether compliances with predefined security standards and policies.

IAM standards and protocols

The two main protocols for security to cloud computing are considered by the IAM are:

A. Security Assertion Markup Language (SAML)

SAML is based on XML standards, used as a tool to exchange the authorization and authentication attributes between two entities – in the case of the cloud, between the Identity provider (IdP) and Cloud Service Provider (CSP)-. The main goal of SAML is trying to achieve is to support SSO using the internet. In SSO, Password management consists of how the password will be stored in the cloud database.

The fig 6. describe the SAML communication process:

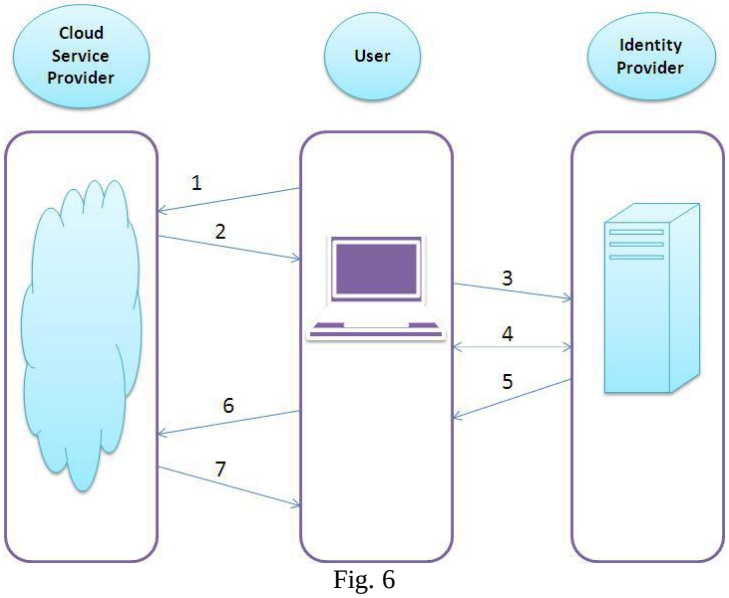

Fig. 6

1. User will request a web page from the CSP.
2. CSP will respond to the User by redirecting the user's browser to the SSO website located at the IdP.
3. Browser redirecting process.
4. Exchange authentication protocol between the IdP and user for identification.
5. IdP responds using encoded SAML to user.
6. User browsers will send SAML response to CSP to access the URL.
7. User will be able to log in the CSP application.

B. Open Authentication Protocol (OAuth)

Protocol, which allows users to share their private resources such as files, pictures located on one CSP with another CSP without exposing the personal identity information such as user names and passwords [4]. It is main objective is to build an authorized access to a secure Application Programming Interface (API) used in mobile and desktops designs and it is based on the open source implementations.

Fig. 7 describes the communication process of OAuth protocol:

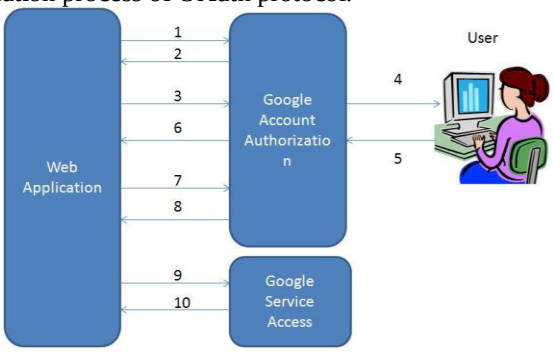

Fig. 7

1. Web application well asks Google Authorization for OAuth *request token*.
2. Google will response with *unauthorized request token*.
3. Web application will direct users to Google web authorization page to request *authorized token.*
4. User will access the Google Authorization page to verify their identity and either to allow or deny web application access to their data.
5. If user denies access then he/she will be directed to the Google page rather than the application page.
6. If user grants access, he/she will be redirected to the application web page, which includes *authorized request Token.*
7. The authorized request token will be exchanged between the web application and Google Authorization.
8. Google will verify the request and send *Access Token.*
9. The web application will request for user data from Google Authorization.
10. The request in step 9 will be verified and signed by Google Authorization and if the access token known by the Authorization the requested data will be send.

OAuth Token is used to authenticate users to the service requested. There are two types of OAuth token:

(a) Request tokens – used for requesting tokens from service provider to establish access token.

(b) Access token – used to get user data from the service provider to access requested pages. Request tokens can be either authorized or unauthorized. Initially, token are unauthorized, after the user successfully access the web application the requested token will be authorized and only authorized tokens can be used as access tokens.

IV. COMPARISON

From the point of view it is found that the cloud service providers may prefer more then one-authentication protocols to provide better security model to control their user identities. The SAML is mostly used in the enterprises due to its SSO functionality. It supports digital signature and encryption as well communication process between CSP ,USER and IdP takes less time.

On the other hand OAuth belongs to the open source applications libraries. These libraries are new and need more work to be done to improve the protocols of this category. So the SAML will be preferred by the most cloud services providers.

V. CONCLUSION

The cloud computing is internet based computing so firstly data stored into the cloud through web services so the first we have to protect the web services and the data shared to multiple applications through virtual machine that should be protect by entering some encrypted keys to the user who use the services on cloud. The security issue is the biggest challenge in the cloud computing having security, privacy etc. some protocols and standards are proposed by the IAM which describe various methods to protect the data in the cloud. Data encryption keys and auditing the users are the main requirements during the cloud computing.

REFERENCES

[1] Gartner. "Seven cloud-computing security risks". http://www.infoworld.com July 02, 2008.
[2] Nils Gruschka, Luigi Lo Iacono. "On Technical Security Issue in Cloud Computing". IEEE International Conference On Cloud Computing, 2009.
[3] Jianfeng Yang. "Cloud Computing Research and Security Issue". IEEE International Conference, 2010.
[4] Bhagyaraj Gowrigolla, Sathyalakshmi sivaji. "Design and auditing of cloud computing security: IEEE 2010.
[5] Sameera Abdulraman Almulla. "Cloud Computing Security Management" . October 2010.
[6] "Architectural Strategies for Cloud Computing". Oracle Corporation August 2009.
[7] Mingi Zhou, Rong Zhang, " Security And Privacy In Cloud Computing: A Survey". Sixth International Conference On Semantics, Knowledge And Grids,2010.
[8] Ramgovind S, Eloff Mm, Smith E, " The Management Of Security In Cloud Computing" .IEEE International Conference, 2010.
[9] Kresimir Popovic, "Cloud Computing Security Issue And Challenges". Mipro 2010, May 24-28, 2010 Opatija,Croatia.
[10] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009.
[11] Gunner Paterson, " A Security Architecture Stack For The Cloud". September-October 2010 IEEE Security And Privacy Article.
[12] Hassan Takabi, James B. D. Joshi, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud ComputingEnvironments", 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.
[13] M. Jensen, N. Gruschka, and R. Herkenh¨oner, "A survey of attacks on web services," Computer Science - Research and Development (CSRD), Springer Berlin/Heidelberg, 2009.
[14] Bhagyaraj Gowrigolla, Sathyalakshmi Sivaji, "Design and Auditing of Cloud Computing Security", IEEE 2010.

