e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Cloud Computing Security Issue And Barriers

Vishal K Upadhyay[1], Dr. Vinod L Desai[2]

[1] DCS, Research Scholar Mewar University Chhittogarh (Rajasthan),

[2] Govt. Science College, Chikhali (B.Sc.Computer Science Dept.)

Abstract - The cloud computing security is most important thing now a day. In this paper we discuss about the cloud computing security issue and barriers about cloud computing security. And also discuss cloud computing security modern issues. And in this paper we also discuss the characteristics, service models and deployment models of cloud computing.

Key Words - Cloud Computing Security, Barriers to Cloud Computing, Security strategies of cloud computing.

I. INTRODUCTION:

NIST defines cloud computing by:[1]

5 - essential characteristics.
3 - cloud service models.
4 - cloud deployment models.

Essential Characteristics:

1. On-demand service:
   Get computing capabilities as needed automatically.
2. Broad Network Access:
   Services available over the net using desktop, laptop, PDA, mobile phone.
3. Resource pooling:
   Provider resources pooled to server multiple clients.
4. Rapid Elasticity:
   Ability to quickly scale in/out service.
5. Measured service:
   control, optimize services based on metering.

Cloud Service Models:

1. Software as a Service (SaaS):
   We use the provider apps.
   User doesn't manage or control the network, servers, OS, storage or applications.
2. Platform as a Service (PaaS):
   User deploys their apps on the cloud.
   Controls their apps.
   User doesn't manage servers, IS, storage.
3. Infrastructure as a Service (IaaS):
   Consumers gets access to the infrastructure to deploy their stuff.
   Doesn't manage or control the infrastructure.
   Does manage or control the OS, storage, apps, selected network components

Deployment Models:

1. Public:

Cloud infrastructure is available to the general public, owned by org selling cloud services.

2. Private:

Cloud infrastructure for single org only, may be managed by the org or a 3rd party, on or off premise.

3. Community:

Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rd party.

4. Hybrid:

Combo of >=2 clouds bound by standard or proprietary technology.

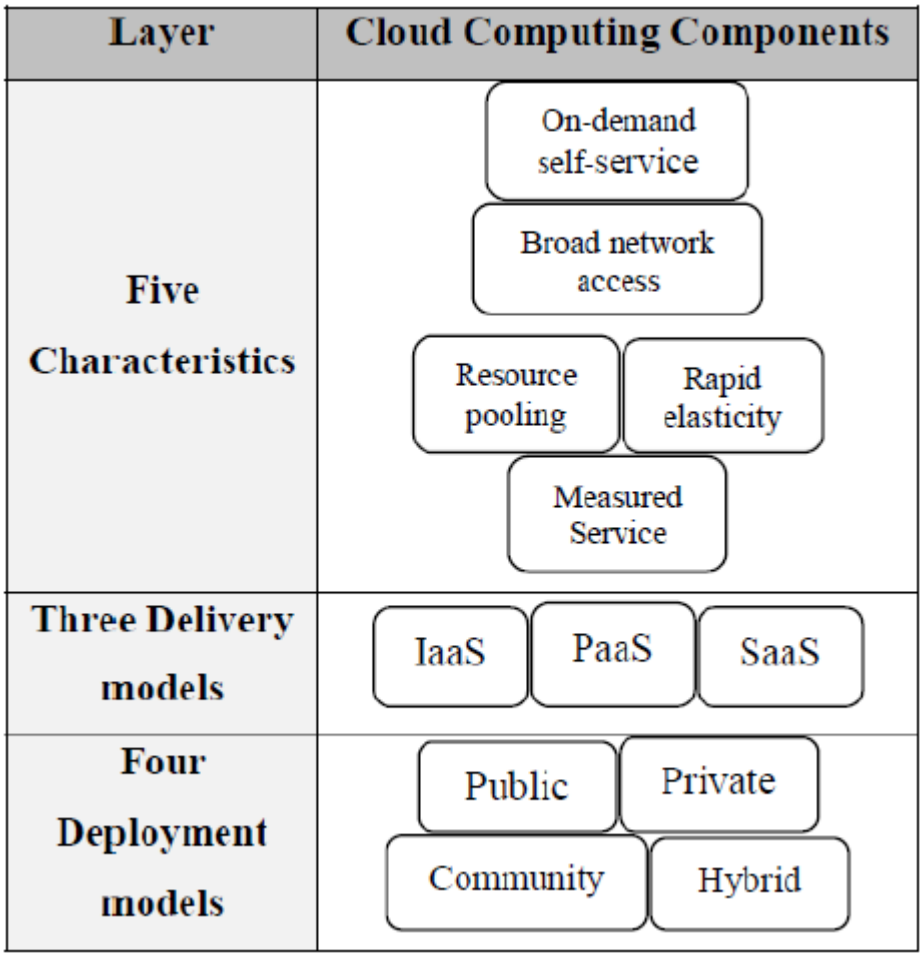

Fig.1. the NIST's definition model of cloud computing [2].

The cloud model itself is a three-tiered structure based on (1) infrastructure-as-a-service (IaaS); (2) platform-as-a-service (PaaS); and (3) software-as-a-service (SaaS). Infrastructure and software are particularly important for corporate counsel to master.

Provisioning infrastructure from a third-party cloud vendor allows corporations to take advantage of processing, storage, networks, and other fundamental computing resources on which its computers can run software, including platforms, Operating Systems, and applications.

IaaS Infrastructure as a Service offers the possibility for the end-user/developer/admin to upload the OS images large files and to load directly in virtual machines players, in order to start the applications from guest operating system.

Infrastructure as a Service - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software, that they need.
Examples of IaaS include: Amazon CloudFormation with its service Amazon EC2, Rackspace Cloud, Terremark and Google Compute Engine plus for the private approach Eucalyptus, OpenStack, OpenNebula.

PaaS Platform as a Service offers the possibility to the end-user/developer/admin to upload an archive file to a dedicated web/application server. The software application is developed in a certain technology with dedicated API (Microsoft Azure IIS Web Server with ASP and C# .NET / Google App Engine - Java).

Platform as a Service - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
Examples of PaaS include: Amazon Elastic Beanstalk, Cloud Foundry, Heroku, EngineYard, Mendix, Google App Engine, Microsoft Azure and OrangeScape.

SaaS Software as a Service offers to the end-user a final product or services that will be valuable and reliable (Microsoft Word/Excel available through Internet browser using Microsoft Office 365).

Software as a Service - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.
Examples of SaaS include: Google Docs, DropBox, Quickbooks Online, Limelight Video Platform, Salesforce.com and Microsoft Office 365.[3]
•IaaS: entire infrastructure from facilities to HW.
•PaaS: application, Middleware, database, messaging supported by IaaS.
•SaaS: self contained operating environment: content, presentation, apps, mgt.

II. PUBLIC VS. PRIVATE SECURITY

So some of the differences between public and private cloud offerings, as far as security goes, are going to be:

- Your control over who sees your data - with the public cloud, you don't know what employee at that company has access to your data. And it could be - typically these companies are very large, what controls do they have over the employees that can access your data. For a company that needs to be compliant in any way, that's not going to be acceptable at all.
- You also don't have any control over any of the firewall resources that you get. It's all done in a virtual environment. So, the changes that are made to the firewall could affect you, even though you didn't ask for those changes. Now, with a private cloud, as far as security is concerned, you control every aspect of it. Those firewalls are dedicated to you. The resources - you know who has access to those resources because it's your company. We don't, as far as Online Tech's private cloud is concerned, we don't access any of your data. It's all on you. With a public cloud, you don't get that.[4]

III. THE COMMON SECURITY ISSUE OF CLOUD COMPUTING

3.1. Seven Security Issues of Cloud Computing Respectively by CSA and Gartner

Cloud Security Alliance (CSA) has published a white paper titled *Top Threats to Cloud Computing* by summarizing various security concerns of cloud computing in March, 2010. seven security risks of cloud computing:[5] 1) *abuse and nefarious use of cloud*, 2) *insecure interfaces and APIs*; 3) *malicious insiders*; 4) *shared technology issues*; 5) *data loss or leakage*; 6) *account or service hijacking*; 7) *unknown risk profile*.

Gartner, a global authoritative IT research and analyst firm, has made a widespread investigation, and summarized seven security risks of cloud computing:[6] 1) p*rivileged user access*; 2) r*egulatory compliance*; 3) d*ata location*; 4) d*ata segregation*; 5) r*ecovery*; 6) *investigative support*; 7) l*ong-term viability*.

3.2. Three Parties' Security Issues of Cloud Computing

We analyze the security risks of cloud computing from the perspective of customer, service provider and government as follows.[7]

• The security risks confronted by customers

The security risks that customers need to confront in cloud computing environment include: 1) The downtime of cloud computing environment that brings great depress to the confidence of customers cannot be avoided totally; 2) The leak of commercial secrets that means a nightmare for customer cannot be avoided totally; 3) How to face the privilege status of cloud service provider and the security concerns such as fault elimination, damage compensation and business migration etc.

• The security risks confronted by service providers

The security risks that service providers need to confront in cloud computing environment include: 1) How to assure the long-term secure operation of the cloud data center and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with; 2) How to fight against the numerous and aggressive network hackers is a disturbing security problem; 3) For customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.

• The security risks confronted by government

The security risks that government administrators need to confront in cloud computing environment include: 1) How to enhance the security protection of a mass-scale data center is one important concern; 2) How to securely manage the numerous and various scale cloud service providers; 3) How to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.

IV. THE MODERN ISSUES ARE AS FOLLOWS

Security of data at data center: Organizations are skeptical about the data security because of "third party vendor and multi tenancy". Choice of cryptographic and hash algorithms used, how it works at transport layer and how data protected from other tenants being the center issue. Multi-tenancy is the obvious choice for the cloud vendors for scalability but large enterprises see it as a weapon to exploit their huge database.

Instance hijacking: when a hackers/intruders captures the instance of the application by simple hacking mechanism or through the other running instances of the application in a different geography. Virtual Machine or Instance attacks can be caused. Vm-Vm attacks can occur which can be lethal for whole cloud environment.

Cloud v/s cloud: People are afraid that the intruders/hackers will abuse the cloud computing power to attack them. Hacker Thomas Roth claims to break all SHA-1 hashes of password length 1 to 6 in just 49 minutes.
Virtualization: Virtualization of the application, desktop and server itself has many security issues, they Hypervisor may not be as powerful as it should be and it may lead to attacks.
What about "data in motion": Generally, a service is replicated 3 or more times as in Windows Azure so considerable amount of data lies over the internet due to high replication for scalability and flexibility with geo-distribution around the world which "makes data available " for good amount of time hence its security is a concern.

No security standards, protocols and compliance on vendors: There is no industry standard definition of cloud computing, it's working model, security algorithm, protocols and compliances which a company must follow. Enterprises resist public & hybrid clouds due to lack of legal support.
Untrusted interfaces or the APIs: It is very difficult for the developer to make a secure applicant ion third party APIs and interfaces are hard to trust.
Threat from future computational models- Quantum computing when it will be applied with the cloud computing then the computation will increase tremendously even without much powerful hardware.

"Security" is always a major issue for the customers be it large enterprise or be it end users. To have a satisfied customer it is essential that they must be provided with reliable security system.[8]

V. BARRIERS TO CLOUD COMPUTING ADOPTION IN THE ENTERPRISE

Although there are many benefits to adopting cloud computing, there are also some significant barriers to adoption.

5.1. Security and Privacy

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing. The ability of cloud computing to adequately address privacy regulations has been called into question.
Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

5.2. Connectivity and Open Access

The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products.
Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.

5.3. Reliability

Enterprise applications are now so critical that they must be reliable and available to support 24/7 operations. In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption. Each aspect of reliability should be carefully considered when engaging with a CSP, negotiated as part of the SLA, and

tested in failover drills. Additional costs may be associated with the required levels of reliability; however, the business can do only so much to mitigate risks and the cost of a failure. Establishing a track record of reliability will be a prerequisite for widespread adoption.

5.4. Interoperability

The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise. Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs. This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information. Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes. SaaS applications delivered through the cloud provide a low-capital, fast-deployment option. Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology. The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company's information and processes.[9]

5.5. Economic Value

The growth of cloud computing is predicated on the return on investment that accrues. It seems intuitive that by sharing resources to smooth out peaks, paying only for what is used, and cutting upfront capital investment in deploying IT solutions, the economic value will be there. There will be a need to carefully balance all costs and benefits associated with cloud computing—in both the short and long terms. Hidden costs could include support, disaster recovery, application modification, and data loss insurance. There will be threshold values whereby consolidating investments or combining cloud services makes sense; for example, it might not be efficient or cost effective to utilize multiple autonomous SaaS applications. Each may contract for disaster recovery program services. There is a point where economies of scale mean these functions should be combined in a similar service.

Application usage may begin with a low volume of transactions that can be supported with semi-automated master data management. As usage expands and interoperability requirements for the business process become more onerous, a new approach is needed. This evolution may be the most cost-effective approach; however, there is a risk that the business transition costs from one solution to another may change the cost and benefit equation, and hence the solution that should be employed.

5.6. Changes in the IT Organization

The IT organization will be affected by cloud computing, as has been the case with other technology shifts. There are two dimensions to shifts in technology. The first is acquiring the new skill sets to deploy the technology in the context of solving a business problem, and the second is how the technology changes the IT role. During the COBOL era, users rarely programmed, the expectations of the user interface varied, and the adaptability of the solution was low. Training was delivered in separate manuals and the user used the computer to solve problems only down predefined paths. With the advent of fourth-generation languages, roles within IT, such as system analyst and programmer, became merged into analyst/programmer, users started to write their own reports, and new applications, including operational data stores, data entry, and query programs, could be rapidly deployed in weeks. IT's role will change once again: the speed of change will impact the adoption of cloud technologies and the ability to decompose mature solutions from hype to deliver real value from cloud technology; and the need to maintain the controls to manage IT risk in the business will increase.

5.7. Political Issues Due to Global Boundaries

In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, different privacy

rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional. For cloud computing to continually evolve into a borderless and global tool, it needs to be separated from politics. Currently, some major global technological and political powers are making laws that can have a negative impact on the development of the global cloud. For example, as a result of the USA Patriot Act, Canada has recently asked that its government not use computers in the global network that are operating within U.S. borders, fearing for the confidentiality and privacy of the Canadian data stored on those computers. Providers have been unable to guarantee the location of a company's information on specified set of servers in a specified location. However, cloud computing service providers are rapidly adopting measures to handle this issue. For example, Amazon Web Services recently announced the Amazon Virtual Private Cloud that allows a business to connect its existing infrastructure to a set of isolated AWS compute resources via a VPN connection. To satisfy the European Union data regulations, AWS now allows for companies to deploy its SimpleDB structured storage physically within the EU region. Cloud computing depends largely on global politics to survive. Imagine if the telecommunications companies in the United States get their way and do away with the current Internet standard of network neutrality completely. Having data throttled and information filtered goes against the basic concept of cloud computing and global knowledge. You can't have a working cloud of information and services to draw from and build on if someone or something is constantly manipulating the data held within it, or worse, if something is blocking it from your view to achieve a hidden agenda. Politics are affecting the scalability of the Internet, the availability of Internet access, the free flow of information, and the cloud-based global economy on a daily basis.[10]

VI. SOME SECURITY STRATEGIES OF CLOUD COMPUTING

When constructing or migrating customer business to a cloud environment, its security must be assured. Here, we give several strategies to contribute a secure cloud environment. Regarding to the security risks of cloud computing, we proposed several security strategies as follows.

6.1. Securely Construction Strategies of Cloud Computing[11]

6.1.1. Traditional Security Practice Mechanism

Traditional security practice such as the security protection of physical facilities, network, computer system, software application, and data still work in a cloud environment, and constructing a cloud environment should obey the common international information security standards such as ISO27001.
Therefore, the traditional security practice mechanisms should be assured for a secure cloud environment.

6.1.2. Virtualization Security Risks Assessment

Regardless of a public or private cloud, the construction and deployment of a cloud environment cannot lack numerous virtualization products. Therefore, we need to assess the merits and drawbacks and security level of various virtualization technology resolutions and suite products, and choose the best one to reduce the security risks brought by virtualization.

6.1.3. Development Outsourcing Risk Control

Constructing a cloud environment is a large-scale systematic engineering with heavy work load and many advanced technologies, so it is hard to take charge of all development work for an organization. A practical action is to handover partial development work to several outsourcing parties, which will introduce some security risks. Therefore, we should identify the security risks incurred by outsourcing service and establish strict control strategies to assure their quality level and security requirement.

6.1.4. Portability and Interoperability

Customers must keep in mind that they may have to change service providers for the sake of unacceptable cost increase at contract renewal time, business operations ceasing by service providers,

partial cloud service closure without migration plans, unacceptable service quality decrease, and business dispute between cloud customer and provider etc. Therefore, portability and interoperability should be considered up front as part of the risk management and security assurance of any cloud program.

6.2. Securely Operation Strategies of Cloud Computing[12]

6.2.1. Business Continuity Assurance

Rapid change and lacking transparency within cloud computing requires that business continuity plan and disaster recovery expertise be continuously engaged in monitoring the chosen cloud service providers.

Regular inspections of a cloud service provider about cloud infrastructure and its physical interdependencies, disaster recovery and business continuity plans, contract documentation about security control action, recovery time objectives (RTOs), and access to data should be performed.

6.2.2. Attack Proactive Alerting

Security incidents will be inevitable during in a cloud environment's operation. As cloud is an ultralager-scale distributed network system that contains a lot of physical infrastructure, host system, and business application, the range attacked by malicious people is very widespread and traditional attack proactive alerting mechanisms in small network environment may fail to work. Therefore, how to monitor the network access all the time and alert timely on the malicious intrusion should be resolved.

6.2.3. Data Leak Prevention.

Sensitive data leak is an important security risk of cloud environment. There are two potential data leaking ways: static data leakage and dynamic data leakage. Static data leakage means that the data stored in data center, application memory and terminal memory is accessed and leaked by unauthorized users, dynamic data leakage means that the data being transformed in cloud environment is accessed and leaked by customer account hijacking or network channel wiretapping. Therefore, all static and dynamic data are facing the security risk of leakage and tamper, and how to resolve it should be concerned seriously.

6.2.4. Security Accident Notification & Response

Once security incidents occurred in a cloud environment, cloud service providers should notify their customers at first time, so as to customers can evaluate the potential damage incurred by these security incidents. Furthermore, cloud service providers should start the emergency plan to response these security incidents, including application-level firewalls, proxies, application logging tools, disaster recovery project, and cloud service backup etc. Therefore, cloud service providers should create their respective standard security incident response mechanisms.

6.2.5. Security Incidents Audit

To avoid the same security incidents occurring again, cloud service providers should find out the reasons of security incidents. Auditing can contribute to the reason analysis of security incidents in cloud environment. However, traditional security auditing techniques (e.g. security log, compliance check tools) might not satisfy the auditing demand of cloud environment. Therefore, cloud service providers should develop some new security auditing approaches. In addition, as a new evidence-obtaining way, electric discovery is gradually accepted by court. Courts now are realizing that information security management services are critical to making decisions as to whether digital information may be accepted as evidence.

While this is an issue for traditional IT infrastructure, it is especially concerning in Cloud Computing due to the lack of established legal history with the cloud

VII. CONCLUSION AND FUTURE WORK

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention.

However, the prevalence of cloud computing is blocked by its security to a great extent. To contribute some effort to improving the security of cloud computing, we surveyed the main existing security models of cloud computing, and summarized the main security risks of cloud computing from different organizations. Finally, we gave some security strategies against these common security issues of cloud computing. In the future, we will fulfill these security strategies with technology and management ways.

REFERENCES

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Oct 19, 2014].
[2] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In : ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009.
[3] "Internet Available:" http://www.ajocict.net/uploads/V6N5P13-2013_AJOCICT_-_Paper_13.pdf [Oct 20, 2014].
[4] http://www.onlinetech.com/resources/wiki/cloud-computing/private-cloud-security-how- your-data-security-changes-in-the-cloud[Oct 20, 2014].
[5] Cloud Security Alliance. Top Threats to Cloud Computing, 2010. http://www.cloudsecurityalliance. Org accessed on: March,2010.
[6] Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.
[7] "Internet Available": http://www.jisajournal.com/content/4/1/5 [Oct 20, 2014].
[8] "Internet Available": http://www.thewindowsclub.com/security-issues-with-cloud-omputing [Oct 20, 2014].
[9] Hashizume et al. Journal of Internet Services and Applications 2013,4:5 http://www.jisajournal.com/content/4/1/5
[10] "InternetAvailable":http://www.seu.ac.lk/fac/freedownload/Advantages%20and%20Challenges%20of%20Adopting%20Cloud%20Computing%20from%20an%20Enterprise%20Perspective.pdf
[11] "Internet Available": http://www.ijcsits.org/papers/vol3no52013/3vol3no5.pdf [Oct 21, 2014].
[12] 2011 International Conference on Power Electronics and Engineering Application Study on the security models a nd strategies of cloud computing http://www.shahidalamolhoda.ir/Files/3.pdf

