# Review on Cloud Computing and Security Issues in Cloud

Prof. Bhavani. S, Ankit Hatwal
[1]Assistant Professor , SITE, VIT University, Vellore, India
SITE, VIT University, Vellore, India

***Abstract—*** Today cloud computing is one of the new trends emerging in IT sector which allows us to access large number of applications as utilities over the internet. By providing large data storage, different on-demand services, virtualization, data sharing, data accessibility etc., it reduces the operational and capital cost. Cloud computing provides three different fundamental service models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) that makes the cloud computing feasible and accessible to the end user. There are many issues in the cloud computing and security is one of the main issues. Data leakage, data availability, data privacy, load balancing, network security are some of the security issues and threats in cloud computing. In this paper, we review what cloud computing is, the various cloud models and the main security risks and issues.

***Keywords— Cloud computing, Ssecurity issues, Cloud models, Cloud Service, Cloud Service Provider (CPS).***

## I. INTRODUCTION

Cloud computing is the future of IT technology. Today everything that we do on our computers is web based and not desktop based. Cloud computing is the technology that is playing the major role in making everything web-based. The term cloud refers to network or internet and it provides service over the network. Cloud consist of thousands of computers and servers, all linked together and accessible over internet. Most of the applications that we uses in modern era like email, image sharing, calendar, documents, web conferencing, customer management relation etc. all run in cloud. Cloud can be said to be divided into two parts: Front part and the back part [1]. The Front part includes the users and the customers. The second part includes collection of various computers, data storage and servers. The front part and back part are connected with each other via internet. Cloud computing is also a new mode of business computing, and most of the companies are preferring it because of its different service providing capabilities such as anywhere and anytime accessible, large data storage, pay as you use and so on just by using simple internet connection.. As cloud computing is widely adopted across many industries sectors and is very vast area of technology, there still exist many issues in cloud computing. Many surveys have been done and they show that data security and privacy risks are one of the primary concerns for people to shift to cloud computing [2]. Due to security issues in cloud computing the adoption of this technology has slow down. Figure 1 shows the IDC survey that ranked the security challenges first [3].

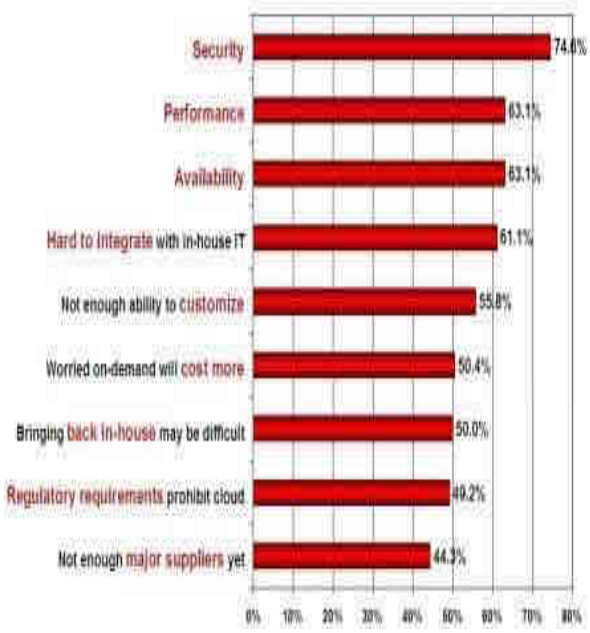


*Fig. 1. Results of IDC survey ranking security challenges, 2008.*

## II. WHAT IS CLOUD COMPUTING

As described by Ian Foster "Cloud computing is a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet". Cloud computing is everywhere, the only problem is that every person has its own perception about the cloud computing. Some of the great researchers, scientist and research organization have described the cloud computing as,

i) "Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center"-Lewis Cunningham.
ii) "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and

virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers."-Rajkumar Buyya.

iii) "A style of computing in which massively scalable IT-related capabilities are provided as a service using internet technologies to multiple external customers"-Gartner (Gartner 2008b)

iv) "An emerging IT development, deployment and delivery model, enabling real time delivery of product, services and solution over the internet(i.e. enabling cloud services)"-IDC (Gens 2008)

v) "The idea of delivering personal (email, word processing, presentation) and business productivity application (sales force automation, customer service, accounting) from centralized servers"-Merrill Lynch.

vi)

### *A. CLOUD SERVICE MODELS*

With cloud computing the software we use are stored in the server at unknown place accessed via internet and not on our personal computers. And to the users this technology and infrastructure behind the cloud is invisible. These cloud services are provided to the users, built around three different fundamental cloud service models

*A.1.* **Software as a Service (SaaS) -** This layer provides business applications that are hosted by the service providers and are running on the cloud infrastructure. The applications are accessible from various customer devices through interface such as web browser. The cloud service provider manages and controls the underlying cloud infrastructure, servers, network, storage, operating systems, and even individual application abilities, but some restricted user-specific application configuration settings are managed by the customers [4]. Google Docs, Evernote are some of the examples of SaaS.

*A.2.* **Platform as a Service (PaaS)** – This layer offers environment which is used by IT organizations to create cloud ready business applications. Here also the consumer does not manage or control the underlying cloud infrastructure. This layer allows programmers to code and use the different tools offered by the service. Force.com, Microsoft Azure are some popular example of PaaS.

*A.3.* **Infrastructure as a Service (IaaS)** – This layer offers storage, processing, networks and other fundamental computing resources that developers and IT organizations uses to deliver custom business solutions. The IaaS consumers does not have authority to manage or control the underlying cloud infrastructure but they have control over operating systems, storage, deployed applications and limited control on the networking components like firewalls. Amazon S3 and EC2, Rackspace are some examples of IaaS.

### *B. CLOUD DEPLOYMNT MODELS*

The cloud computing is deployed through four different deployment models with different characteristics that support the needs and requirements of the customers.

*B.1.* **Private cloud**- A private cloud gives a single Cloud Consumer's organization the exclusive access to use the infrastructure and computational resources. The infrastructure is operated solely for a single organization. It may be managed by the third party or the organization itself and may exist on-premises or off-premises. When it is hosted in organizations premises it is known as on-premises and when outsourced to hosting company it is known as off-premises. Private cloud is more costly and more secure as compared to public cloud. Unlike in public cloud environment, there are no extra security ordinance and guidelines, legal requirements and bandwidth restrictions in private cloud environment. By using private cloud, control of the underlying infrastructure is enhanced and security is also improved since user's access and the networks used are confined to specific users [5].

*B.2.* **Public cloud** – A public cloud offers the cloud infrastructure to general public or a large industry over the public network. It is owned by the organizations selling cloud services and serves as a diverse pool of clients. Consumers access the resources and only pay for the operating resources. Though the public cloud environment has many advantages like better elasticity, better utilization rates, greater economies of scale etc. but still there exist hidden risk of security, regulatory compliance and quality of service (QoS) [6].

*B.3.* **Community cloud** – A community cloud is shared by the group of organizations that have the same concerns, mission objectives, policies, requirements, values and security concerns. Similar to private cloud it may be managed by the organization or by third party and can be implemented either on customer premises or outsourced to hosting company. The costs are shared among the users than a public cloud. Hence a community cloud benefits from medium costs as a result of a sharing policy.

*B.4.* **Hybrid cloud** - A hybrid cloud is a combination of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability. Hybrid clouds provide the flexibility of in-house applications with the fault tolerance and scalability of cloud based services.

## III. CLOUD COMPUTING SECURITY ISSUES

Today cloud computing, no doubt is an emerging and trending area in IT sector but it doesn't come without its drawback. Cloud computing comes with numerous possibilities and challenges simultaneously. From the different challenges, security is considered to be a critical issue and one of the most crucial barriers for cloud computing in its path of success [7]. As security and privacy issues still constitute to significant challenges, they should be resolve before Cloud Computing makes huge impact in the market [8].

### *A. Data privacy and Security*

Data privacy and security has been identified as one of the main concerns for widespread adoption of cloud services. As user provide CSP's with their sensitive and critical data, it becomes important for service providers to secure the privacy and security of user data. Data in cloud is globally distributed on multiple third party servers which raise concerns about jurisdiction, data exposure, data leakage and privacy. A CSP needs to ensure that private data of its clients is protected from unauthorized discloser.

### *B. Performance and Reliability*

When a user access resource that is not located in their premises, they need to be sure that they are satisfied by the services provided by the different CSP's. Additionally sometimes failures may occur and how users are notified and how quickly issues are resolved is critical. Users are highly dependent on cloud service providers. As there are different CSP's so are their different service models, for using cloud services customer have to select a particular CSP which may bound them or they may be locked in, which brings potential business security risk [9]. If a cloud storage system is unreliable, it becomes a liability to users to save their data in cloud.

### *C. Transparency*

This is the difficulty that users have to face while auditing their IT resources since they don't have true visibility in the cloud they can't be sure that who has access to their data and how they can keep people out of their sensitive data. To ensure reliability and more complete understanding and to trust cloud service stability, users need transparency. Public cloud is more transparent as compared to private or hybrid cloud models. Transparent security would prevent cloud providers from disclosing sensitive information about customer's security policies, design and practices [10].

### *D. Lack of control*

This is one of the biggest issues when using cloud computing. By design the company gives up control when they sign up to use firm's cloud resources. This means that cloud provider can make changes to cloud infrastructure without informing the users at any time. There are threats associated with the data being stored, processed remotely and sharing of platforms between users. In many cases individuals are requested for their personal information which arises concerns that why it is asked or how will information be used or passed on to other groups. This lack of control arises suspicion and eventually distrusts [11].

### *E. Service Level Agreements (SLA)*

When consumers migrate their core business to entrusted cloud, they need to ensure the reliability, quality, availability, performance and accessibility of the resources. So, it's important for the customers to get assured that providers deliver the services. This can be provided by SLA i.e. the negotiation or agreement between the customer and service provider. SLA is provided by the service provider as the service based agreement rather than customer based agreement.

### *F. Identification management*

Most cloud applications will be deployed to provide access to mobile users. Important concern here is how user gets access and how to prevent fraud access. While the application in the cloud are convenient, provisioning user access and authorizing user to access application is much more challenging. If organizations don't have identification management strategy then the cost can be enamours. At the same time most of the organizations have to perform quarterly security audits to trust regulatory compliance.

### *G. Multitenancy*

Multitenancy is a key security concern in cloud. Multitenancy is a concept where multiple virtual machines (VM's) are stored in a single infrastructure, or are hosted by a single server. In case of public cloud different organization or customers may use different VM's stored in same infrastructure or server. This is where Multitenancy brings new security threats where same infrastructure and resources are shared thus increasing the attack surface. For CSP's also this brings new challenges as they to enforce uniform security controls and measures.

### *H. Law and jurisdiction*

To overcome the data loss and availability problem, data in the cloud is replicated and stored in different location that is unknown to the customers. Data may be stored in different places or in different country. The security concern here is that the data that is secured in one country may or may not be secured in other due to different laws for example Data stored in Europe comes under EU legislation and data stored in US comes under US legislation which are different from each other. Catteddu [12] has categorized some of the legal risks that are associated with cloud computing as follows:

- Subpoena and e-discovery

- Risk from changes of jurisdiction
- Data protection risks
- Licensing risks

*I. **Network security***

As data is transferred to servers through network, so network need to be secured. Main concern here is the leakage of sensitive information and malicious attacks on data. Sharing of resources between servers through network allows attackers to launch cross-tenant attacks [13]. While interconnectivity in VMs is an important security challenge in cloud computing, Virtual Networks is a solution to this challenge [14].

*J. **Virtual Machine***

VM theft is a big security threat. VM theft is a vulnerability that enables an attacker to copy or move a VM in an unauthorized manner. Virtual machine is saved as a file in the virtual environment, so if the file does not have proper access privilege it can be attacked in a malicious way. Copy and move restrictions are essential to safeguard against VM theft and this can be achieved by limiting these restrictions to critical/sensitive VMs only.

## IV. CONCLUSION

No doubt cloud computing offers many potential benefits to enterprises such as lower cost, rapid elasticity, unlimited data storage, anytime accessibility, pay as you use, fast deployment, improved performance, instant software updates, document format compatibility and so on, there are still some security issues that need to be taken into account. In this paper some of the key security issues and threats which are currently faced by cloud computing are highlighted. Although having discussed different security issues, if they are solved in future, cloud computing has potential to provide one of the most important IT technology solutions.

## REFERENCES

[1] Manju, Dr. P.C. Vashist, Security Issues related with cloud computing, Int. Journal of Engineering Research and Applications, Vol. 4, Issue 9( Version 1), September 2014, pp.83-86.

[2] Randolph Barr, Qualys Inc, “How to gain comfort in losing control to the cloud”.

[3] Kuyoro S. O., Ibikunle F. & Awodele O, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.

[4] Florin OGIGAU-NEAMTIU, CLOUD COMPUTING SECURITY ISSUES, Journal of Defence Resource Management, Vol. 3, Issue 2(5):2012.

[5] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, Cloud Computing: Security Issues and Research Challenges, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[6] Dr Dwivedi S K, Dr Kushwaha D S, Maurya Ankit, Security Issues And Resource Planning In Cloud Computing, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 2 Feb 2013.

[7] Monjur Ahmed, Mohammad Ashraf Hossain, CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[8] CEPIS, Cloud Computing Security and Privacy Issues, available at: http://www.cepis.org/index.jsp?p=641&n=825&a=4758.

[9] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues, Computational Intelligence and Software Engineering (CISE), Dec 2010.

[10] Brodkin J, 2008, ‘Gartner: Seven cloud-computing security risks’, Infoworld, viewed 13 March 2009, available at: http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853?page=0,1.

[11] Catteddu, Daniele. “Cloud Computing: benefits, risks and recommendations for information security”. Springer, Berlin Heidelberg, 2010.

[12] Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50-57.

[13] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). DC, USA: IEEE Computer Society Washington. pp 18-21.

[14] Wu H, Ding Y, Winer C, Yao L (2010), “Network Security for virtual machine in Cloud Computing”. In: 5th International conference on computer sciences and convergence information technology (ICCIT). DC, USA: IEEE Computer Society Washington. pp 18-21.