A Survey on Cloud Security and Various Attacks on Cloud

Sana Khan   Shumaila Khan   Zuber Farooqui

ABSTRACT
Cloud computing provides a means to store and process data through a collection of resources which can be accessed online. Cloud is a collection of storage and physical machines which are termed as datacenter. Cloud consists of many datacenters located at geographically different places. Every physical machine of datacenter can handle more than one user. Virtualization is the technology behind the cloud to utilize the resources. Virtualization offers that many virtual machines corresponding to every task of user can be submitted for execution on the same physical machine. The virtual machine will get destroyed as soon as task will be finished. To balance load of the cloud datacenters these virtual machines are migrated between physical machines. In this paper a survey is done on cloud security issues.

Keywords
Cloud, hypervisor, malware, side channel attack

1. INTRODUCTION
The cloud computing is computing technique within which giant teams of remote servers square measure networked to permit centralized information storage and on-line access to laptop services or resources. It provides flexibility and completely different computing platform for organizations. The Interest is associate example of cloud computing, it's a free web site that needs registration to access, wherever users will transfer, save, type and manage pictures called pins and different media content like videos and pictures, through collections called inboard. It viewed by around seventeen million folks per month and encompasses a nice storage capability. It's hosted on Amazon's cloud platform [2]. Initially, because of absence of cloud computing, maintaining security of the knowledge had been terribly tough task.

However, introduction of the cloud computing has created life straightforward. The cloud consists of bound components like purchasers, servers and therefore the main center wherever all servers square measure managed [3]. Figure 1.1 shows the design of cloud ADP system, wherever the info owner stores the info and applications to the cloud storage. Whenever user required to access information and applications, the owner offers access to the user through the cloud.

Cloud computing could be a model for providing service as Platform, Software, Hardware as a service over web facultative present, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) which will be quickly provisioned and free with nominal management effort or service supplier interaction [1]. Cloud computing is that the latest effort in delivering computing resources as a service. User will rent computing resources on-line as a product these computing resources are utilized by user on-line [1], this helps in reducing prices {and offer andsupply}rest can take hold of it and provide on demand service that's delivered to customers over the net from large-scale information centers or "clouds". While cloud computing is gaining growing quality within the IT trade. Cloud Computing contains assortment of distributed servers called masters World Health Organization offer demanded services and resources to the purchasers called central controller or cloud manager in a very network with the measurability and liableness of servers. On-demand service is provided by distributed servers. Services are also of computer code resources (e.g. computer code as a Service, SaaS) or physical resources (e.g. Platform as a Service, PaaS) or hardware/infrastructure (e.g. Hardware as a Service, HaaS or Infrastructure as a Service, IaaS). Amazon EC2 (Amazon Elastic work out Cloud) is associate example of cloud computing services. Cloud services square measure provisioned to use by service suppliers, for instance, Amazon, Google on the net. Usually, the resources accessible to the user of the cloud square measure virtualized that's (PaaS, IaaS, and SaaS) services square measure virtual service. User gets needed service with none dependencies or constraints reciprocally firms can take some charge for mistreatment their services that square measure nominal as compared to the particular price of that specific service, thanks to this cloud is changing into standard. Cloud computing technology uses web and central remote servers to keep up information and applications [2]. Cloud computing permits any user from anyplace to use the updated version of services and application. We'd like to not purchase computer code with the license as a result of change and maintaining computer code square measure the server's responsibility, solely we'd like to own web affiliation; therewith we will use applications while not putting in it on our system. Gmail, yahoo mail or Hotmail, etc. square measure the common and wide used cloud example, for mistreatment any reasonably cloud service, you need to have a web affiliation. Scientific application desires an outsized quantity of calculation and storage that you desire an outsized computation storage and power. Initially, all the scientific applications square measure deployed on Grid [3]. However, Grid computing is dear and not accessible everywhere the word. Thus the scientific applications square measure moving toward the cloud, Cloud provides another to grid and supercomputers for a person in a very lower price. Cloud is associate rising space and excellent for this type of application. For the advance of deploying associate application of cloud there square measure such a big amount of methods developed, for instance load reconciliation, planning algorithmic program for VM allocation in cloud.
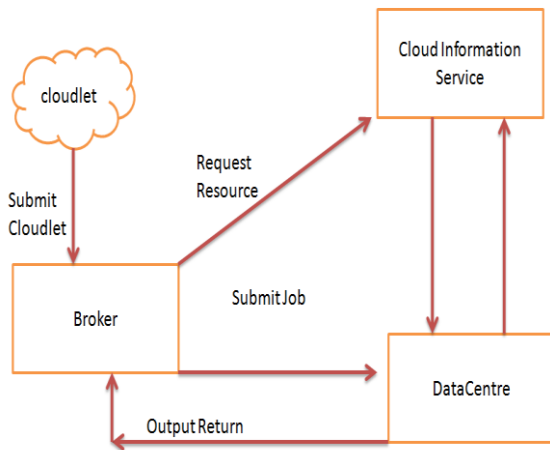
Fig 1: cloud computing architecture

2. TYPES OF CLOUD

There are four types of cloud computing exists which are described as follows.

There are four types of cloud computing exists which are described as follows.

- **Public cloud**

Publically cloud, any subscriber will access data from the cloud house with an online affiliation. Public clouds are in hand and operated by third parties; they deliver superior economies of scale to customers, because the infrastructure prices are unfold among a combination of users, giving every individual shopper a beautiful inexpensive, "Pay-as-you-go" model. All customers share a similar infrastructure pool with restricted configuration, security protections, and convenience variances. These are managed and supported by the cloud supplier. one among the benefits of a Public cloud is that they'll be larger than AN enterprises cloud, so providing the flexibility to scale seamlessly, on demand.

- **Private cloud**

a non-public cloud is for specific cluster or organization and limit access to simply that cluster. Non-public clouds are designed solely for one enterprise. They aim to deal with issues on information security and supply larger management that is usually lacking in a very public cloud.

- **Community cloud**

In community cloud, 2 or a lot of organizations that have similar cloud needs, share their intelligence.

- **Hybrid cloud**

Hybrid cloud contains of the mix of minimum 2 clouds, will be a mix of public, community or non-public cloud. Hybrid Clouds mix each public and personal cloud models. With a Hybrid Cloud, service suppliers will utilize third party Cloud suppliers in a very full or partial manner so increasing the pliability of computing. The Hybrid cloud setting is capable of providing on-demand, outwardly provisioned scale. The flexibility to reinforce a non-public cloud with the resources of a public cloud will be wont to manage any surprising surges in work.

Table 1: security issues in different types of cloud

Model	Cost issues	Security issues	Control issues	Legal issues
Public	Setup: highest	Least secure	Least control	Jurisdiction of storage
Private	Setup: high	Most secure	Most control	-
Community	Relatively low	Less secure	Less control	-
Hybrid	Moderate	Least secure(better than public)	Least control(better than public)	Jurisdiction of storage

3. GARTNER SEVEN CLOUD COMPUTING SECURITY

According to 'Gartner' the cloud computing has "unique attributes that need risk assessment in areas like information integrity, recovery, privacy Associate in Nursingd an analysis of legal problems in areas like e-discovery, regulative compliance and auditing"[20][21].

The following seven specific security problems ought to customers rise with venders before choosing a cloud vendor.

- Privileged user access

The client ought to have data concerning those users UN agency have given privileged access, to produce specific data. On the hiring and oversight of honored directors and therefore the controls over their usage.

- Regulatory compliance

Customers have the responsibility for security and confidentiality for his or her own information, even once it's control by a service supplier.

- Data location

The cloud solely stores user's information in its own space for storing, user specifically doesn't understand the situation of knowledge that wherever is it stored? User ought to realize the info supply report from the cloud supplier.

- Data segregation

The cloud suppliers ought to have ability for secure delivery of cloud information, for privacy the simplest coding techniques applied on cloud data; this should be ensured by cloud supplier.

- Recovery

The backup or restoration method ought to be on the market within the system within the case of any disaster or failure.

- Investigative support

Investigation of cloud information square measure lately tough method attributable to language in and mistreatment information for varied customers can be co-located and conjointly might cover completely different hosts and information centers. once the written agreement commitment to support specific sorts of investigation, with warranty that the cloud supplier has already with success supported such activities, the user permits themselves to use those cloud information.

• Long-term viability

If the cloud supplier gets nonheritable and enveloped, the user should take care that the info can stay on the market even once such an incident. The user/subscriber ought to raise to the cloud supplier concerning the info replacement or restoration of system within the case of any demand.

4. ATTACKS ON CLOUD

As a lot of corporations square measure moving to cloud computing. Thus, hackers are increasing within the same field. a number of the potential attack vectors that hacker could try include:

4.1 Denial of Service (DoS) attacks:

A denial of service (DoS) attack could be a malicious decide to build a server or a network resource inaccessible to users, sometimes by briefly interrupting or suspending the services of a bunch connected to the net [22]. The cloud suppliers use sort of ways to partition resources in such the simplest way that denial of services, whether or not accidental or deliberate square measure less doubtless to happen. suppliers like Amazon divide their cloud into "availability zones" that square measure designed to fail severally [23]. Tomaximise time period, developers should replicate their applications in multiple zones and permit fail over between them.

4.2 Breach of confidentiality

With collocation-based breaches of confidentiality, attackers decide to use collocation so as to compromise the confidentiality of a virtual machine (VM). info concerning the info hold on within a VM may be inferred by noticing patterns of resource usage, significantly electronic equipment usage. Such resource usage may be inferred through resource rivalry with a co-located assaulter virtual machine [23].

4.3 Cloud Malware Injection Attack

a primary significant attack try aims at injecting a malicious service implementation or virtual machine into the cloud system. Such reasonably cloud malware will serve any specific purpose the opponent is fascinated by, starting from eavesdropping via delicate information modifications to full practicality changes or blockings [24].

4.4 Side Channel Attacks

Associate degree assaulter may decide to compromise the cloud by inserting a malicious virtual machine in shut proximity to a target cloud server then launching a aspect channel attack [25]. Side-channel attacks have emerged as a sort of effective security threat targeting system implementation of scientific discipline techniques. Evaluating a scientific discipline system's resilience to side-channel attacks is thus vital for secure system style.

4.5 Authentication Attacks

Authentication could be a liability in hosted and virtual services and is often targeted. There square measure many alternative ways that to manifest users [26]; For example, supported what someone is aware of, has, or is. The mechanisms wont to secure the authentication method and also the ways used square measure a frequent target of attackers. Currently, concerning the design of SaaS, IaaS and PaaS, there's solely IaaS giving this sort of data protection and encryption.

4.6 Man-In-The-Middle scientific discipline Attacks

This attack is distributed once associate degree assaulter places himself between 2 users. Anytime attackers will place themselves within the communication path, there's an opening that this may result in interception and modification of the message [26].

5. CONCLUSION

In this paper a survey is done on cloud computing security risks. As cloud is been widely used so its security is a prime concern. Gartner cloud computing risks and various attacks have been discussed in this paper.

6. REFERENCES

[1] P. Mell, and T. Grance, "The NlST Definition of Cloud Computing," vol 15, 2009.

[2] S. Dogra and Sahil, "Cloud Computing and its Security Concerns A Survey," *International Journal of Innovative Technology and Exploring Engineering*, vol 3, no. 12, pp. 15-18, May 2014.

[3] K. Weins, *Cloud Computing Trends: 2014 State of Cloud Survey*, accessed December 15, 2014, http://www.rightscale.com/blog/cloudindustry-insights/cloud-computing-trends-2014-state-cloud-survey.

[4] D. Hubbard, and M. Sutton, "Top Threats to Cloud Computing V1. 0," *Cloud Security Alliance*, 2010.

[5] Wikipaedia, *System Profiler*, accessed September 4, 2014,http://en.wikipedia.org/wiki/System_profiler.

[6] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," *10th European Conference on Information Warfare (ECIW), Tallinn, Estonia*, pp. 307-314, 2011.

[7] K. Xu, F. Wang, and L. Gu, "Profiling-as-a-service in multi-tenant cloud computing environments," *32nd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 461- 465, 2012.

[8] J. W. Rittinghouse, and J. F. Ransome, *Cloud computing: implementation, management, and security*, CRC press, 2009.

[9] U. Oktay, and O. K. Sahingoz. "Proxy Network Intrusion Detection System for cloud computing," *IEEE International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE),"* pp. 98-104, 2013.

[10] M. Rouse, *Fuzzy Logic*, accessed September 5, 2014, http://whatis.techtarget.com/definition/fuzzy-logic.

[11] J-SR Jang, "ANFIS: adaptive-network-based fuzzy inference system," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 23, no. 3, pp. 665-685, 1993.

[12] C.C. Lee, "Fuzzy logic in control systems: Fuzzy logic controller-Part II," *IEEE Transaction on. System., Man, Cybernetic,* vol. 20, no.2, pp. 404-418, 1990.

[13] C.C. Lee, "Fuzzy logic in control systems: Fuzzy logic controller-Part II," *IEEE Transaction on. System., Man, Cybernetic,* vol. 20, no.2, pp. 419-435, 1990.

[14] J. Mirković, D. Cvetković, N. Tomča, S. Cvetićanin, S. Slijepčević, V. Obradović, M. Mrkić, I. Čakulev, L.

Kraus, and V. Milutinović. "Genetic algorithms for intelligent internet search: a survey and a package for experimenting with various locality types," *IEEE TCCA Newsletter*, pp. 118-119, 1999.

[15] M. Skinner, *Genetic Algorithms Overview*, accessed September 12, 2014, http://geneticalgorithms.aidepot.com/Tutorial/Overview.html.

[16] D. H. Park, Y. Choi, H. K. Kim, and J. K. Kim, "A Review and Classification of Recommender Systems Research," *International Proceedings of Economics Development & Research*, vol. 5, no. 1, 2011.

[17] C. Chen, D. J. Guan, Y. Huang, and Y. Ou, "Attack Sequence Detection in Cloud Using Hidden Markov Model," *Seventh IEEE Asia Joint Conference on Information Security (Asia JCIS),"* pp. 100-103, 2012.

[18] W. R. A. Ibrahim, and M. M. Morcos, "Artificial Intelligence and Advanced Mathematical Tools for Power Quality Applications: A Survey," *IEEE Power Engineering Review,*vol. 21, no. 11, pp. 62-62, 2001.