International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Security Concerns in Cloud Computing

Gopal K. Shyam*, Mir Abdul Samim Ansari
*Associate Professor,
School of C&IT, Reva University, Bangalore, Karnataka, India

ABSTRACT
Cloud computing is a revolutionary way of storing and accessing data with five essential characteristics, three service models, and four deployment models. Businesses have realized the tremendous potentiality and benefits of cloud computing and have accepted the technology, but still a small amount of scepticism hovers around. In defiance of its potential characteristics, the organizations risk their sensitive data by storing it in the cloud. In this paper, we have identified various privacy and security challenges associated with the novelty of cloud computing. The security and privacy challenge listed in this paper perceives demand for implementation of sophisticated technologies to deal with them.

Keywords: *Cloud Computing Security, Network security, and Distributed Networks Security*

1. INTRODUCTION

In the evolution of distributed systems, clouds have become a new trend and grid computing being the forerunner. Cloud computing was introduced in the industry by the companies like Microsoft, Sales force, Amazon, Google and Yahoo. Cloud computing has centralized server resources in a distributed architecture such that it can provide on-demand service or resources on a scalable platform. Cloud computing is based on pay-on-usage model for allowing convenient and provide access to a shared pool of configurable resources [1] [4] [5].

The pay-on-usage characteristic of cloud enables the cloud service providers offer services to the customers to utilize and create their own web services. Generally the cloud purveys three services, i.e., to lease a business application (Software as a service or SaaS), to lease computing and storage (Infrastructure as a service or IaaS), and to build a remote platform and customize according to business processes (Platform as a service or PaaS) [1] [2] [3] [4].

The organizations prefer an IT solution that comprises cloud computing for various reasons as they just have to pay with respect to resource consumption. The management and control of the cloud infrastructure is encapsulated from the users, therefore, the burden of organization’s infrastructure management is diminished. Cloud has four deployment models through which it can offer services to the costumers: Public cloud, Private cloud, Hybrid cloud, and Community cloud.

A deployment models that allows the public to use the resources dynamically and on self-service basis over the internet hosted by a third party is called the public cloud. The data is stored in the cloud provider’s data center and the provider is accountable for maintaining it. The public clouds are comparatively less secure as they are prone to malicious attacks. Private cloud provides a discrete and reliable cloud environment that can be operated only by an authorized client. The authorized client has the privilege to configure and manage according to their requirements. An additional advantage of this model is that the availability of resources to all the departments is enhanced. The private cloud is secure as it is confined only to an authorized organization. A hybrid cloud provides IT resources through a combination of public and private cloud. Hybrid clouds are private clouds that are managed centrally, provisioned as a single unit through a restricted secure network, and linked to other cloud services [1].

The community cloud infrastructure purveys the resources to be shared among a group of organizations for a purpose. In this, the cloud can be managed by the organizations themselves or given to the third party to manage it. These clouds have an agreement between the related organizations.

2. Cloud Security Composition

The confidentiality and integrity of the users data within the cloud is a huge responsibility and a major concern. The users might store valuable information in cloud are not aware of what is happening to it in the cloud, therefore, the information has to be safeguarded without the user's privacy being compromised. The security of data in cloud is becoming extensively demanding with the growing technology as the loopholes in it is targeted by the attackers to gather user's information in cloud [1] [6] [9].

The cloud service provider should have the important security components such as the SLA monitor, load balancer, Resource monitor, Pay-per-use monitor, etc. The protection of data, attack on interfaces, attack on software and hardware virtualization, etc., are a few security issues in cloud. The virtual machines in cloud are created using the hypervisor, also known as Virtual Machine Monitor (VMM). The VMM creates virtual resources depending on the capacity of the underlying physical resources. A few security issues at the virtual machine layer are: virtual machine sprawl, identity management, access management, hypervisor protection, visibility lack of virtual network, etc.

Cloud Security Alliance and Open Security Architecture are organization that work on the security of cloud computing. The focus on the security issues and foster practicing the best vulnerability mitigation procedures, The other standards that focus on cloud security are Internet Engineering Task Force and Storage Networking Industry Association [8].

3. Cloud Computing Challenges

Protection and private ness square measure the two primaries worries concerning cloud computing. Within the cloud computing international, the virtual surroundings cloud clients get admission to computing energy that exceeds that contained inside their physical international. to travel into this virtual environment a user is to transfer records within the course of the cloud. There for many issues of safety arises [4] [7] [8] [16].

Figure 1: Challenges of Cloud Computing

3.1 Information Security

It is attached shielding the confidentiality, integrity and accessibility of statistics irrespective of the shape the data may to boot take [9].

Losing control over data:

These can be extensively arranged as dread of losing control

- ➢ The cloud world is altogether different from on-Prem corporate processing.
- ➢ The cloud specialist organization claims the physical Premises and controls access to the offices.
- ➢ The supplier possesses the equipment, programming, and system get to, none of which are committed to any single Client.
- ➢ Multiple clients could be utilizing the assets (multi-Occupancy) in the meantime.
- ➢ Common specialized and activities principles apply over all Clients.
- ➢ SaaS applications are pre-characterized and might be Configurable yet have restricted customization.

Data Uprightness:

Information uprightness is en sure that realities alterations least complex in response to approved exchanges. For example, if the supporter is chargeable for building and approving database questions and the server executes them aimlessly, the interloper will for the most part be fit for control the client viewpoint code to accomplish something he has authorization to do with the back-end database. Typically, which means the gatecrasher can read, change, or erase records voluntarily [3]. The basic stylish to ensure certainties honesty does not yet exists [8]. On this new universe of processing clients are all around required to just acknowledge the basic commence of acknowledge as valid with. In truth, a couple have guessed that concur with is the greatest concern managing distributed computing [7].

Danger of Seizure:
In an open cloud, you are offering figuring assets to different organizations. Uncovering your information in a domain imparted to different organizations could give the administration "sensible reason" to grab your advantages on the grounds that another organization has disregarded the law. Basically in light of the fact that you share the earth in the cloud, may put information in danger of seizure [4][8]. The main security against the danger of seizure for client is to encode their information. The subpoena will urge the cloud supplier to turn over client's information and any entrance it may have to that information, however cloud supplier won't have client's entrance or unscrambling keys. To get at the information, the court should come to client and subpoena client. Subsequently, client will wind up with a similar level of control client have in his private server farm [4] [16].

Disappointment in Supplier's Security:
Disappointment of cloud supplier to appropriately secure segments of its foundation – particularly in the upkeep of physical access control – brings about the bargain of supporter frameworks. Cloud can contain various substances, and in such a setup, no cloud can be more secure than its weakest connection [3][7]. It is normal that client must put stock in supplier's security. For little and medium size organizations supplier security may surpass client security. It is by and large troublesome for the points of interest that assistance guarantee that the correct things are being done [3] [7].

Cloud Supplier Goes Down:
This situation has various variations: chapter 11, choosing to take the business toward another path, or an across the board and expanded blackout. Whatever is going on, endorser chance losing access to their generation framework because of the activities of another organization, Supporter likewise hazard that the association controlling endorser information won't not ensure it as per the administration levels to which they may have been beforehand dedicated [4]. The main choice client have is to picked a moment supplier and utilize mechanized, consistent reinforcements, for which numerous open source and business arrangements exist, to ensure any present and recorded information can be recouped regardless of whether client loud supplier were to vanish from the substance of the earth [4].

3.2 Network Protection

The important network security categories are:

Disseminated Refusal of Administration assaults: are specific kinds of Foreswearing of Administration assault. Disseminated Refusal of Administration assaults have turned into an instrument of decision for noxious associations around the world. In a DOS assault, the expectation is to a web application inaccessible to its proposed clients, more often than not by flooding the objective application with counterfeit activity or solicitations, which can over-burden frameworks and keep authentic movement from achieving the application server. In a Disseminated Refusal of Administration assaults assault, the assailant utilizes various sources to dispatch the phony activity normally tens or a huge number of traded off frameworks (referred to all in all as a botnet). This makes it hard to stop the assault by distinguishing and hindering a rundown of particular sources. Hence, Disseminated Refusal of Administration assaults can accomplish more harm than common Disseminated Refusal of Administration assaults assaults, by making your business-basic applications inaccessible to authentic clients for a more drawn out timeframe [14].

Man in the Center Assault:
A technique for recognizing a man-in-the-center assault against correspondences between a customer gadget and a particular remote end point over a system, the strategy utilizing test programming introduced on the customer gadget, the technique including the test programming sending an association start ask for from the customer gadget over the system, coordinated to the remote end point, to at any rate halfway start a safe system association between the remote end point and the customer gadget, accepting at the customer gadget encryption accreditations sent to the customer gadget in light of the association start ask for, the test programming contrasting the got encryption qualifications and expected encryption certifications for the remote end point, and the test programming confirming that a man-in-the-center assault is available if the gotten encryption certifications do no match the normal encryption qualifications [13].

IP Satirizing:
The gatecrashers imitate the IP address of a trusted host to get unapproved get to and send messages. To accomplish IP satirizing, the interloper should first execute different procedures to recognize the IP address of a put stock in have. Once the programmer distinguishes the IP address, the bundle headers can be altered and seems like it was sent by a confided in have. The gatecrashers imitate the IP address of a trusted host to acquire unapproved get to and send messages. To accomplish IP caricaturing, the gatecrasher should first execute different systems to distinguish the IP address of a put stock in have. Once the programmer recognizes the IP address, the parcel headers can be changed and seems like it was sent by a put stock in have. IP mocking is normally used to dispatch web assaults or to get unapproved access to PCs [15].

Port Filtering:
Sending inquiries to servers on the Web with a specific end goal to acquire data about their administrations and level of security, On Web has (TCP/IP has), there are standard port numbers for each kind of administration. Port checking is additionally generally used to see whether a system can be traded off. In referencing the system this could be a neighborhood in your home or office or it could be the Web. A system is traded off of frameworks with addresses and on those frameworks you have administrations. The address is called an "IP Address" and the Administration could be numerous things however is essentially programming that is running on the framework and open over the system on a port number. It could be a web server, email server or gaming server [8].

Packet Sniffing:
Packet sniffing by other Tenants: Packet sniffing is listening (with software program) to the uncooked network device for packets that hobby you [4]. When that software sees a packet that fits certain standards, it logs it to a record. The maximum commonplace criterion for an interesting packet is one that consists of phrases like “login” or “password” [12] [17].

It isn't possible for a digital example walking in promiscuous mode to receive or “sniff” site visitors that is meant for a one of a kind virtual example. At the same time as clients can place their interfaces into promiscuous mode, the hypervisor will not supply any visitors to them that aren’t addressed to them [9]. Even two virtual in stances which might be owned through the identical purchaser, located on the same physical host, cannot listen to each different site visitors. Assaults which include ARP cache poisoning do not paintings inside Amazon EC2. While Amazon EC2 does provide enough safety towards one patron inadvertently or maliciously attempting to view some other ought statistics, as a general practice client to encrypt sensitive visitors [9].

3.3 General Security Issues

They are more confused in a virtualized surroundings since you by and by must keep up music of security on levels: the physical host wellbeing and the virtual gadget security. On the off chance that the substantial host server's insurance will move toward becoming traded off, the greater part of the virtual machines living on that one of a kind host server are affected [20].

Example Separation:
Seclusion ensuring that unique kind occurrences walking around the equiva lent real device are remote from each extraordinary. Virtualization efficiencies in the cloud require virtual machines from different organizations to be co-situated on the indistinguishable substantial resources. Despite the fact that regular records focus security still applies inside the cloud condition, physical isolation and equipment fundamentally based security can't monitor contrary to assaults between virtual machines at a similar server [18].

Authoritative motivate section to is through the web as opposed to the over saw and compelled coordinate or on-premises association that is clung to inside the ordinary insights focus demonstrate. This development threat of presentation will require stringent following for changes in machine control and inspire passage to oversee confine [8]. Particular examples going for strolls at the indistinguishable contraption are segregated from each other by means of Xen hypervisor. Amazon is enthusiastic in the Xen People group, which guarantees insight of the stylish patterns. So also, the AWS firewalls live inside the hypervisor layer, among the real group interface and the example's virtual interface. All parcels need to by go through this buildup, therefore an illustration's buddies don't have any additional entrance to that occasion than some other host inside the net and can be dealt with just as they are on isolated physical hosts. The real Slam is isolated the utilization of comparable instruments [9] [15].

Host running device:
Chiefs with a business venture need to get passage to the administration designs are required to us multi-segment validation to access reason manufactured organization has and those regulatory hosts are structures which are extraordinarily outlined, built, arranged, and solidified to shield the control flying machine of the cloud. All such inspire admission to logged and reviewed [12] [11].

At the point when a worker never again has a business need to get to the control flying machine, the benefits and get right of section to those hosts and significant structures are disavowed [18].

Visitor working contraption:
Virtual occurrences are totally dealt with the guide of the client. Customers have finish root get to or regulatory control over cash owed, offerings, and projects. AWS does now not have any entrance rights to buyer times and can't sign into the guest OS [10] [17].

AWS prescribes a base arrangement of assurance top notch hones alongside: shopper must impair secret word basically based access to based access to their hosts, and make utilization of some state of multi-segment verification to advantage get passage to their circumstances, or at a negligible endorsements principally based SSH show 2 get section to [9] [13] [15].

Furthermore, clients should utilize a benefit heightening component with running surfing a steady with-individual establishment. For example, if the visitor OS is Linux, in the wake of solidifying their illustration, they should use endorsement based SSHv2 to get right of passage to the advanced case, cripple far away root login, utilize order line logging, and utilize 'sodu' for benefit heightening. Clients should produce their own one of a kind key combines a decent method to ensure that they are exceptional, and never again imparted to different clients or with AWS [9]. AWS Multi-issue Validation (AWS MFA) is an extra layer of security that offers more grounded control over AWS account settings. It requires a substantial six-digit, unmarried-utilize code from a confirmation gadget in your real ownership promote on your in vogue AWS account qualifications sooner than get to is allowed to an AWS account settings. This is called Multi-issue Validation because of the reality components are checked before get right of passage to is conceded for you: supporter need to offer both their Amazon electronic mail-id and secret word (the primary "angle": something you perceive) AND the proper code from customer confirmation apparatus (the second "perspective": something you have) [13] [9].

4. Conclusion

In conclusion, cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses are that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses itself. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

REFERENCES

1. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.
2. Cisco White Paper, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/white_paper_c11-532553.html, published 2009, pp. 1-6.
3. John Viega, Mc Affee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.
4. George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.
5. http://en.wikipedia.org/wiki/Cloud_computing.
6. http://communication.howstuffworks.com/cloud computing1. htm.
7. John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud

Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4, pp 61-64.

8. John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

9. Amazon White Paper, http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-center-and-security-whitepaper/, published June 2009.

10. Marco Descher, Philip Masser, Thomas Feilhauer, A Min Tjoa, David Huemer, " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability and Security, pp. 9-15.

11. David Bernstein, Erik Ludvigson, Krishna Sankar, Steve Diamond, Monique Morrow, "Blueprint for the Inter cloud – Protocols and Formats for Cloud Computing Interoperability, submitted to IEEE, 2009 Fourth International Conference on Internet and Web Applications and Services, pp. 328-335.

12. Liang-Jie Zhang, Qun Zhou, "CCOA: Cloud Computing Open Architecture", published on IEEE, 2009 IEEE International Conference on Web Services, pp. 607-615.

13. Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/, published Aug 26, 2009, pp. 6-8.

14. Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", grid Computing and Distributed Systems and Software Engineering, The University of Melbourne, Australia.

15. Jinesh Varia, Amazon Web Services, "Building Grep the Web in the Cloud, Part 1: Cloud Architectures", Available: http://developer.amazonwebservices.com/connect, July 2008, pp 1-7.

16. Jon Brodkin, "Gartner: Seven Cloud-Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.

17. IBM CIO White Paper, "Staying aloft in tough times", April 2009, pp. 3-19.

18. Steve Hanna, Juniper Networks, "Cloud Computing: Finding the Silver Lining", published 2009, pp. 2-30.

19. Manifesto, "Open Cloud Manifesto, Dedicated to the belief that the cloud should be open", Available: www.opencloudmanifesto.org, published spring 2009, pp-1-7.

20. Peter Finger, "Dot. Cloud: the 21st century business platform built on cloud computing", First edition, Meghan-Kiffer Press, February 18, 2009, ISBN 9780929652498, pp. 81-99.