Advances and Applications in Mathematical Sciences
Volume 20, Issue 12, October 2021, Pages 3129-3134
© 2021 Mili Publications

SECURITY ISSUES IN CLOUD COMPUTING AND ITS PRECAUTIONS

KHUSHBU S. KUSHWAHA

CMC Department, Hislop
College, RTM Nagpur University
E-mail: khushbuskushwaha@gmail.com

Abstract

Cloud computing is a Professional online company that provides customers to work from wherever and anytime on the internet. When using cloud services, it is very important to take protection and privacy into consideration. Cloud computing helps to minimize the use of on-site software or hardware. The cloud is very simple as they have a large space available in which we can store the data as needed. by providing space along with protection, the cloud service helps. We can store the data and provide remote access to the user by purchasing a device or software that can be expensive but using cloud services. There are several security problems, but it is crucial to secure and protect information from unauthorized access.

I. Introduction

Cloud Computing network can be used anywhere anyplace anytime by using internet. Cloud computing offers online data storage, infrastructure and software for storing, executing, and managing information without using local drives. Cloud computing is a registering model in which assets are used and benefits are provided via internet. Cloud computing is the term used to describe the new technology that involves sharing of computational resources and other data representations from various sources, typically geographically distance systems, providing them to organizations and end-users on demand [1].

2010 Mathematics Subject Classification: 68Qxx.
Keywords: cloud computing, security hazard, security strategy.
Received September 28, 2020; Accepted 21, 2020

II. Characteristics of Cloud Computing

A. On-demand self service. A cloud services are available on demand whenever we want to use any service it is available to use anytime, anyplace.

B. Multi-Sharing. Cloud computing allow multiple user and application to be used by many users .Resources can be shared by many users without huge infrastructure cost.

C. Resource pooling. The IT firm uses resources like (networks, storage, software, servers, services) are shared across multiple application. Various customers are offered support from an equivalent physical asset.

D. Rapid elasticity. If an application receives an unusual traffic measure, more staff should be made to provide the assistance. Consequently, with demand, the application will scale smoothly and naturally. It is given to him at whatever point the client's needs administration and it is scale out when its need gets finished.

E. Pay as you use service. No additional charges needed for cloud storage services used by the customer have to be charged for such services. The customer is permitted to request such services, but they have to pay for the service.

III. Types of Cloud Computing

A. SaaS (Software-as-a-Service). SaaS can also be known as on demand software service. A software service is available to the end user over the internet for eg. Google apps, Net Suite etc. Programming as-a-Service is the administration of distributed computing. That give the product application to the client accessible over the internet [2].

B. PaaS (Platform-as-a-Service). PaaS allow user to create, test, run and deploy the application. PaaS provides runtime platform and environment to the user for eg. Azure, Google apps engine. Extra permits clients to change and tweak their additional highlights and arrangements with the utilization of the given condition. While open stage is similar to independent, clients can make their own environment [3].

C. IaaS (Infrastructure-as-a-Service). As a service, IaaS can also be referred to as hardware because it offers servers, networking, processing storage, virtual machines and other services eg. TATA communication, Amazon Web Services. IaaS provides virtual machines that allow complicated system frameworks to be created by clients not only does this approach minimize the cost of buying physical hardware for organisation's, it also promotes and organization of the device heap [4].

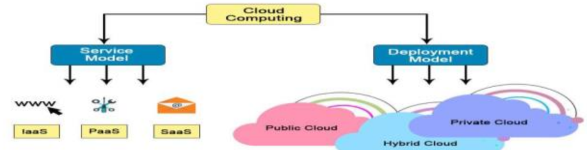

Figure 1. Types of Cloud Computing.

VI. Cloud Computing Deployment Models

A. Private Cloud. The private cloud is made for the one house or private organization for their own purpose use. Private cloud cannot be used outside the organization. The advantages of the private cloud are high security and protection, more control, cost and vitality efficiency [6].

B. Public Cloud. The public cloud is resources and services are available for everyone and everywhere for general public use. Open cloud services are less secure than other cloud models because it puts extra weight on ensuring that all open cloud applications and data are not exposed to pernicious attacks [7].

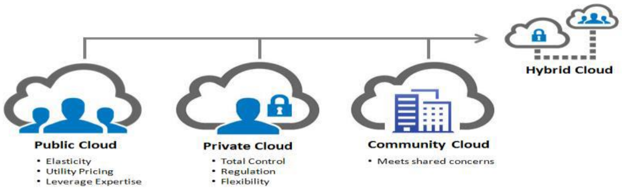

Figure 2. Types of Deployment Model.

C. Hybrid Cloud. A hybrid clouds is a mixture of public and private clouds. This can be achieved if the private cloud wants any essential public cloud resources, such as private cloud that can be store any data. On their private cloud, and that data can be used on the public cloud [8].

D. Community Cloud. A community cloud extends the private cloud to incorporate multiple customers within a defined organization. A people group cloud is shared among a few associations and that is worked, overseen and made sure about normally by the gathering of associations or an outsider help provider [9].

V. Cloud Computing Security Issues

Cloud computing is step by step coordination. In the greater part of the associations, the security need has been introduced to extend. Cloud security methods for organizing control based advances that are designed to address security and to ensure data, information security and all related applications.

A. Data Loss. Cloud computing's most popular security concern is data loss. For several purposes, data on cloud servers may be lost, such as a cyber-attack, a natural tragedy, or a data wipe by the service provider. For rganization's that don't have a contingency plan losing valuable information can be devastating.

B. Data Breach. In Data Breach the confidential data is viewed, accessed, or stolen by the third party without any authorization to access data. Due to the improved technology, large amount of data is stored in cloud servers, which becomes a target for the hackers. More the amount of data exposed, greater will be the damage to the society and users [10].

C. Account Hijacking. The hackers use the stolen account of user or organization to perform unauthorized activities. Attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [5].

D. Malicious Insider. The malicious insider may be current staff, service providers or business associates with permitted access to the network of the company, who may exploit access to impact the organization's confidentiality, credibility or availability of information. An insider's disruptive actions may potentially have an effect on the security, credibility and availability of the data and resources involving internal activities, the reputation of the company and customer confidence [11].

E. Denial of Service (DoS) attacks. Dos attacks occurs suddenly when system receives too much service request or traffic to buffer the server. Systems can run slowly or simple run out of time. Such dos attacks consumes significant quantities of computing resources a bill the consumer can eventually have to pay [12].

VI. Cloud Security Precautions

(1) One ought to be recognizable where the information stores so that if the catastrophe happens or the supplier leaves business the information can recover from the areas. Devoted equipment ought to be there as it takes into account distributed computing administrations to pass the security rules.

(2) There ought to be a depiction of the information and the information should store in better places. The reinforcement of the information ought to ensure with the goal that whatever happens the safe reinforcement can recover without any problem.

(3) The cloud suppliers ought to be dependable then they should ensure that the server farms truly secure. Oversee administrations can give incredible advantage and ability information and business Resilient. Additionally, administrations like firewalls antivirus can likewise offer by cloud suppliers to expand the security of the servers.

(4) Appropriate testing ought to be done how to ensure that everything is secure. The organization can likewise recruit a moral programmer to test the security arrangements. There ought to be an appropriate helplessness checking and appraisal ensures that there is no unapproved get to.

VII. Conclusion

Security is a significant perspective and it can’t exaggerate. We can say that Cloud security assumes a significant job in the Cloud industry. The hazards can be coordinated by stealthy listening, unauthorized interference, and disavowal of administration assaults but also clear distributed computing hazards such as side channel assaults for example. The issue can explain with the assistance of appropriate reconnaissance and the executive’s tools. To eliminate these difficulties of cloud, we can get assistance with legitimate administration and gifted experts. There are a few devices, for example, cloud cost the executive's arrangements, computerization, compartments, auto-scaling highlights, and numerous different devices which help to lessen the difficulties of Cloud Computing.

References

[1] Usman AbudakarIdris, Jamilu Awwalu and Buharikamil, Security threat on Cloud Computing, International Journal of Computer Trends and Technology (IJCTT) ISSN: 37(1) (2016), 2231-2803.

[2] Muhammad Rehan Faheem, Security Issues of Cloud Computing, International SAMANM Journal of Business and Social Sciences ISSN: 2(338) (2014), 2308-2372.

[3] Hamza Ahmed, Cloud Computing Security threats and Countermeasures, International Journal of Scientific & Engineering Research 206 ISSN 5(7) (2014), 2229-5518.

[4] Te-Shun Chou, Security Threats on Cloud Computing Vulnerabilities, International Journal of Computer Science & Information Technology (IJCSIT) DOI: 10.5121/ijcsit. 5(3) (2013), 530-679.

[5] Varsha, Amit Wadhwa and Swati Gupta, Study of Security Issues in Cloud Computing, International Journal of Computer Science and Mobile Computing 4(6) (2015), 230-234.

[6] M. B. Benjula Anbu Malar and J. Prabhu, An Analysis Of Security Issues In Cloud Computing, International Journal of Civil Engineering and Technology (IJCIET) Article ID: IJCIET_10_02_212 10 (2) (2019), 2138-2153.

[7] S. O. Kuyoro, F. Ibikunle and O. Awodele, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN) 3 (5) (2011), 247.

[8] Adnaan Arbaaz Ahmed and M. I. Thariq Hussan, CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH CHALLENGES, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) ISSN: 7(4) (2018), 2278-1323.

[9] S. Venkata Krishna Kumar and S. Padmapriya, A Survey on Cloud Computing Security Threats and Vulnerabilities, International Journal Of Innovative Research In Electrical, Electronics, Instrumentation and Control Engineering 2(1) (2014).

[10] Moulika Bollinadi and Vijay Kumar Damera, Cloud Computing Security Issues and Research Challenges, Journal of Network Communications and Emerging Technologies 7(11) (2017).

[11] Florin OGIGAU-NEAMTIU, Cloud Computing Security Issues, Journal of defense resource Management 32(5) 2012.

[12] Rohan Jathanna and Dhanamma Jagli, Cloud Computing and Security Issues, Int. Journal of Engineering Research and Application, ISSN: 7(6) (Part -5) June (2017), 2248-9622.