Asian Journal of Applied Science and Technology
Volume 4, Issue 3, Pages 01-08, July-September 2020

A Survey of Cloud Computing Security Issues and Consequences

Nandhini K.[1] & R.Venkatesh[2]

[1]PG Student, [2]Associate Professor, Department of Computer Science & Engineering, Sri Shakthi Institute of Engineering and Technology (Autonomous), Coimbatore, Tamil Nadu, India.

DOI: 10.38177/ajast.2020.4301

Article Received: 10 April 2020 Article Accepted: 05 June 2020 Article Published: 20 July 2020

ABSTRACT

The paradigm called "Cloud computing" acts as a mechanism for attaining the resources of shared technology and infrastructure cost-effectively. The on-demand services are accomplished to execute the various operations across the network. Regularly, the last client doesn't know about the area of open physical assets and devices. Developing, using, and dealing with their applications 'on the cloud', which includes virtualization of assets that keeps and guides itself are led by arranged activities to clients. Calculation experience the new methodology of cloud computing which perhaps keeps the world and can set up all the human necessities. At the end of the day, cloud computing is the ensuing normal step in the development of on-request data innovation administrations and items. The Cloud is an allegory for the Internet and is an idea for the secured confused foundation; it likewise relies upon drawing network graphs on a computer. In this work, thorough investigations of distributed computing security and protection concerns are given. The work distinguishes both the identified and unidentified attacks, vulnerabilities in the cloud, security attacks and also the solutions to control these threats and attacks. Moreover, the restrictions of the present solutions and offers various perceptions of security viewpoints are distinguished and explored. At long last, a cloud security system is given in which the different lines of protection and the reliance levels among them are identified.

Keywords: *Cloud computing, Security, Threats, Attacks.*

1. Introduction

Improvement of many procured advances and advances to registering into something other than what's expected is summed up in a "Cloud computing" or "cloud" term which disengages essential foundation from application and data assets, and the components used to convey them. Cloud improves cooperation, action, scaling, and accessibility, and causes to decrease the cost under the aegis of enhanced and proficient processing. Particularly, the cloud portrays the utilization of an assortment of administrations, applications, data, and framework comprised of pools of the figure, system, data, and capacity assets [2]. Orchestrating, planning, achieving, and decommissioning and scaling up or down are quickly performed on referenced constituents and they are provided for an on-request utility-like model of assignment and utilization. Proximity and a decent variety of cloud from present models of processing are so bewildering, thinking about design perspective; furthermore, there are a lot of inquiries concerning their impacts on the authoritative, operational, and mechanical capacities to network and data security models. Today academicians, engineers, designers, supervisors, and clients all have their particular portrayal for the cloud [5].

Distributed computing doesn't have a typically acknowledged definition yet. The National Institute of Standards and Technology (NIST) characterized five fundamental qualities of distributed computing, to be specific: on-request self-administration, huge system access, asset pooling, quick versatility or development, and estimated administration. Likewise, cloud computing is depicted as a dynamic and regularly handily stretched out stage to give straightforward virtualized assets to clients through the Internet. Cloud computing engineering comprises three layers:

(i) Software as a Service (SaaS)

(ii) Platform as a Service (PaaS) and

(iii) Infrastructure as a Service (IaaS).

The clouds are likewise seen as five-part structures that include customers, applications, stages, framework, and servers.

The present clouds are sent in one of four sending models:

(a) Open clouds in which the physical foundation is possessed and overseen by the specialist co-op. (b) Network clouds in which the physical framework is claimed and overseen by a consortium of associations. (c) Private clouds in which the framework is claimed and overseen by a particular association. (d) Hybrid clouds which incorporate blends of the past three models. Figure 1 shows cloud arrangement models together with their interior framework (IaaS, PaaS and SaaS). Cloud arrangement models have the comparative interior framework, yet fluctuate in their strategies and client get to levels.

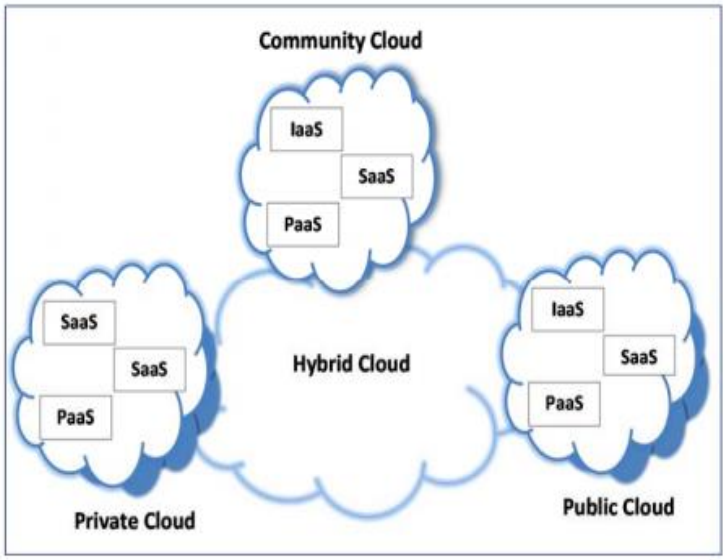

Figure No: 1 Cloud Deployment Models and Infrastructure

Cloud computing is one of the present most energizing innovations as a result of its ability to diminish costs related to computation while at the same time expanding adaptability and versatility for PC forms. In the previous years, cloud computing is being developed from promising business and thought to one of the quickest developing segments of the IT business [1]. In any case, IT associations have communicated troubles about basic issues, for example, security that goes with them across the board execution of cloud computing. Security, specifically, is one of the most discussed issues in the field of cloud computing and a few endeavors see distributed computing attentively because of anticipated security dangers. Additionally, there are two different issues. They are the unwavering quality and accessibility of the cloud which are as significant as security. Even though every one of those three issues is related to the utilization of the cloud, they will have various degrees of significance. Assessment of the advantages and dangers of distributed computing is vital for a full assessment of the practicality of distributed computing. This work depicts the issues and difficulties of cloud computing are dependability, accessibility, and security.

2. Cloud Computing Issues and Attacks

The cloud computing security-related issues are characterized into the accompanying five classes, which are likewise summed up. A comparable way to deal with characterizing the issues is found however it is constrained to the little arrangement of cloud security concerns and just in part covers various classifications.

1) The Security Standards classification manages administrative specialists and governing bodies that characterize cloud security arrangements to guarantee a secure workplace over the clouds. It incorporates administration level, inspecting, and different understandings among clients, specialist organizations, and different partners.

2) The Network classification alludes to the medium through which the clients associate with the cloud framework to play out with the ideal calculations. It incorporates programs, associations, and data trade through enlistment.

3) The Access Control classification is a client situated class and incorporates identifiable proof, verification, and approval issues.

4) The Cloud Infrastructure classification incorporates security issues inside SaaS, PaaS, and IaaS and is specially related to virtualization conditions.

5) The Data class covers information security and secrecy issues.

Exceptional consideration is required towards shared security principles, for example, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), XML signature, XML Encryption Syntax and Processing, and Key Management Interoperability Protocols. At present, cloud computing needs proper security norms [4].

Regardless of whether security norms are characterized appropriately, numerous security issues are still connected with consistent chances because of the absence of a governess for reviews and corporate standard assessments. Cloud clients need more information on systems, procedures, and practices of the supplier, and isolation of obligations.

When the service provider re-appropriates the support of an outsider where usefulness isn't straightforward, clients must have the option to review the entire procedure. Security principles and administering bodies are a piece of service level agreement (SLA) and lawful viewpoints, separately which have not been taken into rehearses for cloud computing. The client may endure if there should arise an occurrence of information misfortune if the above elements are not taken for granted as he will be unable to put asserts on service providers.

Network classification-related issues are considered to be the greatest security challenges in clouds since cloud computing is progressively inclined to organize related assaults contrasted with the conventional figuring standards. Furthermore, cloud activities are firmly coupled and profoundly rely upon systems administration. Accordingly, cloud security issues get more consideration in this work contrasted with the other security classes. Security specialists foresee that clouds will be the focal point of programmers in the future because of the grouping of important "resources" (information and calculation) inside the mists [6].

The conceivable absence of appropriate establishments of system firewalls and the neglected security designs inside clouds and on systems, make it simpler for programmers to get to the cloud for genuine clients. Programmers can possess assets (equipment or application) by producing false information or they can run pernicious code on the commandeered assets. Denial of service can be propelled by first recognizing vulnerabilities in Internet conventions, for example, SIP (Session Initiation Protocol) which could esteem the Internet to be un-trusted.

Account and Service hijacking include phishing, misrepresentation, and programming vulnerabilities where aggressors take certifications and increase unapproved access to servers. This unapproved access is a danger to respectability, secrecy, and accessibility of information and administrations. Unapproved access can be propelled from inside or outside the association. Noxious insiders, for example, untrustworthy heads seriously sway associations' security. Given their degree of access, they penetrate corporate and cause brand harm, money related, and efficiency misfortunes. In this manner, it is basic for cloud clients to decide that the cloud suppliers use to identify and shield against insider dangers.

The present validation instruments may not be material in cloud situations as clients no longer have a place with or can get to a solitary firmly controlled framework [3]. A solitary client may have access to information and form administrations from different cloud suppliers utilizing a versatile application or a program.

This sort of access acquires a characteristic degree of hazard and this hazard has been called advantaged client access. Unapproved access gets conceivable through program vulnerabilities. Also, the Internet program is the main stage where safety efforts ought to be considered that vulnerabilities in the program open the entryway for some follow-on assaults. The unreliable interface of Application Programming Interface (API) issue covers the vulnerabilities in the arrangement of APIs in the cloud entryway (clients utilize these APIs to associate with a cloud) which can open an association to a few dangers, for example, unapproved access, and content transmission, reusable token and logging capacities.

A large portion of cloud sellers erroneously guarantees to give secure information and computational situations for cloud clients. It may tend to be reasonable, aggregate endeavors are required at more significant levels (e.g., overseeing bodies) rather than leaving it to singular associations. The present work helps in accomplishing the objectives by giving an extensive investigation of the assaults against clouds, setting up conditions among different assaults, and connecting assaults to vulnerabilities across different cloud parts. This examination can bolster the undertakings to give preventive measures just as proactive apparatuses in protecting the clouds.

Utilizing this examination, it is found that information and framework security ought to be inserted in the plan of cloud design to accomplish better security. Also, safety efforts ought to be dynamic and self-governing. The cloud computing foundation is changing quickly requiring safety efforts and approaches to be refreshed routinely at a similar pace to coordinate the changing conduct of the clouds. Besides, authorizing is urgent to the security of clouds.

Standard arrangements ought to be carefully executed in clouds and hierarchical/administering bodies should visit clouds' framework to assess the proficiency of the security safety measures received by the sellers. The insights for assaults, happening in any cloud, ought to be publically accessible to decide the unwavering quality of cloud merchants.

3. Results and Discussions

Cloud computing is enriched with enormous issues such as reliability, maltreatment, malicious attacks, availability, vulnerabilities due to shared technology, traffic skyjack and data leakage. The most important part is privacy and

security which is required for the cloud provider. The attacks are also given and at the same time solutions to those problems are included in table 1.

The aggregation of privacy and security is necessary for many enterprises because they store their confidential information onto the cloud. The performance may not be a critical requirement for many users. The cloud providers must ensure security and reliability to meets the needs of the enterprise.

Table No: 1 Comparative Analysis of Cloud Computing Attacks, Consequences, Solutions

S.No	Attacks	Consequences	Solutions
1	Maltreatment and Wicked Usage of Cloud Computing	The spam and malware are made to spread by botnets. The path is found by the intruder to transmit the malware to numerous PC's. The cloud infrastructure's power is utilized by the attackers to assault the other PC's in the network.	Infrastructure based security, Access control and Identity management.
2	Malicious Attackers	The attacker aims to generate malicious software which is entrenched on other's machine. Despite their knowledge, the intruder takes the privilege by damaging the system for the financial commotion.	Storage and Information security management. Also, the privacy management plays a major role.
3	Usage of apprehensive Application Programming Interfaces	The clients often communicate with the cloud by the usage of APIs. The attacker tries to analyze the encryption pattern of both the sender and receiver. Also, the activities of the clients are captured by the intruders.	Authentication management, Access control and security management.
4	Vulnerabilities of Shared Technology	Various virtual machines access is attacked by the intruders. The intruders have the capability of	Defense-in-Depth technology and layers of virtualization.

		utilizing the entire computing resources that applies to other machines.	
5	Information Leakage or Loss	The illegal access attempts to remove the data before any backups. The attacker also tries to obtain the encoded key.	Access Control, Encryption algorithms and Privacy management.
6	Privacy, Account and Traffic Skyjack	Denial of service attacks, a man in the middle attacks and phishing attacks took place.	Authentication mechanism, security policies for providers and proactive monitoring.
7	Unknown Profile	The attacker aims to attain the security policies and the update of the code.	Infrastructure management and monitoring and alert management.
8	Provider Security Failure	The intruder attempts to manage the hardware. He also tries to supervise the stored data and process the application.	Authentication mechanism and Security management.
9	Other Client Attacks	Once the interface among the clients breaks down then other client aims to get the other client's information or attempts to obstruct the other applications.	Privacy management and information security management.
10	Reliability and Availability Issues	The intruder acts as a cloud provider and executes a hosted application for broadcasting accurate results.	Maintenance and Privacy mechanism.
11	Virtual Machine Attacks	The attackers will hack the resources in a multi-tenant architecture. The intruders will enhance or minimize the VM's.	Authorization and authentication mechanism.
12	Distributed Denial of Service Attacks	Botnets have introduced with a large number of virtual machines. It also transmits the huge packet	Data storage and backup.

		traffic from various sources to a web server.	
13	Intrusion Attack in SaaS	The attackers will obtain the system logs and the custom application is monitored by the intruders.	Host-Based and Network-Based Intrusion detection system
14	Intrusion Attack in PaaS	Close to SaaS. The difference is the system is embedded on the centralized server.	
15	Intrusion Attack in IaaS	Transparency is an important dispute in IaaS.	
16	Regulatory issues	Jurisdiction as well as data export issues externally.	Security management.
17	Perimeter Security Attacks	The most critical application is attacked by the intruders.	Security and Privacy Management.

4. Conclusion

IT enterprises need the concept of cloud computing in a cost-effective approach. In this work, the various types of attacks, consequences and the solutions are analyzed. The solutions are effective in solving the attacks. Each method helps in solving the attacks created by intruders. Still, the method of cloud computing is embedded with positive and negative things that are developed for a large scale enterprise. Nowadays the total number of intruder attacks has been increased. By protecting the information and cloud infrastructure, cloud security can be attained against various attacks. The attacks such as known and unknown attacks still exist in the infrastructure of cloud computing and it may not be identified and protected. This happens because of the computation overhead. The existing solutions like firewalls, antivirus installation may be very expensive and also the network performance can be degraded. Hence the work not only relies upon security and also the method must involve a low amount of resources as well as minimal degradation in the performance. The current survey achieves the solutions by affording various solutions to the attacks and its consequences. By utilizing this survey, information and system security must be entrenched in the cloud architecture design to afford the utmost security.

References

[1] Tripathi, A.; Mishra, A. Cloud computing security considerations. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 14–16 September 2011; pp. 1–5.

[2] Wang, J.-J.; Mu, S. Security issues and countermeasures in cloud computing. In Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 September 2011; pp. 843–846.

[3] Jain, P.; Rane, D.; Patidar, S. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of the 2011 World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11– 14 December 2011; pp. 456–461.

[4] Samarati, P.; di Vimercati, S.D.C. Data protection in outsourcing scenarios: Issues and directions. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 1–14.

[5] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 5–8 October 2011; Volume 2, pp. 632–634.

[6] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A. Cloud security issues. In Proceedings of the IEEE International Conference on Services Computing, 2009 (SCC '09), Bangalore, India, 21–25 September 2009; pp. 517–520.