Cloud Security Issues &Network Security in Private Cloud

Priyanka[1], Dr.Rashid Hussain[2]

[1] *Department Of CSE,SKIT Jaipur,* [2]*Department Of ECE,SGVU,Jaipur*

[1]trikha_priyanka@gmail.com

[2] rashid.hussain@mygyanvihar.com

***Abstract*— As per Cloud Security Alliance (CSA), over 70 percent of the world's organizations currently work on the cloud, which is increasing day by day during COVID-19 pandemic. Similar to any new innovation appropriation, adopting cloud opens new types of security dangers. Even though there are numerous advantages of cloud computing, the security issue is a main concern. With the popularity of private cloud, how to protect the private cloud network security has become the focus of more and more organizations. The Organization information security system needs to integrate the information security construction into the infrastructure construction itself.**

This paper is focusing on variety of security issues identified in cloud computing, examines a portion of the key research difficulties of cloud security and answers for securing the dynamic cloud condition and gives a down to earth answer to avoid the difficulties that the cloud suppliers and buyers face. This paper also talks about the basic network security situation, big data security, private cloud network security situation as the entry point, analyzes the relevant evaluation indexes and also elaborates on the private cloud network security situation in an organization.

Keywords- Cloud Computing, Cloud Security, Privacy, threats, Cybersecurity

I. INTRODUCTION

With the fast improvement of the system innovation, cloud computing has bas developed as a comprehensively acknowledged sending in business and has been driving individuals' lives towards an associated domain [1],[3]. One of the major points of interest of cloud computing is that it can offer various administration models relying upon clients' requests. Administration models can be spoken to as a X-as-a-Service (XaaS), in which X alludes to the processing contributions [4]. Essential figuring contributions incorporate framework, programming, and stage [5]. In the interim, administration contributions, Xs, can be spoken to in any habits that are deliverable to clients, for example, data, security, back-end, and procedure [6]. The adaptable assistance conveyances have surprisingly scaled up the administration content on the system. Regardless of the high comfort and adaptability brought by cloud computing, the usage of cloud-based arrangements is as yet experiencing limitations getting from security concerns. Because of the associated condition, cloud figuring usage are confronting all vulnerabilities of the system [7], [8]. Then, other than systems administration vulnerabilities, cloud applications likewise need to manage potential dangers from involvers in the cloud, for example, obscure third party specialist co-ops or sudden information clients. It suggests that most cloud applications are confronting dangers from both insiders and pariahs [9], [10]. Normal cloud dangers spread information misuse, malignant insiders, uncertain interface and APIs, common innovation issues, information misfortune or spillage, account or administration commandeering, and obscure hazard profile. A legitimate and exact comprehension on cloud security is a key prerequisite for an accomplishment of the cloud sending. This paper along these lines centers around perceiving normal perspectives of the cloud security. So as to give an all encompassing perspective of cloud security, we show a high structure of security measurements in cloud computing . Computer security,information security and network security are three measurements will control the structure of this overview. At each measurement, the overview just chooses huge and agent perspectives for surveys because of the restriction of pages. In addition, writing audits finished by this study work for the most part center around refreshed research achievements as opposed to experiencing a background marked by cloud computing. The target of this work is to give researchers and experts with an information platform about later The fundamental commitments of this study are triple:

(1) this work features fundamental vulnerabilities of cloud security and spreads key issues in the field;

(2) we orchestrate trademark answers for each kind of dangers in cloud security.

II.TRADITIONAL METHODS VS CLOUD

A. Common Responsibility model

With a common obligation model on the cloud, it is basic for an association to screen, recognize and remediate on any potential dangers and misconfigurations on their cloud resources. Difficulties with making sure about Cloud Dynamic condition: The flexible idea of conditions on the cloud, makes opportune continuous perceivability of virtual examples troublesome. Ensuring of such conditions require a constant disclosure, security evaluation and proactively take activities to ensure them. Edge definitions: Cloud outstanding tasks at hand are frequently divided over a few diverse geo-areas and situations, making it hard to midway oversee resources Loss

of control on physical security: As associations lose command over physical security, the duty of securing information and remaining tasks at hand at travel and rest falls into the lap of the client. Virtualized and multi-occupant nature of open cloud make it important that an association is consistently up to speed with the most recent vulnerabilities and take remediation activities when vital.

B. Top Security Issues in Cloud

According to reference [4,5], the top security dangers distinguished in the cloud are: Information Breaches Inadequate Identity, Credential, and Access The executives Uncertain Interfaces and APIs Framework Vulnerabilities:

- Data Hijacking
- Malignant Insiders
- Insecured APIs and Interfaces
- Information Loss
- Account Hijacking
- Misuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Vulnerabilities

To recognize and alleviate the above security dangers they can be classified under the accompanying classifications:
1) Poor Identity and Access Management: Identity and get to the board are critical to answer the 5
W's(Who, what, when, where, why) of availability of assets. Poor Identity and access the executives can result in
a. Data Hijacking: If Cloud seller reassure or Programming interface qualifications are lost, a vindictive entertainer outside of an association can assume responsibility for the cloud condition.

b. Information Breaches: Poor access the executives of object stockpiling pails and information stores cause touchy data to be made open, which has been one of the significant reasons for information breaks on the cloud.
c. Pernicious insiders: Malicious insiders attempting to take administrator/root benefits, can bring about loss of delicate information and frameworks.
d. Misuse and Nefarious utilization of cloud assets: Record seizing of a cloud record can result in the malevolent client to utilize the undermined assets to dispatch DDOS, spam and phishing crusades leaving the association inclined to lawful obligation
e. Inadequate Due-diligence: Organizations which handle information and fall under administrative consistence laws, need to have an unmistakable arrangement to move to the cloud, else this represents a security risk and lawful obligation.

2) Workload dangers

a. Advanced threats(AT): Malware and Progressed persistent dangers once enter an condition, adjust to the safety efforts and after some time increase an a dependable balance in the earth and spread itself horizontally and once it comes to the planned objective, it will exfiltrate delicate information. These dangers are hard to recognize and remediate.
b. Vulnerabilities: With Cloud administrations being multitenant, vulnerabilities that incorporate benefit acceleration and VM limit bouncing can cause information breaks and leave the applications and remaining burdens defenseless.
c.Insecure API's: Insecure API's serving diverse help of an application can leave the application defenseless against known assaults furthermore, bring about application vacation or information breaks.

III.THE INTERNET NETWORK SECURITY

Network security circumstance is a full scale reaction to network activity, which mirrors the past and current circumstance of the network, and predicts the conceivable network state in the next stage[11]. It basically gathers data through observing network equipments, through the data preparing, numerical, symbol and different approaches to react the genuine activity of the network.
A. Network Security Situational Awareness : Network security circumstance is a far reaching research point. It predominantly contains three levels. To start with, manage the gigantic network data, show network security circumstance with designs. Besides, the data are quantitative investigation, the qualities are disconnected, and the history and current circumstance of network security are assessed.
B. The Key Technology of Network Security Situational Mindfulness :One of the key advancements of network security circumstance is the data combination innovation, a bound together of various security equipments are gathered and changed into a standard data position which screens the security log or cautioning data. As the historical backdrop of security occurrences are analyzed , the expectation of network circumstance are precise. After the combination of network security data, we have to compute the enormous data through a particular scientific formula, that is, through a particular numerical equation, a run is gotten, which mirrors an estimation of network security state in a specific period. There are four principle computation techniques: Analytic Hierarchy process (AHP), fuzzy Analytic Hierarchy process (FAHP), Delphi technique and an elaborating analysis method.[12]. The Network security situational mindfulness depends on logical, the chronicled security events and network security status are analyzed and compared, and the network security status later on is anticipated . The sorts for organize network security circumstance are three: qualitative prediction strategy, time networkment examination technique and causality prediction strategy. Consolidated the present network hardware security status data, the network security dangers and covered up perils later on period are anticipated by the Scientific hypothesis and reasonable strategy.

IV. THE NETWORK SECURITY SITUATION OF PRIVATE CLOUD

With the fast improvement of Internet in addition, Data is the center intensity of any Organization. Data have numerous types, for example, client data, budgetary data and other data. At Open(public) cloud, the main data of the organization is by and large put away in the Public network capacity which is provided by the organization. [13]. The data which put away in the network are for ever increasing extent of openess and comfort, at similar occasions more and all the more no security and no confidentiality . During the Organization data is transmitted and put away, it is stolen without any problem. It is especially concerned about data encrypting. So as to all the more likely ensure these data, to an ever increasing extent Organizations have built up private cloud. In any case, there are numerous unreliable factors in private cloud networks also: data interchanges problems, attacks on servers, keep sending service requests within short span of time, which may influence the reliabile quality of private cloud. Besides if the private cloud is harmed, it will have a lethal effect on overall Organization.

A. The Security of Virtual Cloud Data With the improvement of new network innovation, the advancement is happening in the field of cloud computing and big data. In the period of big data, organize security can be upgraded from numerous perspectives, for example, physical security, host security, data content security, data transmission security, etc.In an era of Big data, it is a tremendous challenge to investigate gigantic data, prevent the intrusion and attacks of programmers, improve network security countermeasures by taking increasingly dynamic and powerful network security measures.In the period of big data, it is an assistance that how to store and work on the data. The spread of the network virus is twofold, the degree is wide. Antivirus innovation is the key innovation of big data security. In private cloud big data, the innovation of Antivirus are predominantly two sorts: static and dynamic [14]. The static antivirus innovation predominantly screens the network hardware through the checking equipments, furthermore, analyze the security status of the network as indicated by the condition of the hardware. Dynamic antivirus innovation can ensure the base framework assets of the private cloud, which can guarantee its integrity.

B. The Key Technologies of Private Cloud Network Security
In the transport layer and storage zone, so as to guarantee the security of private cloud, the organization will build up a series of network security innovations. In the transport layer, the transmitted data is encoded. The transmissible significant data are encoded by technologies; the recipients decode the encrypted content. After exchange the data security, it is significant that how to store these data securely. The security of data for the most part incorporates the boundary security of network data, the mutual isolation of data, the catastrophe recuperation of data, and so on.Furthermore, private cloud can likewise secure data access through a progression of access verification, remembering single sign for verification, collaborative verification, and authorization etc. In private cloud data limits, a progression of focused security is required. The new intelligent firewall innovation is the most all inclusive. Not the same as the conventional firewall innovation, intelligent firewall innovation is another firewall innovation. It utilizes fuzzy recovery database, through Artificial intelligence to powerfully recognize the data. Intelligent firewall innovation can keep programmers from filtering network data, which can keep up the data security of the private cloud. There are three protection modes of intelligent firewall: intrussion avoidance, cheat prevention also, anti scanning.

V. THE KEY TECHNOLOGY OF NETWORK SECURITY IN PRIVATE CLOUD

Private cloud organize security can be comprised of five levels: gadget security layer, system security layer, network security layer, application security layer and data security layer. By breaking down the danger of each layer and receiving suitable safety efforts, the security objective can be accomplished: confidentiality, integrity, accessibility, controllability and non repudiation.

A. Network Security Situational Awareness of Private In Big Data In the Era of Big Data ,Private cloud enormous data has the accompanying attributes like: Volume (high limit): the size and measure of data decides the size of the data worth and potential data; Variety (type): data types; Velocity (speed): get the data rapidly; Variability: deal with the procedure of data legitimacy; Veracity: data reliability quality; Complexity: a lot of data, numerous sources, numerous channels brought about by the utilization of unpredictability of data; Value: discerning utilization of enormous data by sensible examination, make high incentives with little Inputs. In Examination of enormous data at private cloud platform, an assortment of network security hardware and network checking equipments should be gathered [15]. A huge amount of data will be introduced in different manners such as, observing strategies and security revealing mechanisms, which draw designs and different reports. Private cloud data have numerous qualities: huge log information, repetitive data. But, error data can't be utilized as a direct source of circumstance awarebess; it must do on-line analytical processing and data combination.

In the era of Big data, it can gather different kinds of data designs, including log organize hardware, security hardware, log, the data in private cloud that worked in administration framework. So we are more aware about network security situation. Another highlight of big data is the quick processing of huge data. Individuals can profoundly investigate the parameters of network traffic and network data [16]. Computational assets need to meet the requirements of high insight model algorithms. In Big data time, there are four primary parts of network security: First, data base can be built up by contemplating network attack cases, including standard, attributes, environment, the most well-known equipments and techniques; Second, environment vulnerability data base can be built up by analyzing the limitations of private cloud design

framework vulnerabilities and storage devices; third, environment threat data base can be built up by dissecting the design topology and hardware of private cloud; Finally, by dissecting and looking at the three sorts of data base horizontally, individuals can affirm the adequacy of security incidents[17]. Through breaking down the historical events, the network attacks that influence the current network will be brushed. At last create security circumstance appraisal components of private cloud, counting the security dangers, the weakness, the running wellbeing status, and so on.

B. The Assessment Index of Network Security Situational Mindfulness on Private Cloud:

To assess the security circumstance of private cloud, we should make an exhaustive report from five angles, counting physical security, host security, network security, data security and content security. The examination can mirror the security of the storage disk, the security of the data framework, the security of the data itself, the security of the data transmission and the security of the data use of private cloud. Among them, the best marker of network security circumstance is network security Index. The network security condition can quantify by network security index. It comprises of a three-dimensional organize file ($Run_{net,}$ Vulnet, Threatnet).This index represents the network threat dimensions. The network circumstances can be analyzed by security assessment index.

The assessment of network security situational mindfulness on Private cloud organize comprises of three sections: stability, vulnerability and danger of network. The stability of the network is reflected by the security of the equipment and programming design, which centers around the nonstop and stable activity of the network in a specific timeframe. The vulnerability of the network centers around the ability to prevent and calamity resistance. The risk of the network centers around the different threats that assortment, examination and assessment from outside.

C. The Security Situation Warning of Private Cloud Network:

At present, the most elevated level of security guard framework is network security situation. So to analyze the questionable data in the network for quite a while, the advanced analysis technology will be utilized in the private cloud; the logical principle will be given in the network security situation.

So as to manufacture an ideal network security circumstance gauge pattern map, and improve the accessibility of security circumstance expectation, it is important to build up a long term monitoring technique. With the quick advancement of the network, the network security condition is turning out to be increasingly unpredictable, the attacks force is turning out to be more grounded and more grounded, and the risk is likewise expanding. These days, the risk of Internet is dynamic. So as to give security strategy to clients, right choice ought to be made, and dynamic forecast measures ought to be embraced [18]. The main issue of network security situation warning is to find out most effective method to foresee the network security situation.

VI. CONCLUSIONS

In this paper, a survey was accomplished to review all crucial security aspects of cloud computing. The convergence was comprised of computer security,network security and information security.The literature review analyzed all the major threats and vulnerabilities of cloud computing,along with their solutions .Artificial Intelligence provides new possibilities for solving the problem of network security In the future, based on artificial intelligence and powerful data analysis ability, people can anticipate the danger ahead and greatly enhance the ability of network security defense. In the future, more consideration will be given to the use of artificial intelligence to solve the security problem of any organization's private cloud.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[2] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1):1–11, 2011.

[3] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. *Journal of Network and Computer Applications*, 59:46–54, 2015.

[4] P. Mell and T. Grance. The NIST definition of cloud computing. *Special Publication - National Institute of Standards and Technology, U.S. Department of Commerce*, 2011.

[5] L. Qian, Z. Luo, Y. Du, and L. Guo. Cloud computing: An overview. *Cloud computing*, pages 626–631, 2009.

[6] B. Hayes. Cloud computing. *Communications of the ACM*, 51(7):9– 11, 2008.

[7] T. Dinh, Y. Xuan, M. Thai, P. Pardalos, and T. Znati. On new approaches of assessing network vulnerability: hardness and approx- imation. *IEEE/ACM Transactions on Networking*, 20(2):609–619, 2012.

[8] T. Khorshed, A. Ali, and S. Wasimi. A survey on gaps, threat remedi- ation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation computer systems*, 28(6):833– 851, 2012.

[9] S. Stolfo, M. Salem, and A. Keromytis. Fog computing: Mitigating insider data theft attacks in the cloud. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*, pages 125–128, San Francisco, CA, USA, 2012. IEEE.

[10] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou. Toward secure and dependable storage services in cloud computing. *IEEE Trans. on Services Computing*, 5(2):220–232, 2012.

[11] Zhao Y., Zhou F., Shi R.. NetSecRadar: A Real-time VisualizationSystem for Network Security: VAST 2012 Mini Challenge. Award: Honorable Mention for Interesting Use of Radial Visualization Technique [C]// VAST. proceedings of the Visual Analytics Science and Technology (VAST), 2012 IEEE Conference on, October 14-19,2012,Seattle, WA, USA. New York: IEEE, 2012:281-282.

[12] FireEye. Cybersecurity's Maginot Line: A Real-world Assessment of the Defense-in-Depth Model [R]. FireEye, 2015.

[13] Zhang J. F. Research on key technologies of network security assessment [D]. Changsha: National University of Defense Technology,2013:19-35.

[14] Wei Y., Lian Y. F., Feng D. G..A network security situationalawareness model based on information fusion [J]. Journal of computer research and development,2009,46(3) :353 362.

[15] Lai J. B., Wang H. Q., Zhu L. Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory[C].//Proceedings of the International Conference on Computational Intelligence and Security, Guangzhou, China: IEEE Computer Society,2006:1545~1548.

[16] Lai Y. P., Hsia P. L. Using the vulnerability information of computer systems to improve the network security. Computer Communications. 2007, 30(9) :2032-2047.

[17] Zhao L, Xue Z. Synthetic security assessment based on variable consistency dominance-based rough set approach High Technology Letters. 2010. 16(4):413-421.

[18] Sun F. X. Artificial immune danger based model for network security evaluation. Journal of Networks.2011,6(2) :255-262.