JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

A STUDY ONCLOUD ENVIRONMENT: CONFIDENTIALITY PROBLEMS, SECURITY THREATS AND CHALLENGES

Chandrakala G Raju

Department of Information Science and Engineering, B.M.S College of Engineering, Bengaluru, Karnataka, India, chandrakalagraju.ise@bmsce.ac.in

Radhika K R

Department of Information Science and Engineering, B.M.S College of Engineering, Bengaluru, Karnataka, India, rkr.ise@bmsce.ac.in

Abstract:

In areas such as computer cloud computing, services has flourished. It's a part of computer software that may be way in during the internet. Cloud computing is still very much in infancy, with a slew of unanswered research issues. Cloud computing has benefited the IT industry greatly. It's the then step in the growth of the Internet, by a carefully organized as well as authoritative file storage space network susceptible of massive capacity and applications. It enables ability to haveentrée to a recipient's case or information without the information including to be placed on the user's computer via Internet tune-up. Cloud computing consent to members of the community to access pre-configured computing resources on a shared or on-demand basis. You can to get the most from a computer by having numerous operating systems installed. In this sense, it refers to the creation of a computing machine of resources such as disk drives, a effective operating machine, or the cloud implementation of purpose or programme. Cloud technology is no different; it has both benefits and drawbacks. Some of the repercussions include cloud security, manageability, integrity, fraud, information leakage, and other concerns. We will go over several obstacles and issues related to data security in the cloud in the presented material.

Keywords:Cloud computing, Client management Issues, Cloud Configuration Security Services and Polices, and Exploitation of authentication.

I. Introduction:

In recent years, there has been a considerable increase in the need for data, or the quantity of individuals who exercise the network has raise earlier than usual. Besides, traditional computing technology has become excessively valuable and hard to sustain, preventing information entrée at any anytime. As a result, the use of an exterior drive resolution has become a necessity for information storage. The processing device topologies currently cannot adapt to the growing quantity of web users on working frameworks milieus, long-distance interpersonal connection locales, media dissemination locales, and other destinations. As global Network use has continually increased [1,] a new concept identified as cloud has appeared due to the enormous number of users plus resources accessible.

Distributed computing, like other specialist offices, has a number of advantages. It enabled the storage of a large amount of data and the provision of a variety of services, for example. Furthermore, by distributing essential assets among different clients, addressed the

Submitted: 16/11/2022 **Accepted**: 05/12/2022

constrained reduced administration costs. The stage should be secured against security threats to ensure that the asset maintains its unwavering quality [2]. Distributed computing has recently become one of the most popular topics in safety research. Digital storage security, remote monitoring, plus user authentication are among the topics covered in these studies. According the National International organization For standardization, "a model for permitting quick, resource pooling, universal, on-demand connectivity that can be easily maintained with various aspects of service provider engagement" (NIST). Customers only pay for a service they use in cloud computing, which is defined as Pay and You Can go (PAYG). With the PAYG approach, customers can customise apps, storage, processing plants, and computing resources to meet their specific needs. This is why the science world has spent so much time and effort on this cutting-edge concept [4].

The adoption of virtualization has boosted the availability of end-user services. Distributed computing is characterised by its versatility, reasonability, and moderateness. In practise, these techniques connect available dividing available onto distinct diverts that can be assigned or device or left completely [5]. It offers an affordable demand service, and also elasticity and adaptability. Programming as a service, framework as a service, with staging as a service are the three basic assistance delivery types provided by distributed computing (PaaS). Access to board capacities in apps, such as strategy controls, is emphasised in the SaaS model. Only allowed every one at a time, such as data from applications. Multiple end users profit from a specific incident of the service in this way. SaaS providers include Google, Microsoft Windows 365, Dropbox, and others. PaaS stands for "service platform," and it utilisation of a layer of the positive effect as a platform on which other higher may be built. Clients create their own apps that run on the supplier's platform in the PaaS paradigm. Structure, to name a few, provide a mix of functional frameworks with application workers. It's critical to note that information assurance is one of the PaaS model's main focuses. This is especially true when it comes to ability as a helper. This model should be able to obfuscate data when it is stored on an external stage, and it should be aware of administrative concerns that affect availability throughout the organisation using IaaS. The goal of virtualization is to create self-contained virtual machines (VMs). The virtualization process includes firewalls, intrusion detection systems, and virtual machine monitoring. There are, however, a plethora of other security risks that must be addressed. Businesses prefer such a secure atmosphere.

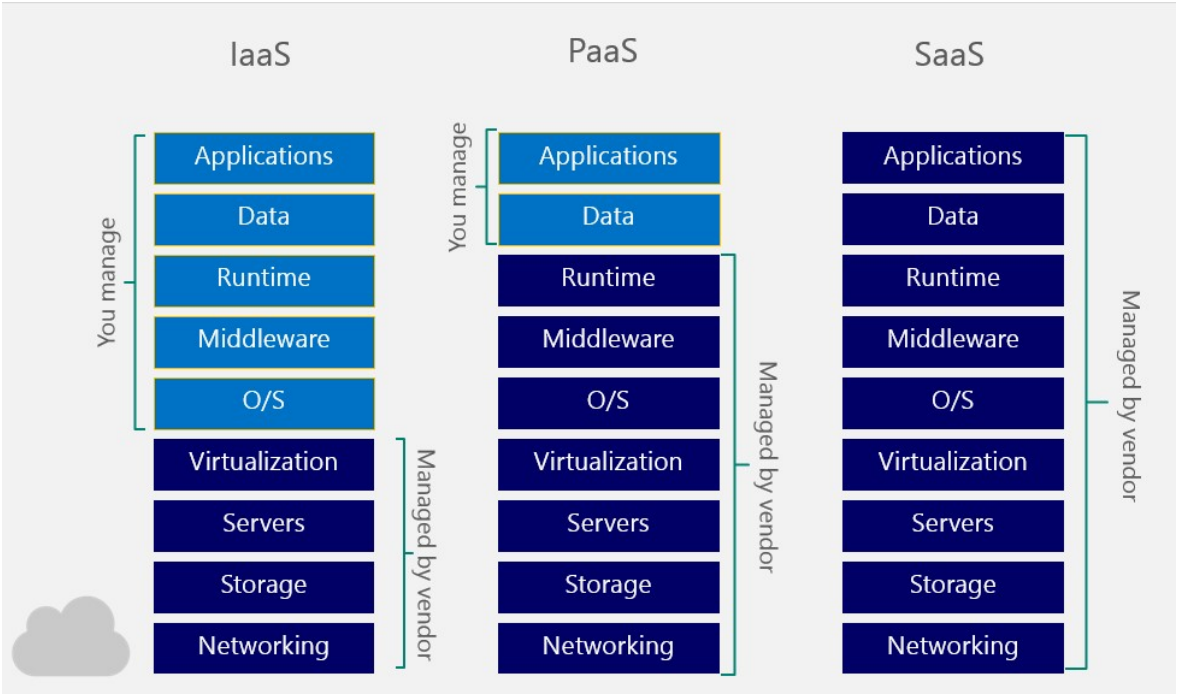

Fig.1 Configuration of cloud delivery model [6]

The rest of the paper is as follows. The significance of this survey is presented in Section 2. Section 3 discusses the associated cloud and security research. Cloud security risks and difficulties are discussed in Section 4 of this report. Section 5 displays cloud-based service security policies. Client management difficulties in the cloud were discussed in Section 5. Securityattacksandthreatsincloudcomputing is shown in section 6. Section 7 discusses how to take advantage of authentication. Section 5 discusses the importance of cloud security challenges. Ultimately, in Section 9, the survey on cloud-based security and concerns comes to a close.

II. Contribution of Survey:

This typical occurrence, however, has a lot of security flaws and vulnerabilities. The cloud environment is undeniably vulnerable to a variety of attacks. As a result, utilizing this phenomena needs enough information and most effective response to these hazards. This article examines a number of papers, with a focus on a few of the most important. In actuality, this study explains how cloud computing security concerns, difficulties, and dangers are expressed. The following are the main contributions of this work:

- All companies involved within cloud computing environment architecture, as well as the fundamental concepts of cloud computing, are implemented.
- It has created a new five-classification categorization of cloud security concerns and difficulties in the security level of cloud conditions.

III. Related Work:

The Context section covers preliminaries to data protection as well as the architecture of cloud computing systems.

a) Security service

Protection refers to all approaches for safeguarding, recovering, and maintaining the stability of information in network devices in the face of multiple threats. Security networks, in practise, impose security agencies that carry out security policies. Computer services including network systems are secured using integrity, confidentiality, identification, non-repudiation, and maybe other resources [6].

- Information get sent (and collected) without even being accessed via unauthorised persons during transmission. Using user authentication to keep information secret is a smart idea. To gain access to information, you can utilise a centralised or distributed key strategy [7].
- Relevant organization that data collected from a reliable source is identical to information supplied. To put it another way, it guarantees that the results have not been tampered with it with a 3rd person (intentionally or accidentally). Whenever there is an attack, the link is broken, and the transfer of incorrect data [8].
- Design ensures that only authorised users have entrée to resources with that information be able to only be viewed with utilized by authorised users on a regular basis. A distributed doublethink hazard prevents a computer from sending data [9].
- To be regarded trustworthy, the sender with recipient of data has to be whoever they claim to be [10].
- Pseudonym refers to the incapacity of sender and recipient to protest acts committed. The two sorts of repudiations are source repudiation or destination repudiation [11].

b) Cloud configuration

We must first understand the cloud structure detailed in the upcoming sections in order to properly understand security risks. Demand-driven services are found in a cloud field. According to NITS, cloud computing installations contain five major actors, as indicated in [8]. The classification is focused on cloud customer risks and risk perceptions.

Cloud user: A cloud customer is the person or organisation that uses the services of a cloud provider. Indeed, a cloud user can select the most suited services by assessing the services offered by cloud operators and signing a contract. To finish this contract, a cloud user must examine technological efficiency as sign a contract (SLA) with either a cloud provider. System development, dependability, prevention, including performance degradation are all

covered by service level agreements (SLAs). A cloud consumer, but in the other end, has a larger selection of vendors to choose from, with many of them offering greater services at lower prices [9].

Cloud contributor: A cloud provider is corporation make available to a data centre. The cloud hosting combines or arranges cloud applications by purchasing and managing cloud services. SaaS services are provided by the cloud provider, who instals, configures, manages, and upgrades software programmes on a constant schedule [10]. According to internet constrained organisational applications, the most of the managing and governing functions in technology and infrastructure are in the service of SaaS providers. The network operator manages the platform's cloud provider, and the system's components are backed by software.

Cloud assessor: The role of conduct an independent assessment of online services. To guarantee conformity with rules, the auditor evaluates a range of technological data. Cloud service providers will be assessed health, protection, cost, as well as other factors [11].

Cloud adviser: Customers utilise a cloud broker to order cloud services rather than approaching the cloud source directly as incorporating online is complicated. In reality, the cloud adviser oversees cloud service usage, performance, and distribution, but also cloud consumer-cloud provider connections. The services provided by cloud brokers can be split into three types [12].

- *Service intermediation:* Intermediation of services By incorporating value-added providing price clients, a cloud system can improve a service. Only a few of the changes include access control, quality control, identity management, and increased security.

- *Service Aggregation* process of combining or merging multiple services into one or more new ones. In reality, serves as a conduit amid the cloud provider and a number of information centres.

- *Service arbitrage* Although it works in a similar way to program restructuring, it does not involve network repair. In actuality, service diversification enables a vendor to select services from a number of different agencies. For example, a network might employ a credit-scoring tool to locate and select the best agency.

- **Cloud carrier:** Works as an intermediary user to deliver cloud services. Cloud services are accessible to consumers via the internet and possibly other devices. As previously stated, by adopting SLAs with a cloud carrier, could service consumers. The clouds carrier is also responsible for keeping a supportive environment [13].

IV. Cloud security issues and challenges

The cloud computing paradigm, which is based on the internet, introduces a plethora of new

difficulties in data protection, access controls, and other domains. Cloud computing security has been the subject of numerous research publications over the previous decade [14]. [15] Offers a taxonomy for virtualized pc assaults that takes into account the size of the target, the source, as well as the attackers' goals. In fact, they must show how risks, networked security, and trust requirements have changed with time in virtual machines at many levels, including hardware, software, and applications. [16] Mentions an examination of cloud technology security issues. The difficulties of collection, storage space, secrecy, ease of access, with integrity were discussed in this study. [17] Demonstrates a wide range of knowledge security challenges as well as a tackling protection difficulty in multi-tenant situations. In fact, the focus of this study is solely for information as well as privacy protection. [18] Presents an overview of problems about security as well as isolation. Throughout this exertion, several types of well-known attacks and menaces, as well as numerous form of cloud flaws, be described. [19] Is a summary of the most serious cloud computing security threats. This evaluation effort also considers both interface' and vendors' key security concerns connected with cloud computing by providing architectures and technologies. [20] Gives an overview of the most serious cloud computing security issues. By giving techniques, this study work simultaneously interface' and vendors' important security challenges linked. But internet technologies have improved and new problems have emerged in current world, security concerns have increased and additional developments have emerged. As a result, a complete examination, issues, are required [12]. Furthermore, the majority of the aforementioned polls concentrated on cloud computing addressing problems, and hazards connected with cloud computing. We've gone over area of data protection as well as issues, as well as existing solutions, to the best of our ability.

V. Security policies

Security strategies define the requirements attacks to be prevented. These rules should protect the cloud-based work place while maintaining [23, 24]. Regulatory agencies regulate standards agreed terms (SLAs), client management questions, and antecedent trust [22].

5.1. Service-level agreement(SLA)

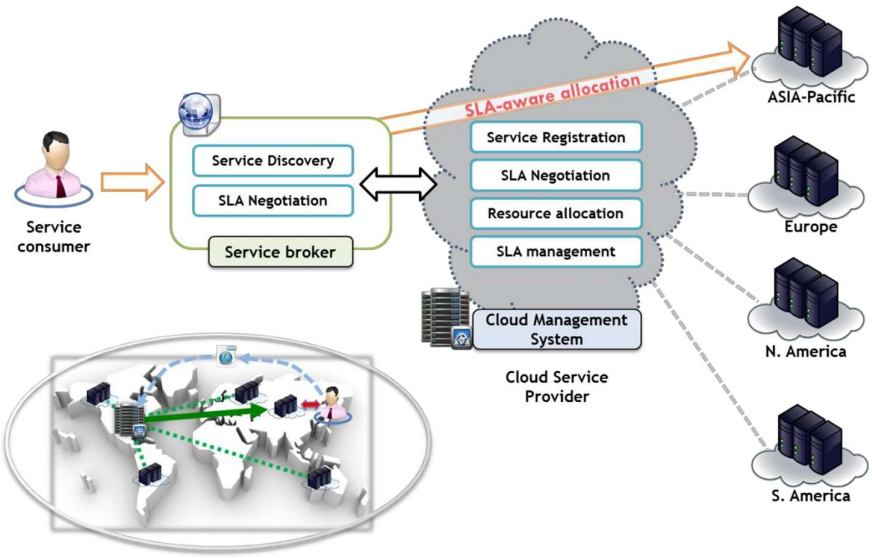

Fig 2: The SLA [23]

SLAs have an impact on customer expectations. SLAs also represent the performance of comparable facilities. SLAs, but at the other contrary, cannot ensure that a specific service will be delivered [23]. To put this another way, SLA allows you to chose a substandard service, but it does not making a subpar service lucrative. A statement of work (SLA) often consists of a statement of purpose. It also describes the company provider's and client's responsibilities under the SLA.

5.1. Clientmanagementissue

In recent years, most organisations have endeavoured to focus on the customer. Client administration includes user experience, user anonymity, a clients authentication method, and a client care agreement. It's one of its most pressing concerns in cloud security. We'll go over the various facets of cloud security in the next chapters [24].

5.2. Client authentication

Cloudsecurity issuesclassification

Securityp olicies	**User-orientedsec urity**	**Datast orage**	**Applicat ion**	**Networ k**
Servicelev	Authenticati	Datawa	Operatings	Intrusionpr

elagreement [47]	on	rehouse	ystems	eventionsystem
Clientmanagementissue [48]	Authorization	CIA Tired	Frontend/Back end	Intrusiondetectionsystem
Antecedenttrust [49]	Identityandaccessmanagement	Malware	Applicationvulnerabilities	Firewalls
		Metadata		

Fig 3:Classification cloud security issues [26]

Illegal activities are also banned from using cloud-based services. Users could control their apps from any device, including televisions, laptops, tablets, and smartphones. The authorisation of limited users can access cloud services is a hurdle for cloud service providers. Cookies reply assaults, credential discovery attacks, login stealing (for example, spamming or social engineering), and other authentication threats and assaults exist in the cloud. [25, 27].

5.3. Client-centric privacy

When privacy is compromised and data is released on the cloud, the most serious dangers develop [28]. In truth, provider data collecting is the origin of this issue, putting clients' privacy at danger. This problem is a major roadblock to clouds service adoption. When data is delivered to a cloud computer for processing, the user has no authority over how it is processed. Users are unaware of the location of the data storage. For example, the service provider may be allowed to share using this method.

VI. Security attacks and threat sin cloud computing

The cloud storage system, which consists of multiple hardware & system modules, is subject. Viruses, trojans, backdoors, and direct cybercrimes are all potential dangers. Data privacy / software protection will become progressively crucial as a result of excellent management and a cost-economic strategy [29].

6.1. Threat model and compromised attribute

Cloud computing benefits from dynamic scaling in a variety of ways, including increased speed and efficiency. Security issues include data breaches, misconfiguration, [30] defines a detection mechanism for attacks by one vms to another. A malicious tenants user might also start an operation by flooding the virtualization layer of the server with ICMP/UDP packets. Threats are divided into six categories, and a glimpse of hazards in a given area is

provided. Each STRIDE classification defines the features of assaults that constitute a specific threat. Indeed, the STRIDE security strategy categorises threats based on the result or influence of their reality. The step is to consider STRIDE has resulted in a more serious appraisal of the issues at hand. Furthermore, this research broadens the scope of the danger to also include advanced cloud technologies [31].

6.2. Spoofing

When an anonymous group transmits a communication that looks to come from a reputable with well-known source, this is known as spoofing. Spoofing is commonly used to get access to a user's sensitive information, infect a user with malware via corrupted file attachments, evade network access controls, even reallocate traffic in order to carry out a denial-of-service attack [32]. Connectivity filtering, which is normally done on something like a router, verifies the source headers on incoming IP packets.

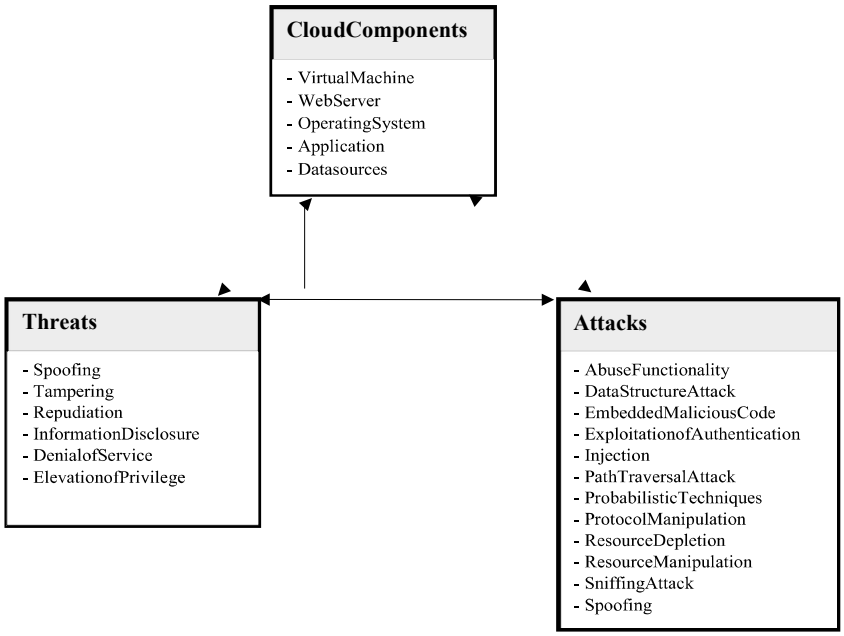

Fig 4: Cloud part, hazard, and attack classification [33]

VII. Exploitationofauthentication

Without a doubt, vulnerabilities in device identity verification systems must be addressed [64]. Most modern cloud computing systems use web-based apps, which become admired amid developer firms. Furthermore, for web-based applications, brute-force authentication assaults are a common target [33].

7.1. Injection

Attackers can change a database by inserting data or an inquiry into it, or by placing one or more kinds of adware on a machine. Buffer overflow attacks take several forms depending

on the software's execution contexts as well as the location of the fault in the programme that results in an attack. This is a popular form of system cracking or cracking attack that involves gaining unauthorised access to a device in order to collect data [34].

7.2. Pathtraversalattack

The fundamental goal of a ’re fully attack is to get access to data and subdirectories that's not in the browser folder. This exploit manipulates settings with "dot-dot-slash" strings as references to get access to remote files and folders on the file system. This technique has also been used to obtain access to personal system data like source code and settings. A have more attack, from the other hand, uses file servers to gain permitted access to remote settings like VM escape [35].

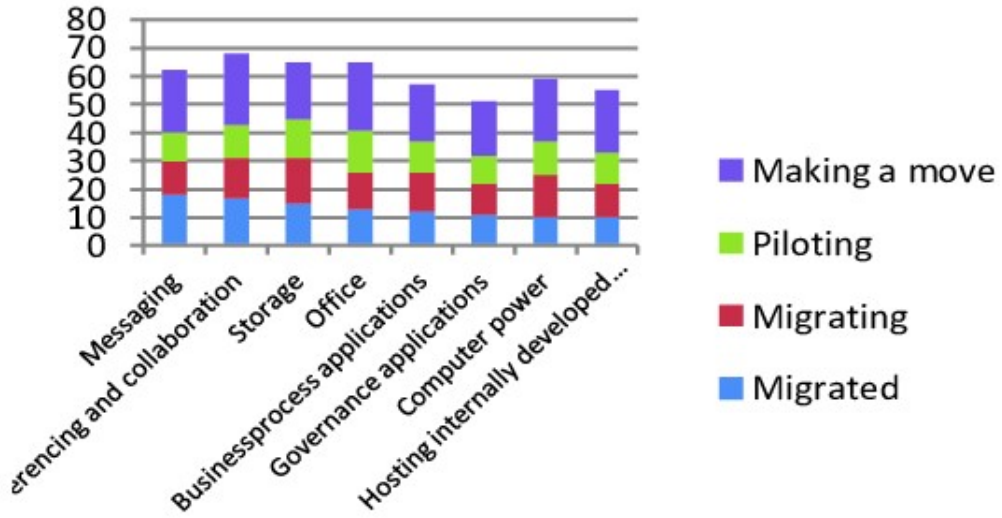

Figure 5: cloud environment in cloud computing

7.3. Protocol manipulation

The network protocols are subject to DoS attacks, which can be used to gather information about just the target's security by exploiting various application weaknesses and modifying the meanings of XML information exchanged between users and servers. Adversaries might force victims' machines to crash or be hijacked by delivering malformed data that exploit weaknesses in protocol implementations [36].

7.4. Resource depletion

A species loss attack is when a corrupted node is utilised to generate more network traffic while consuming the node's resources. in the cloud, including available bandwidth, bandwidth, and other processing capabilities. Despite the cloud's capacity to expand to suit a wide range of workload scales, destruction of natural resources attacks such injustices

documented to cause vulnerabilities are still possible [37].

7.5. Resource manipulation

Resource manipulation is the exploitation of one or much more assets in order to compromise the validity of a service, other than a cloud system., can all be jeopardised by this type of attack. Attackers may potentially utilise parameter tampering to compromise the information with infrastructure of the cloud. Web page's form field data without the user's permission. Manipulation of an object relationship to get unauthorised access the system and XML manipulation are examples of resource manipulation attacks [38].

7.6. Sniffing attacks

If security systems are misconfigured, this form of attack might sniff traffic on the network or allow stored in cloud user information in the cloud system to acquire sensitive data. Passive sniffing and aggressive sniffing are the two types of sniffing attacks. Whereas active sniffing uses programs and techniques to find information on the device. As a result of this type of attack, complete system vulnerabilities and software bugs would indeed be disclosed. These assaults hunt resource and vulnerabilities associated access to networking classified information. To get around normal authentication, scan features, keywords. On the other hand, authentication was among the most practical ensures that private data is protected from malicious attackers by keeping workstations secured mostly on network [39-41].

VIII. Cloud security issues in the future

End-user servers, networking connections, authentication and authorization systems, and cloud architecture are all part of the cloud computing model. Furthermore, when new technologies arise, such as 5G Network, Iot. (IoT), and smart cities, cloud technology will become more crucial than ever before for storing and managing massive data. The current market climate's heterogeneity has resulted in a fresh generation of potential vulnerabilities concerns. In recent years, organisations have been unaware of how much data they have kept, making it difficult to detect and address emerging security concerns [42]. Data duplication, inability to identify dangers in a reasonable timescale without a deep understanding of the broadband network, and a loss of data are all difficulties that security firms confront. Several research have been conducted in attempt to address concerns in cloud settings. However, there are still a number of difficulties that must be addressed get a stable. In such as cloud services, network, confidentiality of information, computer, and software platform security are all prevalent concerns. Security risks related to multi-tenancy, virtual, and shared pool infrastructures are all on the rise. When dealing in a cloud computing, you have access to a wide range of applications and resources, but the degree of skills and financial is determined by the resource. In cloud computing, computation privacy is a hot topic [43]. Encryption protects the majority of the data in the storage. The majority of calculation processes can obtain access to the processor's memory, which is used to save temporary data, on the inside

or outside. As a result, experts are currently developing a solution that ensures privacy when computing. To protect against security breaches, a cloud storage security solution is also required. Insider threat detection in cloud computing would still be a work in progress. This signal may help to improve the security of the cloud device. Similarly, determining who is a legitimate user and who is a malicious consumer is an outstanding challenge in the cloud [44]. Security systems are increasingly using Intelligent automation to simplify roles and deliver a greater level of intelligence [46-50], but it also makes it more difficult for them to stumble.

IX. Conclusion

Cloud infrastructures have become an indispensable aspect of corporate life, offering a widespread possibility to grow a firm through their ability to swiftly scale, allowing us to become resource nimble, and enabling new collaboration opportunities. Cloud computing, in fact, has various advantages for businesses, organizations, and even countries. Despite its many advantages, the cloud remains vulnerable to a variety of security vulnerabilities. As a result, security is the most significant obstacle to cloud adoption. Both the client and the vendors have a good understanding of the security risks. To put it another way, the current major goal is to incorporate all cloud computing capacity protection challenges, as well as effective solutions to these issues. Our paper's goal was to provide a survey various cloud security issues and problems that arise from the cloud's unique properties. A simplified perspective of these challenges has been provided here to illustrate the need of identifying security vulnerabilities within the public cloud machine and developing effective solutions for them. Based here on line of research, we advocate examining existing security schemes reducing connected world. These concerns are made up of facts and carriers.

REFERENCES:

[1] S Garg Algorithm for Virtual Machines in Cloud, p. 2 – 7 Posted: 2016 Mauch, Viktor, Marcel Kunze, Marius Hillenbrand Future Generation Computer Systems International Journal of Grid Computing and eScience, volume 29, p. 167 – 739

[2] S Garg Algorithm for Virtual Machines in Cloud, p. 2 – 7 Posted: 2016 Mauch, Viktor, Marcel Kunze, Marius Hillenbrand Future Generation Computer Systems International Journal of Grid Computing and eScience, volume 29, p. 1408 – 1416 Posted: 2012

[3] Robiah Qusay Kanaan Kadhim, Yusof A Review Study on Cloud Com-putting Crossref IOP Conference Series: Journal of Physics: Conference Series, volume 1018, p. 1 – 8 Posted: 2018

[4] Settu Bharti, Naseeb Singh Load Balancing Issues and its Solution in Cloud Computing: A Review International Journal of Computers and Technology, volume

14, issue 6, p. 5803 – 5808 Posted: 2015

[5] Sambit Mishra, Bibhudatta Kumar, Priti Paramita Sahoo, Parida Load balancing in cloud computing: a big picture Journal of King Saud UniversityComputer and Information Sciences, p. 1 – 31 Posted: 2018

[6] Alam Mahfooz, Zaki Ahmad Khan Issues and challenges of load balancing algorithm in cloud computing environment Indian Journal of Science and Technology, volume 10, issue 25, p. 1 – 12 Posted: 2017

[7] K Bhargavi, B Sathish, Babu Load Balancing Scheme for the Public Cloud using Reinforcement Learning with Raven Roosting Optimization Policy (RROP) CSITSS 2019 -2019 4th Int. Conf. Comput. Syst. InfCrossref

[8] H Gupta, K Sahu Honey bee behavior based load balancing of tasks in cloud computing Int J Sci Res, volume 3, issue 6 Posted: 2014

[9] S Afzal, G Kavitha Load balancing in cloud computing -A hierarchical taxonomical classification J. CLOUD Comput. Syst. Appl, volume 8, issue 1 Posted: 2019-12

[10] A Gupta, R Garg Load Balancing Based Task Scheduling with ACO in Cloud Computing 2017 INTERNATIONAL CONFERENCE ON COMPUTER AND APPLICATIONS (ICCA, p. 174 – 179 Posted: 2017

[11] S Mousavi, A Mosavi, A R Varkonyi-Koczy, G Fazekasi Dynamic Resource Allocation in Cloud Computing ACTA Polytech. HUNGARICA, volume 14, issue 4, p. 83 – 104 Posted: 2017

[12] M Kanthimathi, D Vijayakumar An Enhanced Approach of Genetic and Ant colony based Load Balancing in Cloud Environment IEEE INTERNATIONAL CONFERENCE ON SOFT-COMPUTING AND NETWORK SECURITY, p. 203 – 207 Posted: 2018

[13] P Kumar An Adaptive Approach for Load Balancing in Cloud Computing Using MTB Load Balancing Work. Recent Adv. Innov. Eng, volume 2018, p. 1 – 5 Posted: 2018-11

[14] C Sudhakar, R Jain, T Ramesh Cloud Load Balancing -Honey Bees Inspired Effective Request Balancing Strategy 2018 INTERNATIONAL CONFERENCE ON COMPUTING, POWER AND COMMUNICATION TECHNOLOGIES (GUCON), p. 605 – 610 Posted: 2018

[15] N X Phi, C T Tin, L N Thu, T C Hung Proposed load balancing algorithm to reduce response time and processing time on cloud computing Int. J. Comput.

Networks Commun, volume 10, issue 3, p. 87 – 98 Posted: 2018

[16] R Kaur, D K Singh Dhindsa Efficient Task Scheduling using Load Balancing in Cloud Computing Int. J. Adv. Netw. Appl, volume 10, issue 3, p. 3888 – 3892 Posted: 2018

[17] K P Kumar Gravitational Emulation-Grey Wolf Optimization technique for Load balancing in Cloud Computing

[18] PROCEEDINGS OF THE SECOND INTERNATIONAL CONFERENCE ON GREEN COMPUTING AND INTERNET OF THINGS, p. 177 – 184 Posted: 2018

[19] B N Gohil, D R Patel A hybrid GWO-PSO algorithm for load balancing in cloud computing environment Proceedings of the Second International Conference on Green Computing and Internet of Things India Bangalore , p. 185 – 191 Posted: 2018-08

[20] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, ‘‘ReTrust: Attackresistant and lightweight trust management for medical sensor networks,’’ IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 4, pp. 623–632, Jul. 2012.

[21] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, ‘‘Reputation-based framework for high integrity sensor networks,’’ ACM Trans. Sensor Netw., vol. 4, no. 3, p. 15, May 2008.

[22] L. Gomez, A. Laube, and A. Sorniotti, ‘‘Trustworthiness assessment of wireless sensor data for business applications,’’ in Proc. Int. Conf. Adv. Inf. Netw. Appl., 2009, pp. 355–362.

[23] D. Hui-Hui, G. Ya-Jun, Y. Zhong-Qiang, and C. Hao, ‘‘A wireless sensor networks based on multi-angle trust of node,’’ in Proc. Int. Forum Inf. Technol. Appl., 2009, pp. 28–31.

[24] F. Kazmi, M. A. Khan, A. Saeed, N. A. Saqib, and M. Abbas, ‘‘Evaluation of trust management approaches in wireless sensor networks,’’ in Proc. 15th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST), Jan. 2018, pp. 870–875.

[25] H. Rathore, V. Badarla, and K. J. George, ‘‘Sociopsychological trust model for wireless sensor networks,’’ J. Netw. Comput. Appl., vol. 62, pp. 75–87, Feb. 2016.

[26] R. K. Chahal, N. Kumar, and S. Batra, ‘‘Trust management in social Internet of Things: A taxonomy, open issues, and challenges,’’ Comput. Commun., vol. 150, pp. 13–46, Jan. 2020.

[27] A. Chitra and G. Kanagachidambaresan, ‘‘Fault aware trust determination algorithm for wireless body sensor network (WBSN),’’ in Proc. 1st Int. Conf. Smart Syst., Innov. Comput., 2018, pp. 469–476.

[28] A. R. Bhangwar, P. Kumar, A. Ahmed, and M. I. Channa, ‘‘Trust and thermal aware routing protocol (TTRP) for wireless body area networks,’’ Wireless Pers. Commun., vol. 97, no. 1, pp. 349–364, Nov. 2017.

[29] X. Liang and I. Balasingham, ‘‘A QoS-aware routing service framework for biomedical sensor networks,’’ in Proc. 4th Int. Symp. Wireless Commun. Syst., Oct. 2007, pp. 342–345.

[30] T. van Deursen, P. Koster, and M. Petković, ‘‘Hedaquin: A reputationbased health data quality indicator,’’ Electron. Notes Theor. Comput. Sci., vol. 197, no. 2, pp. 159–167, Feb. 2008.

[31] H. Zemrane, Y. Baddi, and A. Hasbi, ‘‘Ehealth smart application of WSN on WWAN,’’ in Proc. 2nd Int. Conf. Netw., Inf. Syst. Secur. (NISS), 2019, p. 26.