iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.41862

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Cloud, Fog and Edge Computing: Security and Privacy Concerns

Ketaki Patil[1], Saisrijan Gupta[2], Anjali Nair[3], Vitthal Gutte[4]
[1, 2, 3, 4]*School of Computer Engineering and Technology Dr. Vishwanath Karad MIT World Peace University, Pune, India*

Abstract: ***The use of different cloud computing technologies increased with the rise of 5G technology and IoT. Cloud computing also enabled intense data processing and warehousing. Data storage in the cloud comes with several issues and security concerns. Moreover, when the volume of data created by every device increases, the conventional cloud computing architecture fails to address concerns such as excessive latency, bandwidth limits, and resource constraints. As a result, new computational paradigms such as edge and fog computing have been proposed to address the former's issues. Both of these paradigms offer computation and memory storage alternatives. Regardless of their benefits, implementing these technologies introduces many new privacy and security issues. This work presents a list of security and privacy concerns, as well as dangers, that exist in all three computing paradigms: cloud, fog, and edge computing.***
Keywords: Fog Computing, Cloud Computing, Edge Computing Security and privacy issues, Attacks.

I. INTRODUCTION

Cloud cloud computing is an emerging computing approach that stores data and applications on remote servers over the internet. Organizations are focused on decreasing costs and achieving more with less in today's economic environment while still attempting to be competitive. Over the past decade, cloud computing has been the major platform for storing and analysing enormous amounts of data. It has infiltrated a variety of areas, including healthcare, education, real estate, banking, and manufacturing. Instead of maintaining data on their local machines, businesses send it to the cloud.

Emerging technologies like 5G and IoT, traditional cloud computing is becoming ineffective in handling difficulties like excessive latency, resource allocation, and bandwidth limits. New technologies such as edge and fog computing are now being used to manage data from IoT devices and smart applications. Edge computing is a form of IT architecture that allows data from Internet of Things devices to be processed on or near the device. Rather than being processed in a cloud data centre, the data is processed locally on a local computer or server. After that, all of the edge devices send the data to the cloud storage repository. Because both fog computing and edge computing require intermediate processing and storage, the phrases are interchangeable.

II. LITERATURE REVIEW

Identifying and working upon the security and privacy concerns faced in the latest cloud computing paradigms is of utmost importance in the current times. Many researchers have dedicated their time to analyzing and gaining research insights through the extensive study of attacks on the various cloud computing paradigms, their impact and the solutions suggested on them. This section focuses on the works done previously in this field.

Venkatesh et al.[1] Data security was highlighted as an important issue in Cloud Computing. They've uncovered a number of approaches for securing data storage in the cloud.

Ahmed [2]discussed various security challenges relating to data privacy and reliability, as well as critical elements affecting cloud computing and recommendations for specific areas.

Danish J et al.[3]discussed a number of cloud computing security challenges including Browser Security , XML Signature Element Wrapping, and Flooding Attacks, Cloud Malware Injection Attacks, as well as various solutions.

Wani, A.R et al[4] highlighted security vulnerabilities in cloud computing and gave solutions for both cloud service providers and customers. As a result, this paper investigated cloud security by identifying security needs and attempting to provide a practical solution that can mitigate these dangers.

Maurantonio Caprolu et al. [7] have identified security issues in four major Edge/Fog computing scenarios and also have highlighted the practical solutions that affect the security of Edge/Fog paradigm are also presented.

Mithun Mukherjee et al. [8] have presented the security challenges, privacy issues, and main factors that are responsible for them in an edge computing environment.

©IJRASET: All Rights are Reserved

Rahman Atiqur et al. [9] have discussed the MEC (Mobile Edge Computing) concept and architecture of in the IoT domain. Protection and confidentiality mechanisms of MEC are also assessed. At last, use case scenario on autonomous vehicles is presented.

Mithun Mukherjee et al. [13] highlighted the privacy and security issues that are faced by the end-user while using fog computing. It also focuses on identifying the research gaps that are triggering multiple attacks. Various difficulties have been identified, along with corresponding research challenges.

Shanhe Yi et al.[15] has discussed various issues related to fog computing. They have mainly focused on Privacy and Data Storage. Various methods have already been proposed to address the problem however, there are many obstacles to overcome before they can be implemented successfully.

III. CLOUD COMPUTING (CC)

National Institute of Standards and Technology (NIST) defines cloud computing as "concept for providing simple, on-demand network access to a shared pool of programmable computer resources."[5].It refers to saving and fetching data across the Internet, not the computer's hard disk drive.

A. Architecture

CC is a type of internet-based computing which processes applications by sharing computing resources instead of using local servers or private machines. Figure. 1 depicts the cloud computing architecture.

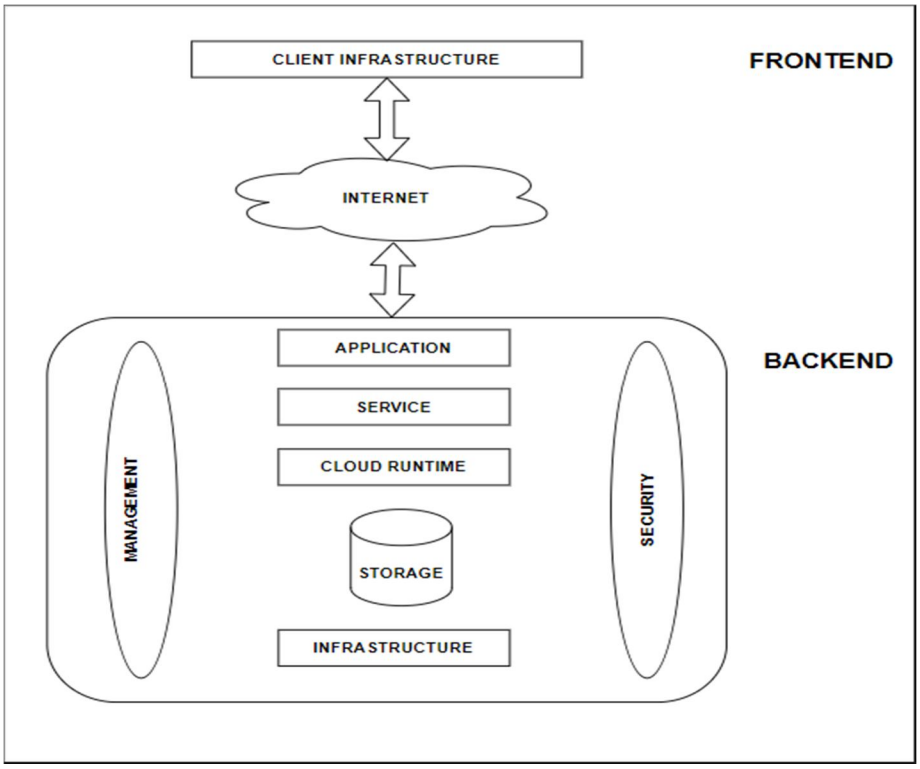


Figure 1:Architecture of Cloud Computing

Cloud computing architecture is a blend of service-oriented and event-driven design. Cloud computing provides 3 levels of Services:

1) *SaaS (Software as a Service):* The consumer is permitted to utilize the provider's cloud-based apps. The applications may be accessible on several client devices via a thin client interface.
2) *PaaS (Platform as a Service):* Users can design, test, run, and manage applications using the PaaS framework. Users get the basic OS and some development software, in addition to the infrastructure required to build the app.
3) *IaaS (Infrastructure as a Service):* Clients can rent networking, storage, servers, and additional computer facilities in the cloud on a pay-as-you-go basis from the seller.

3 kinds of Cloud:

a) *Private Cloud:* A private organization uses the cloud for its own purposes. This category restricts access to a certain set of people. Private clouds, which might be a single house or an industry cloud, are designed for private benefits.
b) *Public Cloud*: In this situation, cloud infrastructure is housed on the vendor's premises. As a result, the user has no control over or visibility into where the cloud infrastructure is housed. As a result, the infrastructure of the public cloud is shared among users who are members of the same public cloud. Used for common purposes, such as providing public services on a rental basis. Charges are imposed on the client as a result of their use of the service.
c) *Hybrid Cloud:* Combines public and private resources. It is handy when a business has certain vital data/applications that must be hosted in a private cloud and others that do not require high security and must be stored in a public cloud.

B. Attacks

1) *Denial of Service(DoS):* DoS attacks are typically directed towards a server that is delivering a service to its users. DoS attackers impersonate real customers to overwhelm active servers, causing the service to become unavailable due to a huge number of outstanding requests and overflowing the service queue. Distributed DoS, type of DoS in which the attackers are a collection of machines attacking a single service [6]. More than 20% of businesses around the world have experienced at least one DDoS assault on their infrastructure[6].
2) *Injection of cloud malware*: The goal of this attack is to infect the Cloud system with a malicious service implementation or VM.
3) *Phishing Attack:* Phishing is a social engineering method used to get access to personal information from an unwary user. It is typically accomplished by including WebPage URLs inside emails or direct chats.

C. Security and Privacy Issues

1) *Data Loss:* One of the problems with CC is data loss. Data Leakage is an alternative word. If the security of a cloud service is hacked by hackers, hackers are likely to acquire access to our personal files or data.
2) *Data Confidentiality:* Confidentiality is a major point of contention in cloud computing. Data confidentiality refers to only allowing authorized users access to data, and it is closely linked to authentication. In another sense, confidentiality refers to the security of user data in cloud systems. Users' data is stored publicly via cloud computing. The user's data and calculation work must be kept private from the service provider and other users to maintain confidentiality. Other users must not have access to the user's sensitive information.
3) *Data Integrity:* Integrity is another important issue with cloud computing. Data integrity refers to ensuring that data hasn't been altered in any way by an uncertified individual. It's a way of guaranteeing that data is authentic, correct, and safe from uncertified access. Because it allows users to share resources, data can be corrupted by unauthorized users.
4) *Data Availability:* The goal of availability in CC systems is to allow customers to access any facilities from any location and at any time. As a result, the provider must ensure that services are available to users at all times and that they are not interrupted.
5) *Data Location:* Cloud computing allows for a lot of data mobility. Consumers aren't always aware of where their data is stored.
6) *Data Breach:* Many users' data and the organization's data are kept together in a cloud. Breach of cloud infrastructure will target all users' sensitive data. A hack in the cloud system could also suggest that the encryption and decryption tools have been compromised.
7) *User Level security:* The vendor has provided a very robust security layer for the customer, and the customer should ensure that no data for other customers utilising the same Cloud is lost as a result of the customer's actions.
8) *Vendor Level Security*: A cloud is beneficial if the company provides excellent security to its clients. The server is well-protected against any external threats, which is something the vendor should ensure.
9) *Trust Issue:* In cloud computing, trust is a critical problem that must be obtained in both traditional IT and cloud computing. Trust is built on the assumption that data, people, information, and things will act or perform as expected. As a result, it is critical for consumers to have complete faith in their cloud provider when it comes to storing data on its servers. Unfortunately, people are still hesitant to retain sensitive data because they are concerned about data abuse or theft. As a result, it is critical for cloud providers to establish a trust relationship with their customers.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

IV. EDGE COMPUTING (EC)

The main aim of edge computing architecture is to bring processing in close proximity to the source of data. In this architecture, the data is partially processed in the device that creates it, or in a separate device at the edge of the network. [7]

A. Architecture

The functional organization of edge computing architecture is described in the Figure 2.

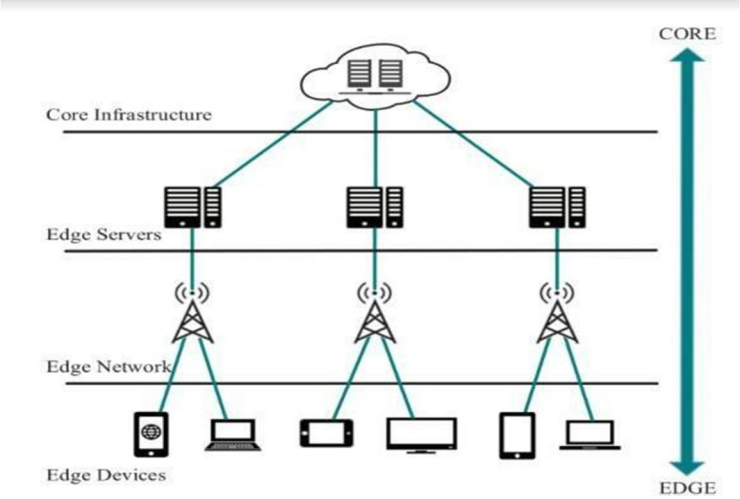


Figure 2:Architecture of Edge Computing[10]

Core infrastructure offers mobile edge devices with core network access as well as centralized cloud computing services and administrative capabilities.

Second, edge servers offer virtualized and multiple management services. These servers are managed by the infrastructure provider have multi-tenant virtualization architecture.

Furthermore, the edge can deploy many edge data centers that work together and do not cut off from the standard cloud. Edge computing infrastructure connects edge infrastructure to the wireless network, data center network, and the Internet. Finally, edge devices are any devices linked to the edge network that act not just as data consumers but also as data providers in the distributed architecture for all four layers.

Every device that creates data falls under this category.

B. Attacks

1) *Jamming Attacks:* An attacker flooding a network with fake messages in order to impair communication, computational, or storage resources, is known as a jamming attack. This will prevent authorized users from accessing the EC network's infrastructure.
2) *Manual Attacks:* When attackers physically get access to Edge Computing nodes/devices, important and sensitive cryptographic data is recovered, and software/operating systems are tweaked or changed.
3) *Eavesdropping or Sniffing:* Attackers listen in on private talks across communication lines, such as usernames, passwords, and so on. They can get vital information about the network such as node configuration, node identification, and the shared network password.
4) *Non-Network Side-Channel Attacks*: Edge Computing (EC) nodes may leak important information even if they are not transferring any data. Identification of known electromagnetic signals or medical machine protocols, for example, can result in major seclusion concerns, as sensitive details regarding the device and patient is exposed.
5) *Forgery Attacks:* When an attacker injects new fake data packets into the receiver, producing system damage or failure, this is known as a forgery attack.
6) *Privacy Breach:* The functionality of Edge Computing nodes is to extract private details from user devices. This sensitive information might be shared with other networks units or users without users authorization, exposing them to attackers during data transfer and sharing.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Security and Privacy Issues

1) The system is vulnerable to unauthorized users due to weak security credentials.
2) Insecure device-to-device communication
3) Data recovery and backup in the event of a system failure
4) Updates are not received and implemented on time.
5) Network visibility is limited.
6) Lack of user-selective data collection
7) Universal access to intelligent edge network services
8) Data and transaction privacy and anonymity

V. FOG COMPUTING (FC)

Cloud computing experiences difficulties in significant traffic jams, end-to-end delay, communication expenses, data processing, etc. [12] Fog computing (FC) is emerging as an another option to standard CC for supporting latency- sensitive, geographically scattered, delay-sensitive, and QoS- aware IoT (Internet of Things) applications. The term "fog computing" refers to " a situation in which a large number of diverse (autonomous and wireless) widespread and distributed devices connect and potentially collaborate among themselves and with the channel to conduct storage and processing functions without the involvement of third parties" [14].

A. Architecture

In the second tier, fog nodes are located above the edge devices, collecting data from many edge devices. This layer's fog nodes are network devices like routers, gateways, switches, etc. Computational Resources and storage can be shared by fog nodes in a cooperative manner. To gather data from the end devices, fog servers use transport layer technologies such as Bluetooth or Wi-Fi. Routers or base stations are commonly used to create fog nodes. The uppermost layer is the cloud centre, that receives data from the fog nodes. Figure. 3 depicts the architecture of fog computing.

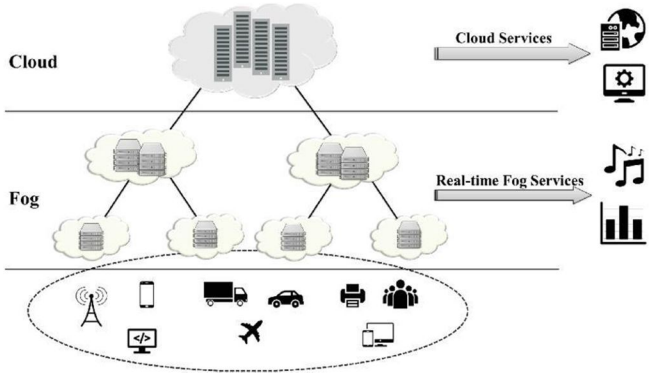


Figure 3:Architecture of Fog Computing[17]

B. Attacks

1) *Virtual Machine based attacks*: In this attack, A hacker gains access to the hypervisor, which generates a virtual environment within a virtual computer, in stealth.
2) *Side-Channel Attack:* The machine's security is reverse engineered by gathering details about its cryptographic algorithms in a side-channel attack.
3) *Session Hijacking:* User session is blocked and taken over by different user in order to acquire user's services and data.
4) *Inessential Logging Attacks:* In EC-assisted IoT systems, this sort of attack might cause damage if log files are not secured. As a result, infrastructure and system developers should keep track of incidents like application faults and failed/ successful authorization/ authentication attempts.

C. Security and Privacy Issues

1) *Virtual Machine Trust:* The reputation-based trust model is one of numerous trust management methods in cloud computing that is frequently utilised in e-commerce services. Because of the powerful nature of End User's machines. and fog nodes in the fog layers makes this service model unsuitable for fog computing.

2) *Authentication:* Because front fog nodes gives services to massive-scale end user, authentication is a critical challenge for fog computing security.
3) *Network Security:* Network attacks can be sniffer attacks, jamming attacks, etc. Normally, we must trust network administrator-created layout and keep network administration traffic separate from regular data traffic in a network. Fog nodes, on the other hand, are installed at the Internet's edge, putting a massive load on network management.
4) *End User's Privacy:* Privacy protection is more difficult with fog computing since fog nodes in close proximity to End User's may acquire private data about end users' identities, utilities usage or the location of users in relation to the core network's remote cloud server. Data leakage could result from higher transmission between the 3 layers that make up the fog architecture. Analyzing an adversary's usage behaviours of fog services, such as smart grid, might also expose user habits. Even if systems are well- designed and properly deployed, side channels might expose sensitive information. Electromagnetic radiation, heat flow from machines, power utilisation of specific machines and observable timing of some activities are some of the examples of possible information leakage via side channels [18].
5) *Secure Data Storage:* The user data is outsourced to fog nodes, and users' control over data is handed over to fog nodes, posing the same security risks as cloud computing. Designing secure storage systems that accomplish support dynamic operation, low-latency, and cope with fog-cloud interaction are new issues in fog computing.

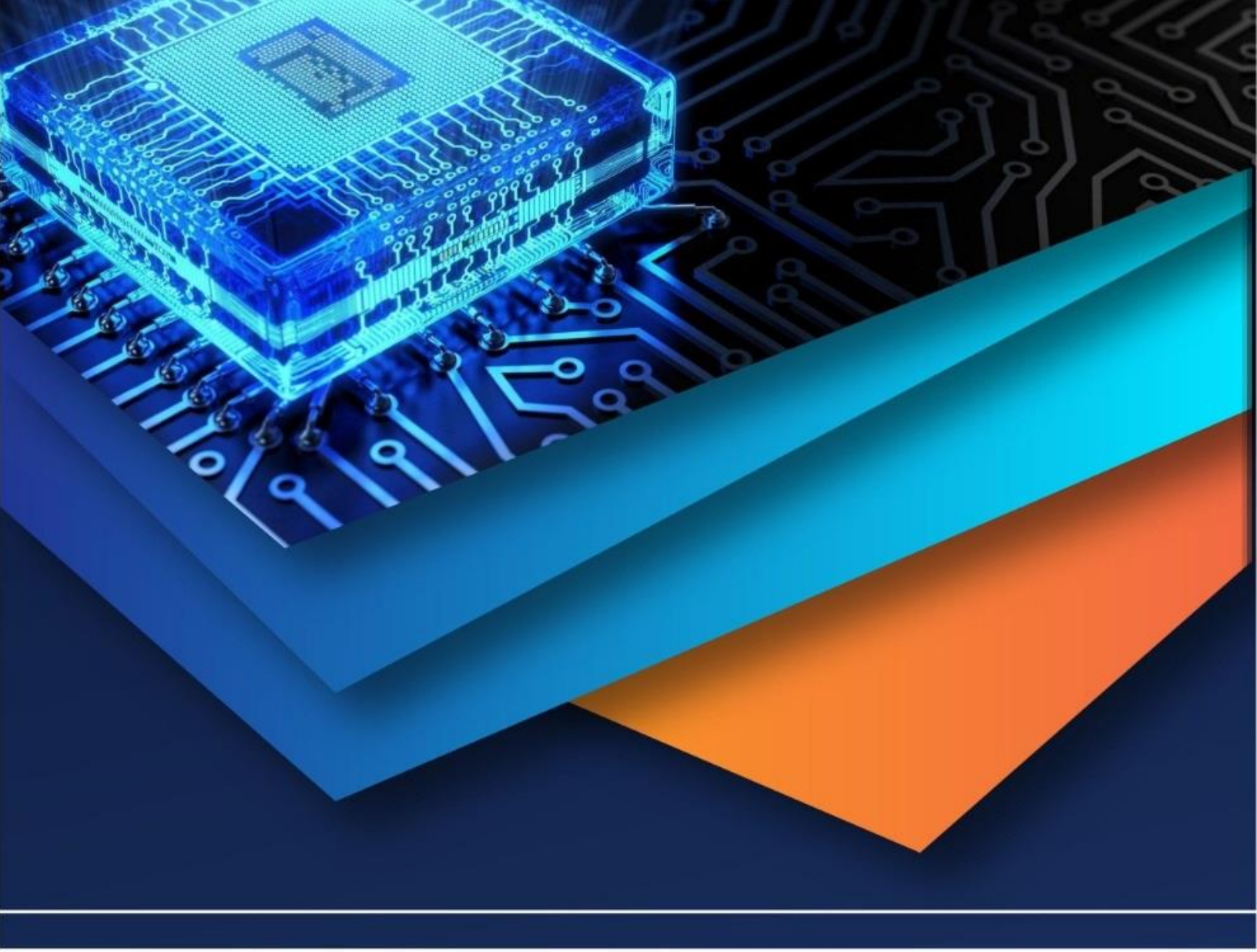
VI. CONCLUSION

Cloud computing is constantly evolving in order to provide customers with various levels of on-demand services. While many individuals appreciate the advantages that cloud computing provides, cloud security is a major concern. Clouds still have a lot of vulnerabilities, and hackers are continually exploiting them. This paper provides an overview of security and privacy concerns for the Cloud, Edge, and Fog computing paradigms.

REFERENCES

[1] Venkatesh, A. and Eastaff, M.S., 2018. A study of data storage security issues in cloud computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(1), pp.1741-1745.
[2] Ahmed, I., 2019. A brief review: security issues in cloud computing and their solutions. Telkomnika, 17(6).
[3] Jamil, D. and Zaki, H., 2011. Security issues in cloud computing and countermeasures. International Journal of Engineering Science and Technology (IJEST), 3(4), pp.2672-2676.
[4] Wani, A.R., Rana, Q.P. and Pandey, N., 2019. Analysis and countermeasures for security and privacy issues in cloud computing. In System performance and management analytics (pp. 47-54). Springer, Singapore.
[5] Ouahman, A.A., 2014. Security and privacy issues in cloud computing. Journal of Defense Resources Management (JoDRM), 5(2), pp.99-108.
[6] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.
[7] Caprolu, M., Di Pietro, R., Lombardi, F., & Raponi, S. (2019, July). Edge computing perspectives: architectures, technologies, and open security issues. In 2019 IEEE International Conference on Edge Computing (EDGE) (pp. 116-123). IEEE.
[8] Mukherjee, M., Matam, R., Mavromoustakis, C. X., Jiang, H., Mastorakis, G., & Guo, M. (2020). Intelligent edge computing: Security and privacy challenges. IEEE Communications Magazine, 58(9), 26-31.
[9] Atiqur, R., Wu, G., & Liton, A. M. (2020). Mobile edge computing for internet of things (IoT): security and privacy issues. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 18(3), 1486-1493.
[10] Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access, 6, 18209-18237.
[11] Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., &Hamdi, M. (2020). A Survey on Security and Privacy Issues in Edge- Computing-Assisted Internet of Things. IEEE Internet of Things Journal, 8(6), 4004-4022.
[12] Alwakeel, Ahmed M. "An Overview of Fog Computing and Edge Computing Security and Privacy Issues." Sensors 21.24 (2021): 8226.
[13] M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," in IEEE Access, vol. 5, pp. 19293-19304, 2017, doi: 10.1109/ACCESS.2017.2749422.
[14] Hu, Pengfei, et al. "Survey on fog computing: architecture, key technologies, applications and open issues." Journal of network and computer applications 98 (2017): 27-42.
[15] Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International conference on wireless algorithms, systems, and applications. Springer, Cham, 2015.
[16] Koo, Dongyoung, and Junbeom Hur. "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing." Future Generation Computer Systems 78 (2018): 739-752.
[17] Zhang, Tiehua & Jin, Jiong & Yang, Yun. (2018). RA-FSD: A Rate- Adaptive Fog Service Delivery Platform. 246-254. 10.1007/978-3- 030-03596-9_16.
[18] Alwakeel, Ahmed M. "An Overview of Fog Computing and Edge Computing Security and Privacy Issues." Sensors 21.24 (2021): 8226.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)