A study of the efficacy of the quality of service and the challenges of cloud computing and fog computing in low latency demand near-real-time IoT applications: a survey

Chinmoy Bharadwaj

Assistant Professor,
Department of Computer Science,
Arunachal University of Studies, Namsai, India

***Abstract*- This paper is a study of the existing real-time applications for fog, edge, and cloud computing. Some security challenges of cloud computing as well as Fog, and edge computing has been applied in the area of near real-time IoT applications. The paper also develops a basic framework diagram for Fog, Edge, and Cloud Computing to reduce the delay period between the data center with the constrained bandwidths for quicker data transfer in near real-time IoT applications. An effective fog computing technique was required to solve the fog, edge, and cloud computing problem with low latency and a finite number of bandwidths for higher efficacy in near real-time IoT applications due to a huge growth in the availability of datasets with different data types. Here our research works out the existing vulnerabilities, threats, and countermeasures in the cloud computing model and fog computing model with concerning layers and presents a solution for Fog and Edge Computing threats in near real-time IoT applications faced by the cloud user in the fog, edge, cloud environment which gave some observations into countermeasures and controls. Lastly, we concluded the paper by highlighting some open challenges in terms of security management, computation, storage, and energy consumption that can be further studied by a researcher in depth to increase the efficacy of fog computing in the cloud. This research paper brought light to the drawbacks of cloud computing, including its inability to identify threats and vulnerabilities, its reliance on energy application interface protocols, and its poor resource management among multiple fog nodes. The paper will further enlighten the near real-time IoT application of Fog, Edge, and Cloud Computing related to healthcare services and media streaming services.**

***Key Words*- Cloud computing model, Fog computing, Edge computing, IoT, Vulnerabilities, Threats, Countermeasures.**

1. INTRODUCTION

The Cloud computing model has its vulnerabilities and security issues which are growing, critical, and intelligent in terms of their level of penetration into the modern high-speed network infrastructure. Many attacks have been targeting cloud service models (SaaS, PaaS, and IaaS) and cloud deployment models (Private, Public, and Hybrid) from large-scale networks since the last decades, and several attacks launched in different real-life active networks such as Google, IBM, sales force.com, google app engine, yahoo, amazon web service, etc. Cloud Service Models and Cloud Deployment Models have many vulnerabilities and threats that are classified based on the layered architecture of the ISO-OSI model like network-layer and application layer. In the network layer, mostly the attack targeting towards the network resources, bandwidth, and architecture cloud computing service model. In the case of the application layer, attacks are launched and targeted toward the user's activity, common protocols, and the resources related to web services. Due to the increasing number of Internet users and intelligent attackers over the globe, it is indeed necessary to protect the users' activity as well as related resources from malicious attempts. These security issues should be nullified and blocked in the future to increase the efficiency of cloud computing models. Although researchers made significant contributions to provide security solutions for cloud computing models, there are yet several problems that remain to solve with adequate features while deploying in real-time networks. These are some academic views of cloud computing models and their security challenges by cloud computing researchers based on different ISO-OSI model layers. Now, we discuss some near-real-time IoT applications of cloud computing like health services, military services, and media streaming services, and its performances analysis in near real-time IoT applications. Cloud Computing applications helped in processing and sharing for immediate and effective decisions. It is also used for controlling different weapons data concerning time on different orders and commands during Wars. Interoperability among hybrid clouds has been recognized as a major tactical cloud issue in net-centric warfare and net-centric operations, that breaks all the organization boundaries between different systems in military organizations by supporting multitasking real-timeline within a tight Observe, Orient, Decide, and Act (OODA) loop. Although cloud computing has its positive side of the fastest sharing of information, controlling, and command of different orders, fastest communication, and connectivity among data centers in the military; still defense agencies are facing high-security challenges and risks in data-related vulnerabilities in traditional cloud computing environments. As a result of high latency in data transfer and high bandwidth in traditional cloud computing, some advanced tactical mobile cloud computing technologies like fog computing and edge computing are used to reduce the latency.

It has examined the aspects, including the use of technologies and methodologies, that can successfully enable the deployment of security policy on fog and cloud computing. The study focuses on Software-as-a-Service (SaaS) and intrusion detection, which offer users and enterprises an efficient and dependable system structure. The survey addressed the necessary

security tools, policies, and services, notably for cloud and fog environments for organizational adoption, intending to provide a framework for a cloud and fog computing security policy [1]. A discussion of a comprehensive literature review to pinpoint the similarities, differences, primary threats, and countermeasures in the various Cloud, Edge, and Fog computing paradigms. Research interest is currently high in the area of information security and privacy. Parallel to this, several computing paradigms, including cloud computing and edge computing, are already developing a distinctive ecosystem with various architectures, storage options, and processing power. This ecosystem's variety has some drawbacks, especially in terms of security and privacy issues [2]. It has been compared and discussed with each computing paradigm to examine the security issues of the cloud, fog, and edge computing paradigms where ingenious developments in cloud computing frameworks provide cooperative services of aid for end users and medium to large enterprises. Concern over data security is growing as more and more personal and corporate data is being stored in the cloud. The biggest obstacle to the growth of cloud computing is security worries. The risk of data breaches in the cloud environment must be understood by clients. Cloud computing storage, networking, and computing capabilities are brought to the edge with fog computing. One of the most urgent issues with fog computing systems is safety and security [3]. A proposed heuristic algorithm to solve the above-mentioned problems of response delay, message failure, fault tolerance, and security provided by the Blockchain. The proposed model gets vehicle messages through SDN (Software defined network) nodes, which are placed on nearby edge servers, and the edge servers are validated by the blockchain to provide secure services to vehicles. The SDN controller, which exists on an edge server, and is placed on the roadside to overcome communication delays, receives different messages from the vehicles and divides these messages into two different categories. By evaluating the timeline, size, and emergency scenario, the edge server divides the messages. These communications were organized by the SDN controller and forwarded to the intended recipient. A fault tolerance system verifies the acknowledgments after the message has reached its intended recipient [4]. Various computing paradigms, features of fog computing, an in-depth reference architecture of fog with its various levels, a detailed analysis of fog with IoT, and various fog system algorithms have presented and also systematically examined the challenges in fog computing. Performance, security, latency, and network failure are just a few of the problems that integrated cloud computing must contend with as IoT applications continue to grow. These problems are addressed by bringing cloud computing closer to the Internet of Things for the development of fog computing [5]. An analysis has occurred of current fog computing system architectures, their features, security concerns associated with IoT devices, and existing countermeasures. Innovative technologies, such as cloud computing platforms, provide end consumers and medium-large businesses with international cooperative services. To maximize efficiency with low latency, location awareness, and geographical distribution applications, fog computing extends cloud computing storage networking and computing capabilities to edge and backbone servers on the cloud for Internet of Things (IoT) devices. Security and privacy issues are among the significant obstacles that fog computing systems must contend with [6]. It has proved the effectiveness of FogBus. A comparison of the features of FogBus to other frameworks already in use and assess the effect of different FogBus settings on system parameters through the deployment of an actual IoT application. According to the experimental findings, FogBus is relatively quick and light, and different FogBus settings can adjust the computing environment to suit the needs of the situation [7]. New paradigms like edge computing and fog computing based on their unique characteristics and application cases have been examined in addition, future research must resolve for societal acceptance, including resource management, security and privacy, and network administration [8]. The possibilities of utilizing mobile edge computing have been analyzed to improve data analysis for IoT applications while attaining data security and computational efficiency. It is also examined the architecture of mobile edge computing and explores the potential of utilizing mobile edge computing to enhance data analysis for IoT applications while achieving data security and computational efficiency. Finally, several promising approaches for edge-powered data analysis research are highlighted [9]. The development of distributed computing from utility computing to fog computing, as well as many research problems for creating fog computing environments [10].

2. METHODOLOGY

A basic framework diagram for Fog, Edge, and Cloud Computing model has been designed to reduce the latency and bandwidth for better efficacy in near real-time IoT applications.

Artificial intelligence is used in this case to make decisions at the edge, where that intelligence wants to make quick decisions in the cloud. Here, the time scheduled is very low because it is done in near real-time. For that, an efficient fog computing technique is required to solve the fog, edge, and cloud computing problem with low latency and a limited number of bandwidths for quicker data transfer in near real-time IoT applications due to a significant increase in the availability of datasets with various data types.

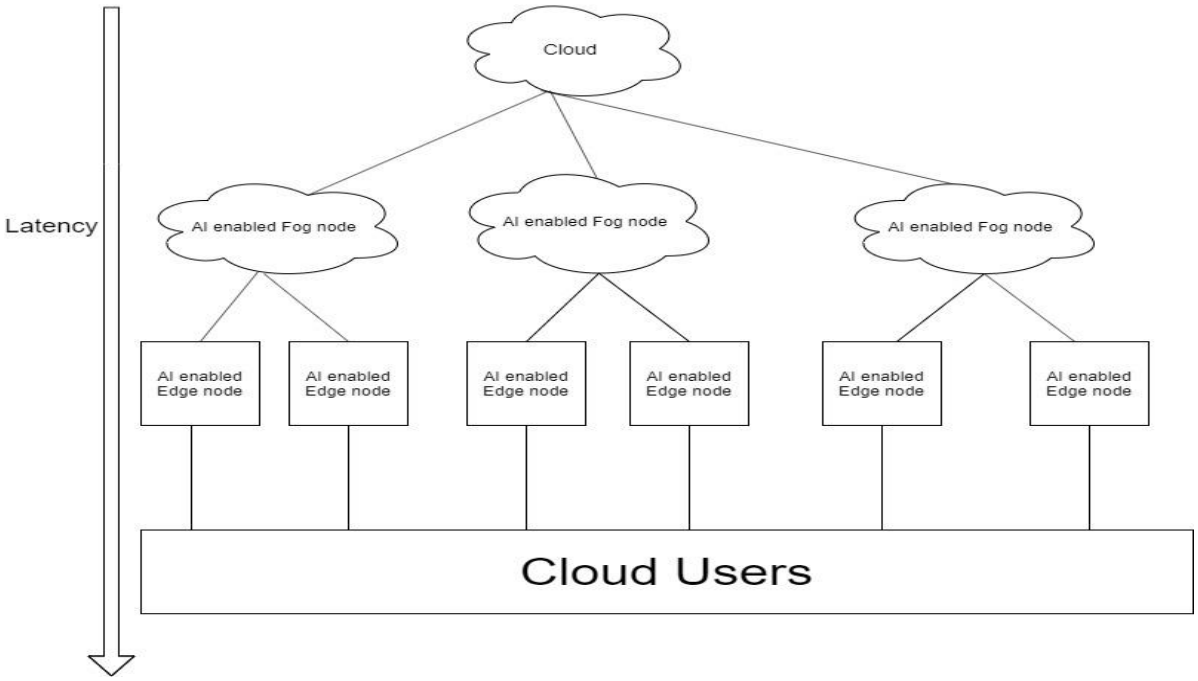

Figure 2(a): A basic framework diagram for Fog, Edge, and Cloud Computing

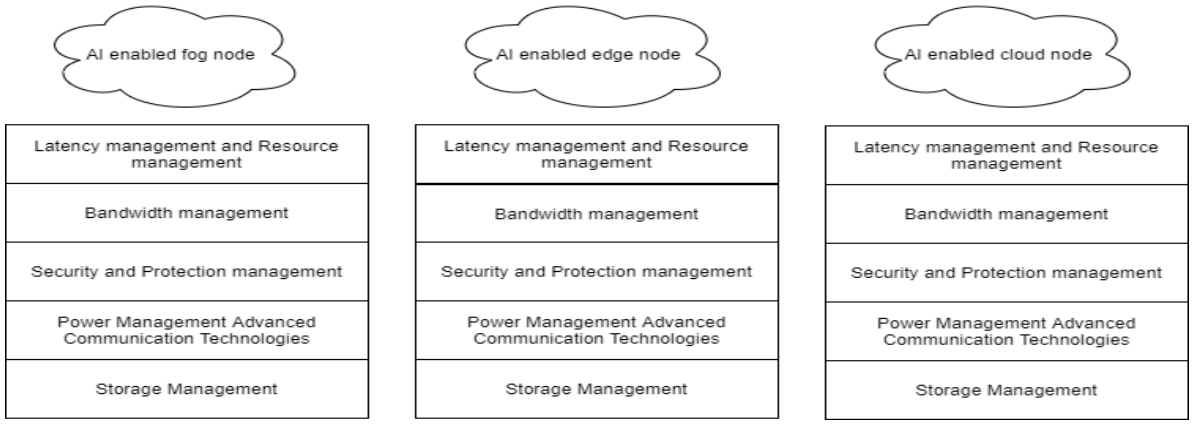

Figure 2(b): Functions of Fog and Edge node

3. RESULTS AND DISCUSSION

Table 1 summarizes the findings of the systematic view which shows the different issues considered in each approach

The majority of the approaches outlined identify, categorize, examine, and compile several vulnerabilities and threats targeted at cloud computing, as indicated in Table 1. There is a clear correlation between the vulnerabilities, threats, countermeasures, potential solutions, and techniques to solve them as a consequence of the studies' analysis of risks and threats and frequent recommendations on how they might be avoided or covered.

Table 1: A summary of the different issues considered in each approach

Paper No. →

Different issues	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**	**[10]**
Threats	√	√	√	√	√	√	√	√	√	√
Vulnerabilities	√	√	√	√			√		√	√
Countermeasures	√	√	√	√	√	√	√	√	√	√
Network Layer	√	√		√			√			√
Application Layer	√				√		√	√		

3.1 CLOUD SERVICE MODELS

Cloud computing has three types of service models such as Software as a service (SaaS) model, Platform as a service (PaaS) model, and Infrastructure as a service (IaaS) model.

From Table 2, we can compare the study of the Vulnerabilities, Threats, and Counter Measures of SaaS, PaaS, and IaaS cloud service models with respect to layers in cloud computing. The attacks of other layers have less impact than lower layers.

Table 2: Comparative study of the Vulnerabilities, Threats, and Counter Measures of SaaS, PaaS, and IaaS cloud service models with respect to layers in cloud computing

Cloud Service Models	**Vulnerabilities**	**Threats**	**Security Issues**	**Cloud Deployment Models**	**Countermeasures**	**OSI Layers**
SaaS (Software as a Service)	1)Data-related vulnerabilities	1) Data leakage	i)Multitenancy	Hybrid Cloud	a) Encryption b) Homo-morphic encryption c)FRS techniques d)Digital Signatures	Network Layer
SaaS (Software as a Service)	2)SQL Injection, OS Injection, Cross Site Scripting which is an API and insecure interface	2)User Data manipulation	i) Data Security ii)Application Security	Public Cloud	Web Application Scanner	Application Layer
SaaS (Software as a Service)	Cookie Poisoning	-	Application Security	Private Cloud	Data hiding techniques for regular cleanup of cookie data	Application Layer
SaaS (Software as a Service)	Google hacking attack	-	Application Security	Private Cloud	-	Application Layer
SaaS (Software as a Service)	Cross-Site Request Forgery	-	Application Security	Private Cloud	-	Application Layer
PaaS (Platform as a Service)	1) Data-related vulnerabilities	Data scavenging	SOA security	Hybrid Cloud	a) Encryption b) Homo-morphic encryption c)FRS techniques d)Digital Signatures	Network Layer

PaaS (Platform as a Service)	Data-related vulnerabilities	Data Leakage	Data Security	Hybrid Cloud	a) Encryption b) Homo-morphic encryption c)FRS techniques d)Digital Signatures	Network Layer
PaaS (Platform as a Service)	Resources unlimited	DOS attacks, DDoS attack	Network security, Fault tolerance	Public Cloud	Cloud policies to limit computation resources	Network Layer
PaaS (Platform as a Service)	-	Man, in the middle attack	Network security, Fault tolerance	Public Cloud	-	Network Layer
PaaS (Platform as a Service)	Insecure Interfaces and APIs	A dictionary attack, Injection attack, and Input validation related attacks manipulate customer's data	Application security	Private Cloud	WebApplicationScanner and for APIs security PAAS uses OAuth to enforce authentication authorization on calls to such APIs.	Application Layer
IaaS (Infrastructure as a Service)	Vulnerability in Virtual Network	Sniffing/spoofing virtual networks	Network security	Public Cloud	Xen Bridged and routed virtualnetworkframework modes	Network Layer
IaaS (Infrastructure as a Service)	Vulnerability in virtual machine	Data leakage	Network security	Hybrid Cloud	a) Encryption b) Homo-morphic encryption c)FRS techniques d)Digital Signatures	Virtualization Layer and Network layer
IaaS (Infrastructure as a Service)	Vulnerability in virtual machine image	Malicious VM creation	Application security	Public Cloud	Mirage is used for the attackslikeVMsuncontrolled snapshot of images	Application Layer
IaaS (Infrastructure as a Service)	Insecure VM migration	Uncontrolled Snapshots that cause data leakage	Application and Network Security	Hybrid Cloud	PALM, TCCP, VNSS	Network Layer
IaaS (Infrastructure as a Service)	Insecure Interfaces and APIs	Account of service hijacking	Application security	Private Cloud	Identity and access management guidance	Application Layer
IaaS (Infrastructure as a Service)	Vulnerability in hypervisors	Virtual machine escape	Application security	Private Cloud	Hypersafe, TCCPComputing platform, and trusted viral datacenter for the vulnerability in hypervisors.	Virtualization Layer
IaaS (Infrastructure as a Service)	No restriction on the allocation and deallocation of resources in VMs	VM hopping	Application security	Private Cloud	To keep hypervisor vulnerabilities out of reach from the attacker so that the attacks cannot communicate with the other VMs.	Virtualization Layer

3.2 LOW-LATENCY SERVICES IN FOG AND EDGE COMPUTING

Here, we have introduced the basic concepts of cloud computing, edge computing, and fog computing in low latency demand real-time IoT applications where the major challenges of using a traditional cloud environment in real-time IoT applications are high latency in data transfer and high bandwidth. This real-time challenge of cloud computing is overcome by Fog computing, which is an extension of cloud computing that provides high storage with high computation, in real-time IoT applications like health services, military services, video streaming, live updates, etc. Therefore, fog computing is the best paradigm that can fulfill such requirements, Augmented Reality system supported by fog computing can reduce latency in both processing and transmission and can maximize the throughput [11]. Fog Computing in Military and Aerospace has used tactical edge fog computing in Defense

applications where Artificial Intelligence out to the decision-making at the edge that intelligence at the edge wants to make quick decisions in the cloud. The time schedule is very low because it is done in real-time. This tactical cloud computing model helps in overcoming the data transferring issues created by low bandwidth and network connection problems [12] [13]. One of the types of tactical computing is Fog Computing which is a superset of Edge Computing that has the efficacy of low latency, high security, and high bandwidth in IoT platforms. These characteristics have made it attractive for real-time IoT applications like the fastest transmission of data among the data centers at high bandwidth around the world. Fog computing is the best option for computation for real-time low latency demand real-time applications [13].

3.3 SOLUTIONS FOR FOG AND EDGE COMPUTING THREATS

Fog computing is a significant area of research in knowledge for low latency among the data center with a finite number of bandwidths for faster transmission of data. Due to an enormous increase in the availability of datasets with various data types, an adequate fog computing technique is necessary for solving the fog, edge, and cloud computing problem with low latency and a limited number of bandwidths for better efficacy in near real-time IoT applications. Although, the use of Fog cloud computing has overthrown the problem of high latency and low bandwidth in IoT in the near real-time scenario by using artificial intelligence for decision-making. It also explains the positive side of fog computing in terms of the fastest data transmission around the edge of a network across the world in near real-time applications. The current countermeasures taken for those challenges in cloud and fog computing in terms of security management, resource management, and power management have been discussed in this paper concerning near real-time applications.

3.4 CHALLENGES AND SOLUTIONS

There are many security risks faced by the real-time IoT application even after uploading, sharing, and updating confidential and secret data in a cloud environment.

Some of the security challenges of the cloud in real-time IoT applications are as follows:

(i) Data duplication and resource pooling (tactical) are the most important advantages of cloud computing in the military still it creates major security challenges in the public cloud deployment models. This is the biggest security threat in the public cloud deployment model concerning the military application.

(ii) In the military, it is difficult to share massive data on the battlefield at low bandwidth and less time in traditional cloud computing models. No proper advanced data encryption technique is used in military applications which causes data-related security issues. Lack of antivirus programs and intrusion detection mechanisms to detect vulnerabilities and threats in the cloud computing models in the military [14]. Low authentication and identity management lead to access and stealing of military confidential information by illegitimate users. No standard strict cloud policies and data control policies are taken to protect cloud military services from attackers. There is no protection against accidental and illegal access to information.

(iii) No data verification technique. Some of the security issues of fog computing are Fault tolerance [15], Authentication and Trust issues, and Access Control. Man, in the middle attack [16] and DDoS attacks [17] [18], are the biggest threats to fog computing.

Some solutions to protect the cloud computing models from different vulnerabilities and threats in real-time IoT applications are as follows:

(i) Authorization and Identity management techniques like Encryption, Homo-morphic encryption, FRS techniques, Digital Signatures, and Smart cards for accessing and sharing data by legitimate users. Regular cleaning of the cookies [19] and secured IP protection and privacy policies.

(ii) Cloud security policies and privacy strategies to limit computation resources [12]. Intrusion detection techniques and antivirus programs to run and detect vulnerabilities and threats.

(iii) Tactical computing is also used for the connection of different weapons and their physical location on the battlefield. It helps in fast reliable networking among data centers and mission area services [14]. Proper data validation techniques to check its accuracy. Some defense agencies DISA, FISA, and DOD have set some standards, policies, and security requirements to protect the cloud military services and applications from illegitimate users and access information globally to military users with less cost and low power consumption [12].

(iv) Visual cryptography, image encryption, and watermarking for military weapons code security and to find out the hidden military weapons [14]. Web application scanner for SQL Injection, OS Injection, and Cross-Site Scripting.

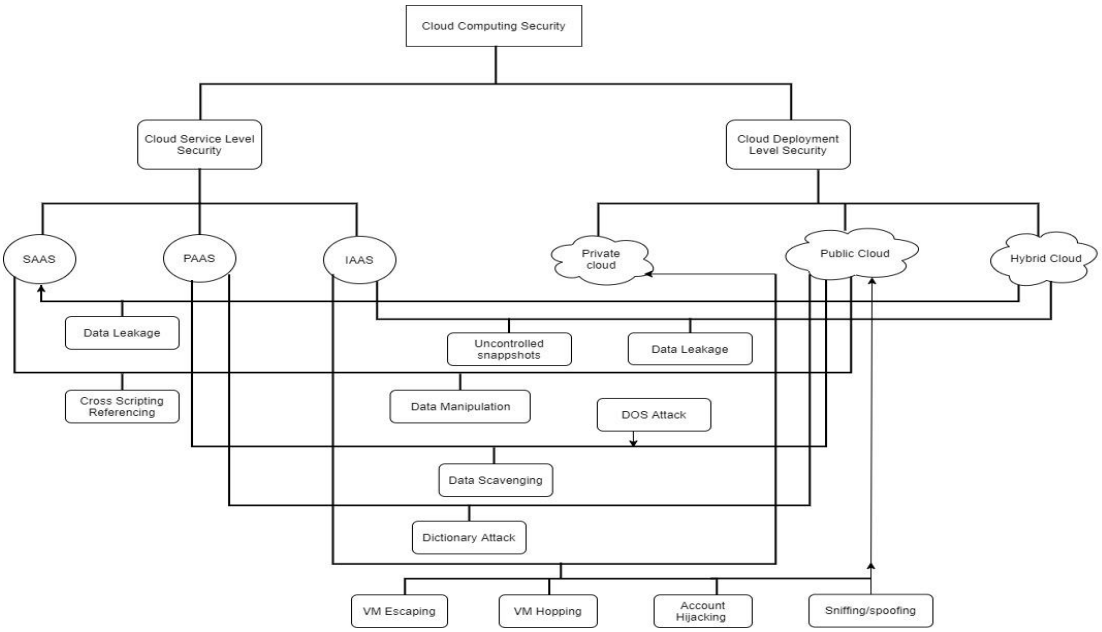

Figure 3.4 (a): Classification of the Malicious attacks of Cloud Computing and Fog Computing with respect to the Service and Deployment model.

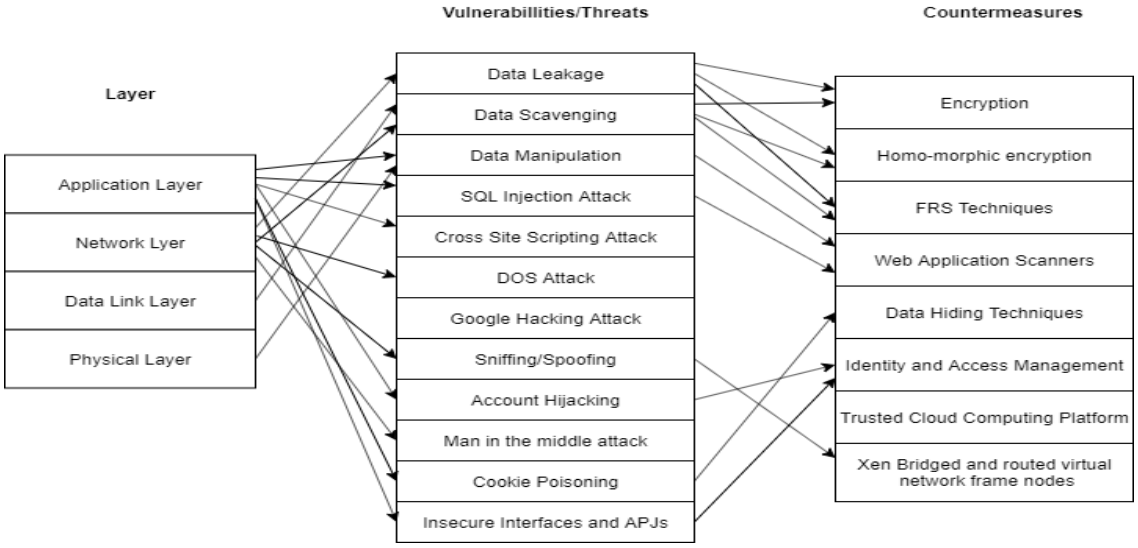

Figure 3.4 (b): It shows the relationships between the vulnerabilities, threats, and countermeasures taken for Cloud computing and Fog computing.

CONCLUSION

However, by applying artificial intelligence for decision-making, the usage of fog, edge, and cloud computing has been able to overcome the issue of high latency and low bandwidth in IoT in a near real-time situation. The fastest data transfer around a network's edge for near real-time applications is one of the benefits of fog computing that is discussed in this paper. On the other hand, we can find out the drawbacks of cloud computing, including its inability to identify threats and vulnerabilities, its reliance on energy application interface protocols, and its poor resource management among multiple fog nodes. This paper will go into further detail about how cloud, edge, and fog computing are used in near real-time IoT applications for healthcare and multimedia streaming.

ACKNOWLEDGMENT

At this juncture, I would like to express my sincere gratitude to Arunachal University of Studies authorities for giving me the opportunity to do the research and express my deep gratitude to all the respected teachers of the Computer Science Department, at Arunachal University of Studies.

REFERENCES:

1. Chang V, Golightly L, Modesti P, Xu QA, Doan LM, Hall K, Boddu S, Kobusińska A. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. Future Internet. 2022 Mar 13;14(3):89. https://doi.org/10.3390/fi14030089
2. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25;22(3):927.https://doi.org/10.3390/s22030927
3. Shah DR, Dhawan DA, Thoday V. An Overview on Security Challenges in Cloud, Fog, and Edge Computing. Data Science and Security. 2022:337-45. HTTPS: //doi.org/10.1007/978-981-19-2211-4_29
4. Ahmed A, Abdullah S, Iftikhar S, Ahmad I, Ajmal S, Hussain Q. A novel blockchain-based secured and QoS aware IoT vehicular network in edge cloud computing. IEEE Access. 2022 Jul 18; 10:77707-22.https://doi.org/10.1109/ ACCESS.2022.3192111
5. Sabireen H, Neelanarayanan V. A review on fog computing: Architecture, fog with IoT, algorithms and research challenges. IctExpress.2021Jun1;7(2):162-176. https://doi.org/10.1016/j.icte.2021.05.004
6. Ashi Z, Al-Fawa'reh M, Al-Fayoumi M. Fog computing: security challenges and countermeasures. Int. J. Comput. Appl. 2020 Aug;175(15):30-6.
7. Tuli S, Mahmud R, Tuli S, Buyya R. FogBus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software. 2019 Aug 1; 154:22-36. https://doi.org/10.1016/j.jss.2019.04.050
8. SchahramDustdar, C. IlirMurturi. Edge and FC: Vision and Research Challenges, 2394-0697. 2019 May 6; http://dx.doi.org/10.1109/SOSE.2019.00023
9. Ni J, Lin X, Shen XS. Toward edge-assisted Internet of Things: From security and efficiency perspectives.IEEENetwork.2019Mar27;33(2):507.https://doi.org/10.1109/MNET.2019.1800229
10. Nath SB, Gupta H, Chakraborty S, Ghosh SK. A survey of fog computing and communication: current researches and future directions. arXiv preprint arXiv:1804.04365. 2018 Apr 12.https://doi.org/10.48550/arXiv.1804.04365
11. Hu P, Dhelim S, Ning H, Qiu T. Survey on fog computing: architecture, key technologies, applications, and open issues. Journal of network and computer applications. 2017 Nov 15; 98:27-42.https://doi.org/10.1016/j.jnca.2017.09.002
12. Tibenszkyné FK. Application of cloud computing in the defense industry. ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 11:(1) pp. 195-296. (2012). 2012.
13. Foster KD, Shea JJ, Michael JB, Otani TW, Peitso L, Shing MT. Cloud computing for large-scale weapon systems. In2010 IEEE International Conference on Granular Computing 2010 (pp. 161-166). IEEE. https://doi.org/10.1109/GrC.2010.171
14. Tom J (2018) US Ballistic Missile System Riddled with Cyber Vulnerabilities. Cyber Security Management: pp. 1-6
15. DoD Directive 8100.1, GIG Overarching Policy, September 19, 2002. Accessed on June 3, 2010: http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d81001_091902/d810 01p.pdf
16. Dhelim S, Ning H, Zhu T. STLF: Spatial-temporal-logical knowledge representation and object mapping framework. In2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2016 Oct 9 (pp. 001550-001554). IEEE.https://doi.org/10.1109/SMC.2016.7844459
17. Gupta H, Vahid Dastjerdi A, Ghosh SK, Buyya R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge, and Fog computing environments. Software: Practice and Experience. 2017 Sep;47(9):1275-96. https://doi.org/10.1002/spe.2509
18. Viega J. Cloud computing and the common man. Computer. 2009Aug1;42(08):106-8. https://doi.ieeecomputersociety.org/10.1109/MC.2009.252
19. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. Journal of Internet services and applications. 2013 Dec;4(1):1-3. https://doi.org/10.1186/1869-0238-4-5