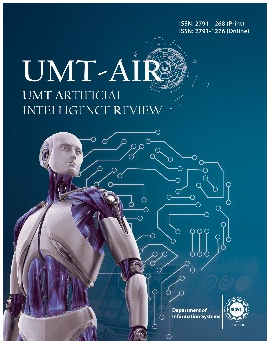

UMT Artificial Intelligence Review (UMT-AIR)
Volume 1 Issue 1, Spring 2021
ISSN(P): 2791-1276 ISSN(E): 2791-1268
Journal DOI: https://doi.org/10.32350/UMT-AIR
Issue DOI: https://doi.org/10.32350/UMT-AIR/0101
Homepage: https://journals.umt.edu.pk/index.php/UMT-AIR

Journal QR Code:

Article: **Architectures, Security Issues, and Usage Scenarios of EC**

Author(s): Amna Mubashar[1], Kalsoom Asghar[1], Rimsha Fareed[1], Muhammad Rizwan[1], Mian Usman Sattar[2]

Affiliation: [1]Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan
[2]Department of Management Sciences, Beacon house National University, Lahore, Pakistan

Article QR:

Amna Mubashar

Citation: M. Amna, A. Kalsoom, F. Rimsha, R. Muhammad, and U. S. Mian, "Architectures, security issues, and usage scenarios of EC," *UMT Artificial Intelligence Review,* vol. 1, pp. 55–73, 2021. https://doi.org/10.32350/UMT-AIR/0101/04

A publication of the
Dr Hasan Murad School of Management
University of Management and Technology, Lahore, Pakistan

Architectures, Security Issues, and Usage Scenarios of Edge Computing

Amna Mubashar[1], Kalsoom Asghar [1], Rimsha Fareed [1], Muhammad Rizwan [1], Mian Usman Sattar [2*]

ABSTRACT: Demand for digital media is increasing exponentially due to the enormous amount of data generated regarding the use of IoT devices. Thus, certain advancements have been made in various technologies, including cloud computing, which has transitioned to fog and edge computing, to meet the growing needs. Differences between each technology of computing relate to multiple factors, such as security, privacy, big data issues, bandwidth, and radio access networking. We discuss in this paper the problems faced by the older versions of cloud computing and how Mobile Edge Computing (MEC) helps to overcome most of these problems. MEC is explored as to where it offers real-time information, providing benefits to the end-users. The growth of MEC is such that, as discussed further, it is used in normal habitual routines, including real-time grocery shopping. This paper explores the various architectures, use cases and security aspects of edge computing.

KEYWORDS: Biometrics, cloud computing, edge computing, fog computing, PAM, RACS, SEcS, WiCloud

I. INTRODUCTION

Image denoising is a common using This research paper focuses mainly on edge computing, a relatively new technology that has yet to be explored. The use of the Internet of Things (IoT) is now widespread. Indeed, studies have shown that most people (75 percent) prefer online transactions. Hence, IoT has significantly contributed to expanding the trend of using online services by ensuring easy access and availability. Cloud computing is a

[1]Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan.

[1]Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan.

[1]Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan.

[1]Department of Management Sciences, Beacon house National University, Lahore, Pakistan.

*Corresponding Author: usman.sattar@bnu.edu.pk

[2]Department of Management Sciences, Beacon house National University, Lahore, Pakistan.

mixture of many previous technologies that have matured in different contexts. Cloud computing offers storage data on a cloud for the users, who may access it at any time[1]. It thus offers an application system running on a distributed network. However, it comes with many privacy and security issues[2]. A third party monitors the storage location. Hence, the users lose control of their data as soon as it is uploaded/stored on the cloud, which is susceptible to both internal and external[1].

Moreover, data integrity is compromised as the generated data can be altered [3].

As depicted in Fig. 1, fog computing extends the current version of cloud computing at the edge of the network, creating a new generation of applications and services [4]. Thus, fog computing incorporates some of the problems of cloud computing. Since devices are set up in public, they are prone to tampering and unauthorized access[5]. Fog is chosen because of the big data generated by IoT devices. A cloud is not efficient enough due to constraints regarding bandwidths. Fog computing enables the data to be better protected with higher bandwidth, as it minimizes or creates a bridge regarding the pace of covering the space between IoT devices and the cloud [6]. The integration of fog computing with IoT has given rise to a new service, commonly known as Fog as a Service (FaaS). As shown in Fig. 1, it gives a concept that conceptualizes fog nodes, with each node depicting information regarding computations, networking, and storage facilities. It also allows big and small companies to operate as private or public[5].

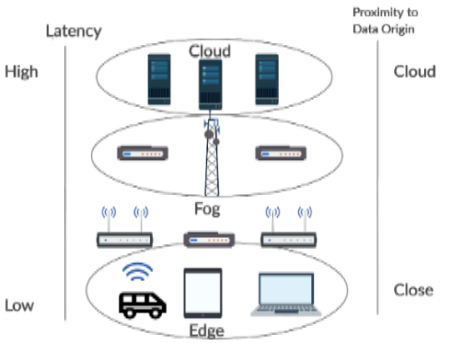

Fig.1. Layers of Edge, Cloud, and Fog Computing

New computing technology has emerged to meet the demand for cloud services known as edge computing. It is aimed to process data at the edge of the network[7]. In this particular technology, computing resources and application services are distributed all along the communication runway, from where the stored data points towards the base inside wireless networks[8]. This makes it

possible for subscribers to access the nearest computing servers located in the range of the particular wireless network[9]. Edge computing solves some cloud computing issues by moving processing and storage away from centralized points. It pushes applications, information, and administrations geographically closer to the source device. Edges may consist of a single computer for fewer nodes, ranging from industry PCs to workstations or servers[10]. Fog or edge computing extends cloud computing by providing it with virtualized resources and engaging in location-based services for mobile networks to serve the mobile traffic[11]. Edge computing utilizes recent technologies, such as offloading, virtualization, and outsourcing [12].

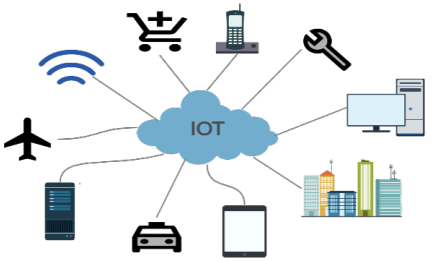

Fig. 2. Representation of the Internet of Things (IoT)

Hence, the basic technology for this purpose is IoT, which is essential in developing advanced technologies regarding these networking techs. Edge computing is a crucial element needed to maintain IoT infrastructure and network base. Fig. 2 clearly shows how IoT has become an integral part of networking. There are, however, security issues with it. Moreover, attacks on these schemes have been easily detected. Many proposals to mount a counter-attack to these threats have been enacted, including preventing proxy attacks and illegal personal data access. Hence, organizations are advised to manage their security framework.

The primary goal of this paper is to discern the effect that virtualization innovations have on the edge/fog network architectures, examining their focal points and featuring the security issues presented by them. In this paper, we utilize the term edge computing to allude to the general architecture, which most of the SDOs allude to as Multi-access Edge Computing or MEC.

Section II includes the architectural prospects of edge computing, followed by discussing six real-life scenarios where edge computing technologies have been employed in Section III. Section IV discusses

security issues and the previously conducted work for ensuring security in edge computing. Section V concludes this paper.

II. ARCHITECTURE

In this section, we delve into the architectural prospects of edge computing. In the edge computing architecture, data is processed either within the device that generates them or in a device located externally but lies at the edge of the same network [13]. Edge computing architectures are broadly perceived as essential to successfully increase the capacities of individual portable devices by providing them with support services that require real-time processing and response systems, such as augmented and virtual reality and speech recognition [14].

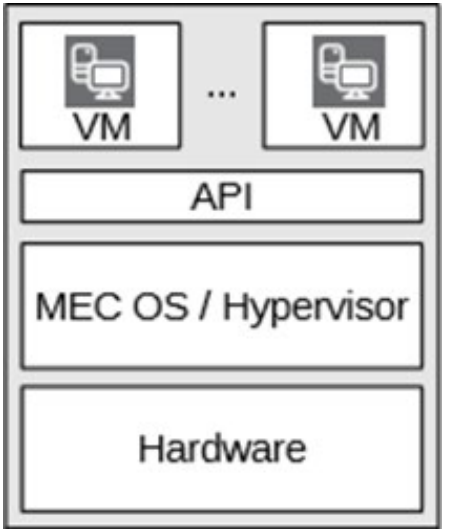

Fig. 3. RACS Architecture [17]

III. USAGE SCENARIOS

This section presents six real-life usage scenarios where edge computing technologies

While to date, there is no standardized definition of edge computing. Consequently, several diverse architectures involving varying technologies and functions have surfaced from time to time. Some features are considered generic and, therefore, necessary for edge computing. Decreased latency, increased battery life of concerned devices, decreased bandwidth costs, and improved security is some of the expectations from a typical edge architecture [15]. However, each architecture caters to a specific problem set, as depicted in Table 1.

Edge computing incorporates three kinds of devices: devices that generate raw data, such as sensors; devices that get processed information, including end-client devices, such as cell phones; and devices that offer computational power or different administrations, such as servers (Caprolu et al., 2019) are employed: cloud gaming and augmented reality, smart homes and cities, e-health, cyber-threat detection in intelligent vehicles, smart

surveillance and smart inventory, and grocery shopping system, respectively. We analyze how edge computing is integrated into the traditional systems for each usage scenario and how it benefits us.

TABLE I. COMPARISON OF EXISTING ARCHITECTURES AND THEIR IMPLEMENTATIONS

Existing Architectures	Description	Issues addressed
Radio Applications Cloud Servers (RACS)	This architecture provides MEC servers and a VM hypervisor (see Fig. 3). The MEC servers are installed right next to the base stations such that they are linked to them directly [16].	Communication delays, bandwidth issues, and scalability.
Scalable Edge computing Services (SEcS)	Based on the Web-Based Intermediaries (WBI) framework, SEcS provides efficient communication via sockets [17].	Scalability, robustness, and fault tolerance.
Multi-access MEC	Multi-access allows data caching and optimized local content distribution [18].	Bandwidth issues and latency.
WiCloud	Based on NFV, WiCloud consists of a layered architecture that provides edge networking [19].	Access to real-time network information, latency.

A. Cloud Gamming and Augmented Reality

Cloud gaming has revolutionized the gaming world by reducing the necessity of a high processing and high power computer or console and by providing the facility of online gaming enabled by a host gaming server giving services to a client. Similarly, Augmented Reality (AR) is another far-reaching technology that allows us to combine the real-world environment with the gaming world. Such technologies require low latency, powerful processors, high bandwidth, and high-speed networks, which is impossible with existing networks and technologies. Moreover, latency is a big problem in the cloud [20] and AR gaming. Consequently, gamers are expected to stop playing a particular game if there is a latency of about 500ms [21]. Fig. 4 below shows how cloud gaming sales will increase in the coming future; hence, the need arises to make it latency-free [22]. Edge computing would allow us to create an infrastructure that provides high-speed computing and processing with reduced lag and

latency, making the gaming experience more comfortable and interactive [23].

Fig. 4. Cloud Computing Market Value

B. Smart home and Cities

Devices for everyday use now require much more compuuttional power and intelligence in today' fast-paced technology orld. Consequently, devices such as the IoT and edge computing devices with a faster response time and more computational ability are being designed and produced. These devices have changed the way our homes and cities work. We have sensors and processors using edge computing in almost every device connected via a network, generating enormous amounts of heterogeneous data. There are models to build smart cities that will make everyday devices bright, giving them the ability to perform computations and store information using edge computing, as shown in Fig. 5. Such models have been incorporated into developed countries' city and urban planning. Examples include smart grids, smart TVs, competent police, smart parking, video surveillance, and environmental monitoring that significantly improve the lives of citizens.

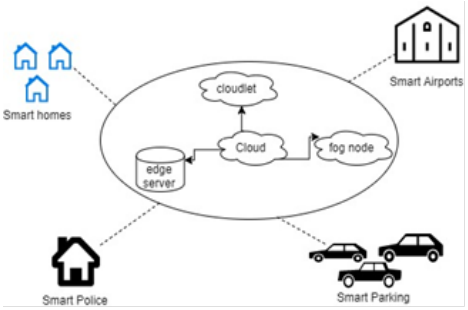

Fig. 5. Smart Homes and Cities using Edge Computing Technology

C. E-Health

The sales of IoT devices providing medical care are likely to increase to 500 billion by 2020 [13]. This illustrates a significant change in the healthcare industry. The cloud is increasingly being replaced by edge technology that performs well without latency, which is crucial in healthcare, where any delay may prove fatal. Doctors can monitor patients with the help of sensors and devices that perform real-time

analysis and generate data, as shown in Fig. 6. Sensors continuously transfer data for analysis to the e-healthcare systems of doctors, who are notified immediately if there appear any threatening changes or unusual patterns in the patient's condition. They are also feasible for individual use, such as monitoring heart rate and blood pressure [13].

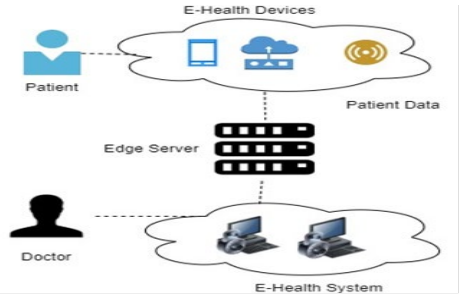

Fig. 6. Connection of E-health Systems and E-Health Devices and Sensors

D. Cyber-Threat Detection in Smart Vehicles

Intelligent vehicles are getting very popular due to their high processing power and faster response times. For the surveillance of intelligent vehicles, we can use a UAV edge. Real-time data can be transferred for analysis using a UAV (Unmanned Aerial Vehicle) as an edge, which acts as an intermediate node between the edge node and the vehicle. Intelligent vehicles and ITS (Information Transport Systems) are a target of choice for cyber-criminals since they lack security due to using an open channel to transfer data between edge and UAV. ITS can be used with a UAV to combat this threat to innovative vehicles by monitoring them in real-time [38].

E. Smart Servelliance

Edge computing can decrease the amount of delay and overhead in systems, including intelligent surveillance that requires real-time decision-making. Video content can be obtained from video sensors and video cameras. The acquired data is vast and needs to be analyzed quickly. This is why edge, combined with Fog and cloud, proves helpful. These cameras can track every move by every object, human being, animal, and anything else that moves. These include real-time analysis of crowds, vehicles, etc. Facial recognition is an excellent example of these surveillance systems [25].

F. Smart Inventory and Grocery Shopping System

Integrated IoT Enabled On-demand Grocery Shopping and Delivery

Cloud (IGSDC) is used to keep track of groceries. When the user runs out of a product, a supplier is chosen, and the product is automatically delivered after purchasing it from the supplier. Suppliers are also connected to the cloud, and they use autonomous robots to deliver their products. Hence, the customers and the suppliers can connect and utilize these systems autonomously [23].

IV. SECURITY ASPECTS

IoT is a vital component that plays an essential role in advancing technology [26]. Edge computing is vital for constructing IoT infrastructure and networks [27]. With these technological advancements come several security issues, as shown in Table 2.

Heterogeneity and the cloud computing environment are distributed in nature and become debatable whenever a user's access control is considered. A user's access controls allow him to perform, control and limit the operations performed by any other user on any system resources [28]. In a cloud environment, users have relatively limited control over a system's resources compared to a non-cloud computing environment. The lack of access control indeed raises security concerns for organizations, making them uncertain about switching to cloud infrastructure [29].

Some of the security issues, trust, and privacy concerns have lately been addressed in several types of research [30]. Recently, specific reports have been published by Vision, which clearly shows companies' reluctance to upgrade their computer-based infrastructure to a cloud computing environment because of security and privacy issues [31].

A recent study conducted by Alert Logic, a software company, stated that hacking attempts on cloud-deployed applications increased by 45% [32].

Furthermore, failures in the cloud environment may lead to substantial losses for organizations. An example of such an attack is given below. In 2010, online customers faced specific issues whilst placing orders using amazon.com, a famous online shopping platform. Due to these issues, amazon.com faced an approximate loss of $1.75 million per hour. Similarly, in 2016, another

incident occurred. Dyn, Inc. faced an attack called "Distributed Denial-of-Service (DDoS)," which impacted several websites. Enterprises depending upon "Software-as-a-Service (SaaS)" for executing their essential business operations experienced critical failures in cloud computing environments. Hence, we can conclude that because of the widespread use of cloud computing infrastructures, hosting any critical services, any potential disruption in the cloud environment will significantly impact an organization's critical services [33]. Thus, in light of technological advancements and, consequently, networking challenges, protection needs are imperative for the cloud environment [34]. Several proposals have been put forth to deal with proxy attacks and illegal personal data access [35].

A. Exposure of Location

The stream of communication required in an advanced computing environment does not isolate the user's identity from the user's location [37]. This allows hackers to target the links carrying critical information, enabling them to identify the location of devices in the network and exploit it [29].

B. Traffic Hacking

Geographical distribution increases in an edge computing environment due to advanced servers and devices. Due to this fact, transferring data, whether encrypted or not, is more prone to hacking and exposure [29]. Whenever hacked, it is conceivable to deceive the device about the information it has gathered, prompting 'awful choices. It can even enable hackers to gain access to the core network. deceive the device about the information it has gathered, prompting 'awful choices. It can even enable hackers to gain access to the core network.

C. Distribution of Virtual Images

In edge computing, virtual images span over long distances [29]. Virtual images are transmitted over links that are public [10]. Hackers can access these links and compromise these images [29].

D. Attacks using Denial of Service (DoS)

Since the location of edge and fog devices can be easily guessed, they are more susceptible to a DoS attack.

E. Jamming of Network

Since the edge computing environment includes extensive use of wireless technology, it is straight forward to jam/overwhelm the network.

F. Privacy

The edge environment connects trusted and non-trusted users with each other. An untrusted user may misuse a wide range of information readily available over the network. Being close to the end clients, Edge nodes can conceivably get vast amounts of sensitive privacy information. If information from an edge node leaks, the outcomes can be devastating. Contrasted with cloud centers, edge devices have restricted assets, so they cannot bolster complex security instruments. Because of the high portability of devices and clients, the MEC environment is continually evolving/evolves continuously. Assailants can, without much of a stretch, join the gathering. Moreover, it is hard to plan security rules with multi-area covering, for example, device provider, information generator, etc.

Since 5G systems offer lower latencies, associations have discovered more approaches to using edge devices. Moreover, the number of these connected devices has been growing exponentially. Most edge
processing is carried out through Application Programming Interfaces APIs. Tragically, over 70 percent of edge devices have no command confirmation for outsider APIs. Furthermore, over 60 percent of edge devices have no encryption of information locally. This absence of control makes these prominent devices targets hackers who can take information straightforwardly from the devices and contaminate them with vindictive code or 'bots.

V. CONCLUSION

Edge computing is an ever-evolving technology. It is being developed and researched continuously. There are many benefits that edge computing provides. However, the issues that arise with its implementation have yet to be dealt with, one of the most important being security threats.Reference

Year	*Topic*	*Initial Architecture*	*Architecture Issue*	*Proposed Architecture*	*Security Issue*	*Proposed Security Solution*
2019	Remote Debugging for Containerized Applications in Edge Computing Environments [29].	The monolithic approach is challenging to implement in the edge computing environment. Thus container-based approach has been used recently.	Containerization is not cost-effective since constant updating of configuration files is required.	Using the remote debugging method (an application), new changes can be checked within the edge computing devices. Microsoft Visual Studio (VS) 2017 IDE provides services for remote debugging.	Secure debugging of applications.	Security is assured by forming an encrypted connection to edge computing devices.
2019	Secure Desktop Computing in the Cloud [28].	Virtual Desktop Infrastructure (VDI) for web desktop applications.	A complete guest Virtual Machine (VM) is visible to the user.	Venia is a cloud-computing environment created to secure desktop-based applications against threats.	When computational resources are shared in the cloud-based environment, new security issues occur from both external and internal ends.	Venia segregates users' data and applications into containers and applies specific security policies regarding data sharing among containers. It also collects thorough logs for auditing purposes.
2019	A Strong Authentication	A method based on 1-factor	The intensity of attacks has	Authentication using smartphone	It is easy to hack.	Twice as much security by one-

Year	*Topic*	*Initial Architecture*	*Architecture Issue*	*Proposed Architecture*	*Security Issue*	*Proposed Security Solution*
	Method for Web Mobile Services [30].	authentication has security and privacy issues.	made it necessary to introduce multiple levels of authentication to increase security and reduce attacks.	and IoT devices is connected to the same network to reduce security breaches.	Therefore, it faces privacy and security challenges. High volumes of data make it difficult to monitor.	time password OTP-based 2-factor authentication, which gives a small code for the users to verify.
2019	SeCoNetBench: A modular framework for Secure Container Networking Benchmarks [33].	Container network security.	No security benchmarks.	SeCoNetBench is a platform for modular benchmarking container network security.	Lack of efficient security protocols.	IPsec, WireGuard (wg) as VPNs.
2019	Research on Improving Network Security of Embedded Systems (Shirazi et al., 2017).	Simple network security architecture does not have high levels of protection.	Limitations in system processing and remoteness between embedded systems and networking devices.	Extends the Design of the security network following OSI/RM.	A variety of hacking attempts and network attacks on the system.	Use of Privileged Access Management (PAM) framework by using a vault to secure credentials.

Year	*Topic*	*Initial Architecture*	*Architecture Issue*	*Proposed Architecture*	*Security Issue*	*Proposed Security Solution*
2017	Location Privacy in Mobile Edge Clouds (Yousefpour et al., 2019).	Simple MEC architecture.	Co-location of a user and his service in MEC.	Introducing chaffs.	Cyber eavesdropping.	Chaffs mimic absolute service while trying not to co-locate with the genuine service as much as possible.
2016	PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services (M. U. Sattar et al., 2020).	Computing environment without cryptology.	No secure method to access services.	PRISMACOLOR	Several security and privacy issues for end-users, including lack of encryption of sensitive information.	Introduce cryptography to enable end-to-end security, preserving the service's privacy and securing the end-users.

Table.II. ARCHITECTURES AND THEIR SECURITY ISSUES

This paper briefly discusses the reasons behind the transition from cloud to fog computing and then to edge computing. We looked into the existing architectures of edge computing to have a broader picture of how edge computing is implemented to cater to specific problems in specific circumstances. Some of the numerous applications of edge computing were also discussed. Finally, we shed light on the possible security threats that emerge with the use of edge computing.

Reference

1. Rao, B.T," A study on data storage security issues in cloud computing." Procedia Computer Science, vol. 92, pp.128-135, 2016.
2. Megantoro, P., Husnan, D.A., Sattar, M.U., Maseleno, A. and Tanane, O," Validation Method for Digital Flow Meter for Fuel Vendors." Journal of Robotics and Control (JRC), vol. 1, no. 2, pp.44-48, 2020.
3. Popović, K. and Hocenski, Ž,", May. Cloud computing security issues and challenges." In The 33rd international convention mipro , (pp. 344-349), 2010.
4. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S," Fog computing and its role in the internet of things." MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop, pp. 13–15, 2012.
6. Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Aktas, E., Bourlakis, M., & Zissis, D" Collaboration in the last mile: evidence from grocery deliveries." International Journal of Logistics Research and Applications, vol. 24, no. 3, 227–241, 2021.
7. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L,"Edge Computing: Vision and Challenges." IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

   [8] Apsari, N. F., Megantoro, P., Sattar, M. U., Maseleno, A., & Tanane, O," Design of laboratory scale fluid level measurement device based on arduino." Journal of Robotics and Control (JRC), vol. 1, no. 5, pp. 145–149, 2020.
9. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B," A

Survey on Mobile Edge Computing: The Communication Perspective." IEEE Communications Surveys and Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.

10. Sanchez-Gallegos, D. D., Galaviz-Mosqueda, A., Gonzalez-Compean, J. L., Villarreal-Reyes, S., Perez-Ramos, A. E., Carrizales-Espinoza, D., & Carretero, J," On the Continuous Processing of Health Data in Edge-Fog-Cloud Computing by Using Micro/Nanoservice Composition." IEEE Access, vol. 8, pp. 120255–120281, 2010.
11. 1Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G., & Sun, L," Fog Computing: Focusing on Mobile Users at the Edge.", pp. 1–11, 2015.
12. Zhang, Jiale, Chen, B., Zhao, Y., Cheng, X., & Hu, F," Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues." IEEE Access, vol. 6, pp. 18209–18237, 2018.
13. Caprolu, M., Di Pietro, R., Lombardi, F., & Raponi, S," Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues. Proceedings - 2019 IEEE International Conference on Edge Computing, EDGE 2019 - Part of the 2019 IEEE World" Congress on Services, pp. 116–123, 2019.
14. Cases, U," Edge-Oriented Computing A Survey on Research and Use Cases.", vol. 15, no. 2, pp. 1–28, 2022.
15. Zahid, Z., Sattar, M. U., Khan, H. W., Zahid, A., & Riaz, M. F, " A Smart Analysis and Visualization of the Power Forecasting in Pakistan.",vol. 10, 2021.
16. Beck, M. T., Werner, M., Feld, S., & Schimper, T," Mobile Edge Computing," A Taxonomy. Proc. of the Sixth International Conference on Advances in Future Internet, pp. 48–54, 2014.
17. Grieco, R., Malandrino, D., & Scarano, V," A scalable cluster-based infrastructure for edge-computing services." World Wide Web, vol. 9, no. 3, pp. 317–341, 2006.
18. Qian, Y," Unmanned Aerial Vehicles and Multi-Access Edge Computing." IEEE Wireless

Communications, vol. 28, no. 5, pp. 2–3, 2021.

19. Ferrer, A. J., Marquès, J. M., & Jorba, J," Towards the decentralised cloud: Survey on approaches andchallenges for mobile, ad hoc, and edge computing." ACM Computing Surveys, vol. 51, no. 36, pp. 1–36, 2019.
20. Ghani, F., Sattar, U., Narmeen, M., Wazir Khan, H., & Mehmood, A," A Methodology for Glaucoma Disease Detection Using Deep Learning Techniques." International Journal of Computing and Digital System, pp. 1–11, 2021.
21. Pottie-Sherman, Y., & Lynch, N, " Gaming on the edge: Mobile labour and global talent in Atlantic Canada's video game industry." Canadian Geographer, vol. 63, no. 3, pp. 425–439, 2019.
22. Cai, W., Leung, V. C. M., & Hu, L," A cloudlet-assisted multiplayer cloud gaming system. Mobile Networks and Applications." vol. 19, no. 2, pp. 144–152, 2014.
23. Aktas, E., Bourlakis, M., & Zissis, D," Collaboration in the last mile: evidence from grocery deliveries." International Journal of Logistics Research and Applications, vol. 24, no. 3, pp. 227–241, 2021.
24. Braud, T., Alhilal, A. and Hui, P," December. Talaria: in-engine synchronisation for seamless migration of mobile edge gaming instances." In Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies, pp. 375-381, 2021.
25. Nikouei, S. Y., Chen, Y., Song, S., Xu, R., Choi, B. Y., & Faughnan, T. R," Real-time human detection as an edge service enabled by a lightweight CNN.", Proceedings - 2018 IEEE International Conference on Edge Computing, pp. 125–129, 2018.
26. U.Farooq, M., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T," A Review on Internet of Things (IoT).", International Journal of Computer Applications, vol. 113, no. 1, pp. 1–7, 2015.
27. Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z, " Towards smart home automation using iot-enabled edge-

computing paradigm.", Sensors, vol. 21, no. 14, 2021.

28. Dsouza, C., Ahn, G. J., & Taguinod, M," Policy-driven security management for fog computing: Preliminary framework and a case study.", Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration, vol. 21, no. 14, pp. 16–23, 2014.
29. Shirazi, S. N., Gouglidis, A., Farshad, A., & Hutchison, D," The extended cloud: Review and analysis of mobile edge computing and Fog from a security and resilience perspective.", IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, 2017.
30. Solangi, Z. A., Solangi, Y. A., Chandio, S., Aziz, M. B. S. A., Bin Hamzah, M. S., & Shah, A, " The future of data privacy and security concerns in Internet of Things." 2018 IEEE International Conference on Innovative Research and Development, pp. 1–4, 2018.
31. Sattar, M., Palaniappan, S., Lokman, A., Shah, N., Riaz, Z., & Khalid, U, " User experience design in virtual reality medical training application.", Journal of the Pakistan Medical Association, 2019, pp. 1.
32. Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H, "Internet of Cloud: Security and Privacy Issues.", pp.271–301, 2018.
33. Mendes, R., Oliveira, T., Cogo, V., Neves, N., & Bessani, A," Charon: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data." IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1349–1361, 2019.
34. Yi, S., Hao, Z., Qin, Z., & Li, Q," Fog computing: Platform and applications." Proceedings - 3rd Workshop on Hot Topics in Web Systems and Technologies, pp. 73–78, 2016.
35. da Costa, K. A. P., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C," Internet of Things: A survey on machine learning-based intrusion detection approaches.", Computer Networks, vol. 151, pp. 147–157.

36. Pfitzmann, A., & Kiel, U. L. D," Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology.", pp. 1–83, 2008.
37. Rodriguez, M," All Your IP Are Belong to Us." Texas A&M Law Review, vol. 3, pp. 663–689, 2015.
38. Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi, E," Digitalization and its influence on business model innovation." Journal of Manufacturing Technology Management, pp. 1143–1160, 2019.
Refrence numbers [39], [40], [41] are missing in intext citations
39. Zhang, Jing, Li, D., Hua, Q., Qi, X., Wen, Z., & Myint, S. H, " 3D Remote Healthcare for Noisy CT Images in the Internet of Things Using Edge Computing." IEEE Access, pp. 15170–15180, 2021.
40. Apsari, N. F., Megantoro, P., Sattar, M. U., Maseleno, A., & Tanane, O," Design of laboratory scale fluid level measurement device based on arduino.", Journal of Robotics and Control (JRC), vol. 1, no. 5, pp. 145–149, 2022.
41. Zhou, X., Ke, R., Yang, H., & Liu, C," When intelligent transportation systems sensing meets edge computing: Vision and challenges.", Applied Sciences (Switzerland), vol. 11, no. 20, pp. 9680, 2021.