VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2021, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 9, Number 4, October-December 2021 *pp: 68-81*

A Survey on Fog computing in IoT

Mansoor Ahmad Rasheed*, Jabar Saleem, Hudabia Murtaza, Hafiz Abdullah Tanweer, Mannan Ahmad Rasheed & Mishaal Ahmed

University of Management and Technology, Lahore Pakistan
*Corresponding author email address: S2020114015@umt.edu.pk, mansoorahmadrasheed@gmail.com

ABSTRACT
Technological advancements in computing and wireless handheld devices have increased tremendously the rate of connected devices to the internet. To solve problems of our daily life are being controlled by these devices that created a new approach called as Internet of things. Cloud computing is a promising solution to store data and perform computations for IoT. But it has many issues like latency, traffic congestion, and poor quality of services. Health-related IoT applications are intolerant to delay or poor quality of service. To tackle these issues a new model of computing known as fog computing came into existence. Fog computing helps for effective communication and processing of the massive data that tackles issues caused by cloud computing in a significant way. This study discusses different types of fog computing architectures, some of the issues related to security and privacy along with their possible solutions. In this survey, some practical applications of fog computing in IoT are discussed which can ease our daily problems.

KEYWORDS
Fog Computing in IoT, Cloud computing in IoT, Edge computing, IoT applications, survey.

JOURNAL INFO
HISTORY: Received: October 11, 2021 Accepted: December 15, 2021 Published: December 31, 2021

I. INTRODUCTION

The growth of the internet and advancement in network architecture along with smartphones gave a new direction to solve many problems in our daily life and thus Internet of thing also known as IoT came into existence. The concept of IoT has tremendously changed the perception of the industry to solve daily life issues smartly. Today, we can see many IoT-enabled devices are available which include smartwatches, smart door locks, Nest Smoke Alarm, and much more. Soon in near future, we will see the self-driving car and the phenomenon of the internet of the vehicle will be no longer be a dream. Similarly, if we look at other domains, we will find IoT as a promising solution in our daily life such as smart cities, e-health, industrial automation disaster management, etc. The world's population approximately is around 7.6 billion-plus and it is anticipated that by the year 2030 the aggregate of IoT devices as per Cisco would be 500 billion**Error! Reference source not found.**.

It means a massive amount of data and computations are being performed by IoT devices. To handle such massive data efficiently is a big challenge. Undoubtedly, cloud computing is a great solution to tackle this issue but these data centers are distributed all over the world and are scarce to have or very little in number per country. Hence, the round time latency time of the cloud is O(100)ms[1]. Some IoT-based applications are intolerant to delay, some applications need to compute using their system and some might generate a very large amount of data which could cause a bigger load on the network. In such a case, if we only rely on cloud computing then decision-making via the cloud would be compromised and also would result in poor performance. [2], [4] Also, cloud computing has other issues such as high latency, mobility, and geographic coverage. But on the other hand, IoT applications demand low latency, mobility, and real-time analytics, and geographic coverage. Thus we need a co-process that can take care of these issues. This debate led to give birth of the new paradigm that is known as Fog Computing as introduced by the CISCO.[4] [5]

In our real life, we can see that in winters fog is closer to the earth as compared to clouds. This is the same analogy that works for IoT-based applications. Instead of that, we use the cloud as our primary source of computation and storage we use fog computing that is a middle layer and is more near to IoT devices [5].

The decentralized Infrastructure of fog computing provides numerous services which include storage, process operations, and interconnection of resources. One fog node uses by one or more IoT devices to perform substantial communication, storage, control and is thus easy to manage. As fog nodes are nearby so there is less burden on the network to process the requests as compared to cloud computing. Furthermore, fog computing increases the quality of service to the end-users as it provides low latency, quick response, and geographic coverage.

As we know fog computing is a new paradigm and it is not inevitable to have some issues. We need to know what type of architecture is the most suitable for IoT devices for optimized computation, storage, and communication. On the other hand, we need to make sure that the fog layer is as secure and private as a cloud. As it is a middle layer so it is more likely prone to attack and hence security risks are higher. There are different service providers and their core business

is to implement fog computing. This could result in less trust and IoT-based devices might be vulnerable to attack easily. Fog computing brings new challenges in terms of security and privacy. In this study, we contributed to knowing about fog computing fundamentals, its different architectures, security and privacy issues along with their practical applications in our real world.

The rest of the paper is divided into five main sections. Section II explains detailed fundamentals to understand the rest of the paper. Section III enlightens on the literature review. Section IV describes a methodology to research along with research questions. Section V discusses our research questions.

II. BACKGROUND

To know in-depth the best architecture of fog computing for IoT we need to understand the complete picture of fog computing. So, we started with features of fog computing and then a compressive difference between fog computing, edge computing, and cloud computing.

A: MAIN FEATURES OF FOG COMPUTING

Fog Consortium addressed Scale (Security, cognition, agility, latency, efficiency) as capabilities of Fog computing[5]. There are 24 regions and 76 zones around the world where AWS operates[6]. Google has 22 regions and 61(Q1 2020) zones around the globe [7]. But usually, these cloud data centers are geographically very far from each other which results in a long round trip, network congestion, and Qos degradation from the EU's point of view. On the other hand, edge nodes are a better option than cloud to reduce the network burden and supports delay-sensitive tasks as shown in Figure 1.

- Security: Provide security to clients' data.
- Cognition: Reduce traffic congestion.
- Agility: Applications are scalable depending
- upon the architecture.
- Latency: Fast real-time access.
- Efficiency: More efficient than cloud computing.

Figure 1: Fog Computing Model [9]

B: BASIC MODEL OF FOG COMPUTING

Fog nodes are formed at the edge of the network by a lot of geographically distributed devices such as EUs, routers, switches, and access points or virtual machines and cloudlets[9],[3]. To download or upload data to the core of the network is a typical process in cloud computing instead of that all these devices obtain data from the nearby devices and small networks using a direct communication link called device to device (D2D) [10],[11].Also, fog nodes have some storage and computing capabilities to support the demand of the devices in their proximity. So, it reduces the networking cost and computing load on the cloud. Only necessary data will be transferred to the cloud which will not be handled by the fog nodes. Moreover, if the data of the group of edge devices is too tied up with each other then a common traffic mechanism is used to send data to the cloud via a single edge entity. Likewise, the cloud sends data to one entity in the group which results to reduce traffic congestion. As mentioned in **Error! Reference source not found.**[13], the contents of the popular tasks are pre-fetched by the cache-enabled network. Thus resulting in low latency.

C: DIFFERENCE BETWEEN EDGE COMPUTING, CLOUD COMPUTING, AND FOG COMPUTING.

We can see that the fog layer resides between edge devices and the cloud many features resemble so it is a good idea before we proceed further let's see are different aspects of fog computing concerning edge computing and cloud computing. The following Table 1 **Error! Reference source not found.** briefly explains the differences between cloud, fog, and edge computing. Fog layer has higher computation capacity than edge computing but not more than cloud [4].

III. RELATED WORK

Many researchers have discussed the potential of fog computing in IoT which belongs to different domains such as smart cities, the internet of vehicles, smart grids, smart health systems, and industrial automation. [15]I. Stojmenovic and S.Wen discussed the advantages of fog computing along with security, privacy, and trust issues. But this survey was limited concerning the architecture of fog computing. Shanhe Yi [14] explained different issues regarding fog computing such as interconnection with devices, trust in fog nodes, and delay in fog computing.This survey [15]was based mainly on issues. Similarly, [17] K.P.Saharan discussed fog computing as another type of cloud computing.

Furthermore, Chiang [17] explained how fog computing is an effective solution for IoT-related research challenges. In 2017, [18] explained an IoT-based infrastructure for smart cities by using data analytics with the help of fog and cloud computing.

Table 1: Difference between Cloud, fog, and edge computing

Features	Cloud computing	Fog computing	Edge Computing
Computing Model	Centralized	Distributed as well as Centralized	Distributed
Data Storage Capacity	Very High	Intermediate	Low
Caching capacity	Very High	High	Low
Latency	High	Low	Very Low
Mobility	Very Hard	Easy	Very Easy
Computation Capacity	Very High	High	Low
Size	Very Large	Large	small
Access	Global	Global as well as restricted depending on the application model.	Restricted

In this same year [19] focused on security and privacy issues. In another [20] Carla et al IoT and CDN(content delivery network) and explained both of them as a driving force to the emergence of fog computing. Mahmud et al.[21] elaborated a detailed taxonomy of fog computing and its features. But resources allocation, service management, latency issues, and caching issues were missing.

In 2019[22] Sravani Ganesh et al discussed potential issues of IoT and their solution via fog computing. In this survey security and privacy issues were mainly discussed. Fog computing has emerged to meet the needs of IoT applications that are currently unmet by current technologies. Various strategies have been proposed to promote fog development, and significant work has been done to improve specific areas. However, a thorough examination of the various options is still required, with details on how they might be combined and applied to satisfy specific requirements. By evaluating a wide number of solutions, we provide a unified architectural paradigm and a new taxonomy in this paper. Finally, we draw some findings and recommendations for the development of fog-based IoT applications[80]. Industrial contexts are a prominent application of the Internet of Things (IoT) paradigm. Indeed, the burgeoning Industrial Internet of Things (IIoT), also known as Industry 4.0, promises to transform production and manufacturing by combining massive numbers of networked embedded sensing devices with new computer technologies like fog/cloud computing and artificial intelligence. The IIoT is defined by a higher level of interconnectivity, which presents potential for both industries that adopt it and cyber-criminals. Indeed, IoT security is now one of the most significant impediments to the mainstream deployment of IIoT technology[81]. Fog computing was developed to address the needs of delay applications such as augmented reality and the Internet of Things (IoT), which generate large amounts of data that are difficult to send to cloud data centres for processing[82]. The numbers of Internet of Things (IoT) connected nodes and gadgets in our daily lives has drastically expanded in recent years. As the number of devices has expanded, fog computing has become a well-established model for maximising various essential Quality of Service (QoS) characteristics such as latency, bandwidth constraint, reaction time, scalability, privacy, and security[83]. The latest developments in information and communication technology have had a considerable impact on distributed systems in the last 10 years, giving rise to models like Cloud Computing, Fog Computing, and the Internet of Things (IoT). In the vast majority of situations, the settings they constructed are closely linked: Sensors and devices connected to the internet of things generate data that must be saved, processed, and analysed by cloud or fog services, depending on the application requirements[83].

Most of the surveys discussed the potential need for fog computing for IoT and focused on issues. While in this survey we will discuss different architectures, privacy, and security issues along with the application of fog computing.

IV.METHODOLOGY

The systematic review is conducted by following the framework used in[Error! Reference source not found.][[73]][[74]][[75]]. Once we have finalized our research questions we defined some rules to minimize biases in our research study. These rules are mentioned below:

1. Inclusion and exclusion criteria.
2. The scientific libraries to get relevant data.
3. To formulate search queries.
4. Screening the data in chronological order, analysis of the data, data extraction, and methods for data selection.

RESEARCH QUESTIONS

The most important task was to define research questions and their motivation for fog computing in IoT. The **Table 2** shows these questions along with their motivation.

Table 2:These questions, as well as their motivation, ae listed

Research Questions	Motivation
Q1: What are the different architectures of fog computing and the best architecture that supports IoT devices with optimized results?	This will provide us an insight into the different architectures of fog computing and enable us to choose the best architecture for IoT devices with optimum output.
Q2: What are the security and privacy issues which are associated with fog computing?	IoT devices are vulnerable easily so it is important to study possible security and privacy issue to provide some solution to avoid such threats.
Q3: What are the different applications of fog computing in IoT?	To get the practical approach of fog computing in IoT.

INCLUSION AND EXCLUSION CRITERIA

In this survey, a mixed research design approach is used that is an amalgamation of qualitative and quantitative. The following criteria are maintained to conduct this survey.

1. It explained the architecture of fog computing concerning IoT.
2. It discussed the security and privacy issues of fog computing for IoT.
3. The search is related to fog computing for any area of the internet of things e.g. internet of vehicles, smart cities, etc.
4. The articles must be published from 2013 till 2020.
5. The article must have at least 20 citations if 20 citations are not available then it must be published between 2019 and 2020.
6. A study is not part of the research if it met the following exclusion criteria.
7. The article only discussed fog computing and does not include IoT.
8. It focuses on cloud computing and IoT.
9. If an article discussed security and privacy issues for one particular aspect either fog computing or the Internet of things

Table 3: search strategies

Databases	Search Query
ACM	(“Fog computing” AND “internet of things”)OR (“Security issues” AND “ Privacy Issues fog computing” AND “IOT”)
IEEE Xplore	(“Internet of things” OR “security issues In fog computing”) AND (“Architecture of fog computing “OR “IOT”)
Springer	“Fog computing in IoT” AND (“Security” OR “Privacy issues of fog computing in IoT”)
Research Gates	(“Latency issues” OR “internet of things”)AND(“Challenges of Fog Computing” AND “IOT”)
Direct Science.	(“internet of things”) AND (“fog computing”) OR (“Security issues” AND “fog computing” AND “IOT”)

SEARCH STRATEGY

Our next step was to search the relevant articles and for this purpose, only electronic searches were performed by using 5 scientific databases such as ACM, IEEE Xplore, Springer, Research Gates, and DirectScience. The date of the last search is April 2020. The search string is designed to find relevant articles.

The following Table 3 [2] shows search queries formulated for 5 databases.

STUDY SELECTION

Once all articles were found then those articles were entered in Mendeley i.e. a reference management tool. It was helpful to remove duplication and further screening of the articles was based on inclusion and exclusion criteria.

DATA EXTRACTION

Data is extracted from the search by using a data extraction form as mentioned in Table 4 below [3].

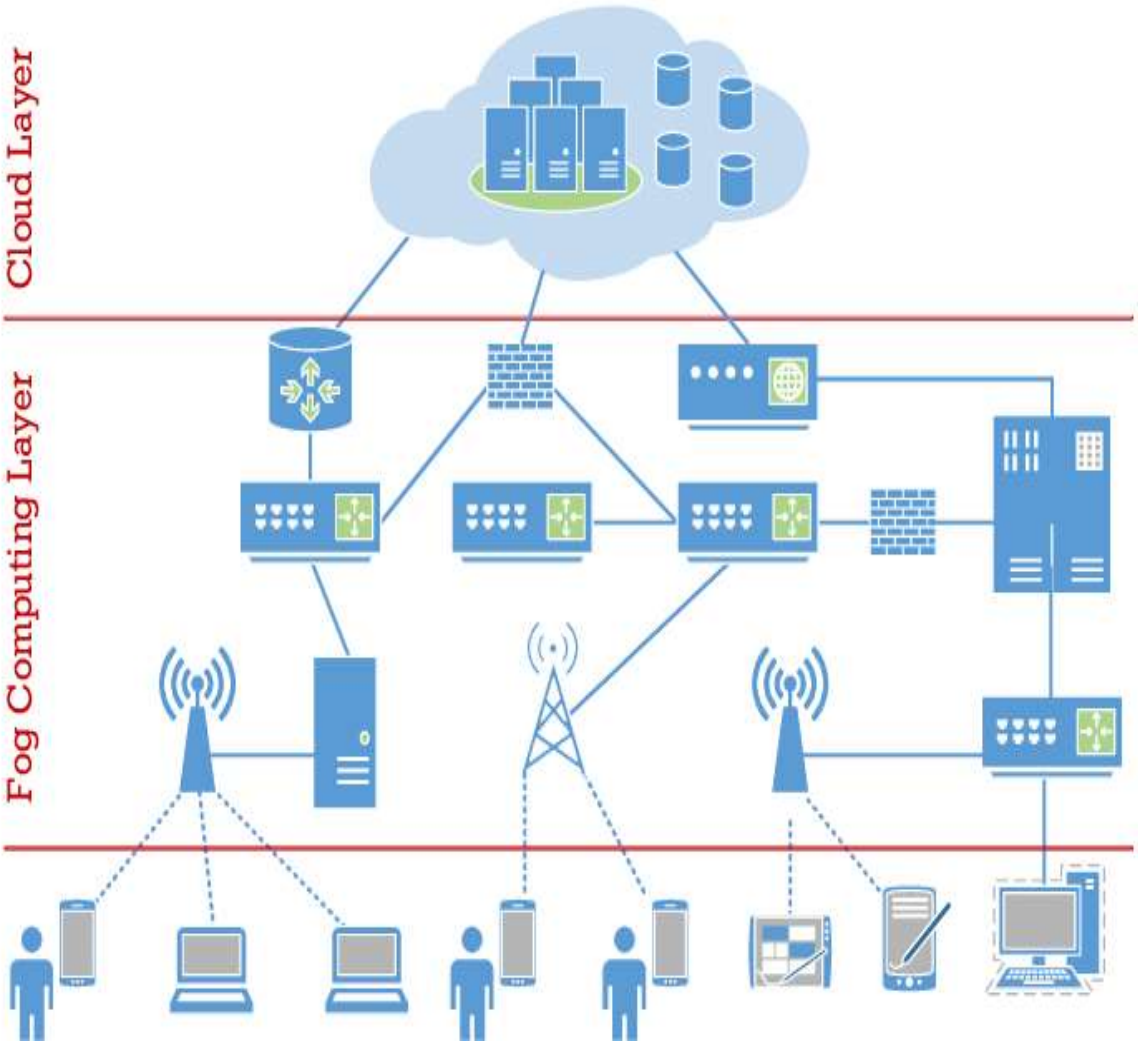

Figure 2: FOG SDN 1

Table 4: Data Extraction Form

Data Items	Description
Reference	Title, author
Goal	The goal of the article is defined by the author.
Approach	The architecture of Fog computing In IoT, applications in real life and their issues.
Publication Type	The article is published in a journal, conference, or workshop.
Year	Year in which that article is published and it must be after 2013.
Publication Channel	Through which publication channel it is published.
Novelty	What is contributed by the author in a specific article?

QUALITY ASSESSMENT

The quality of an article is assessed based on several citations. Any article is considered of good quality if the number of citations is not less than 50.

RESULTS

After performing quality assessment our next step was to synthesis the articles and the key point for synthesis was the same as mentioned in the research question. After doing this synthesis 40 articles were selected out of 100 which we found more relevant for our research.

V. DISCUSSION

RQ1: What are the different architectures of fog computing and will find the best architecture that supports IoT devices with optimized results?

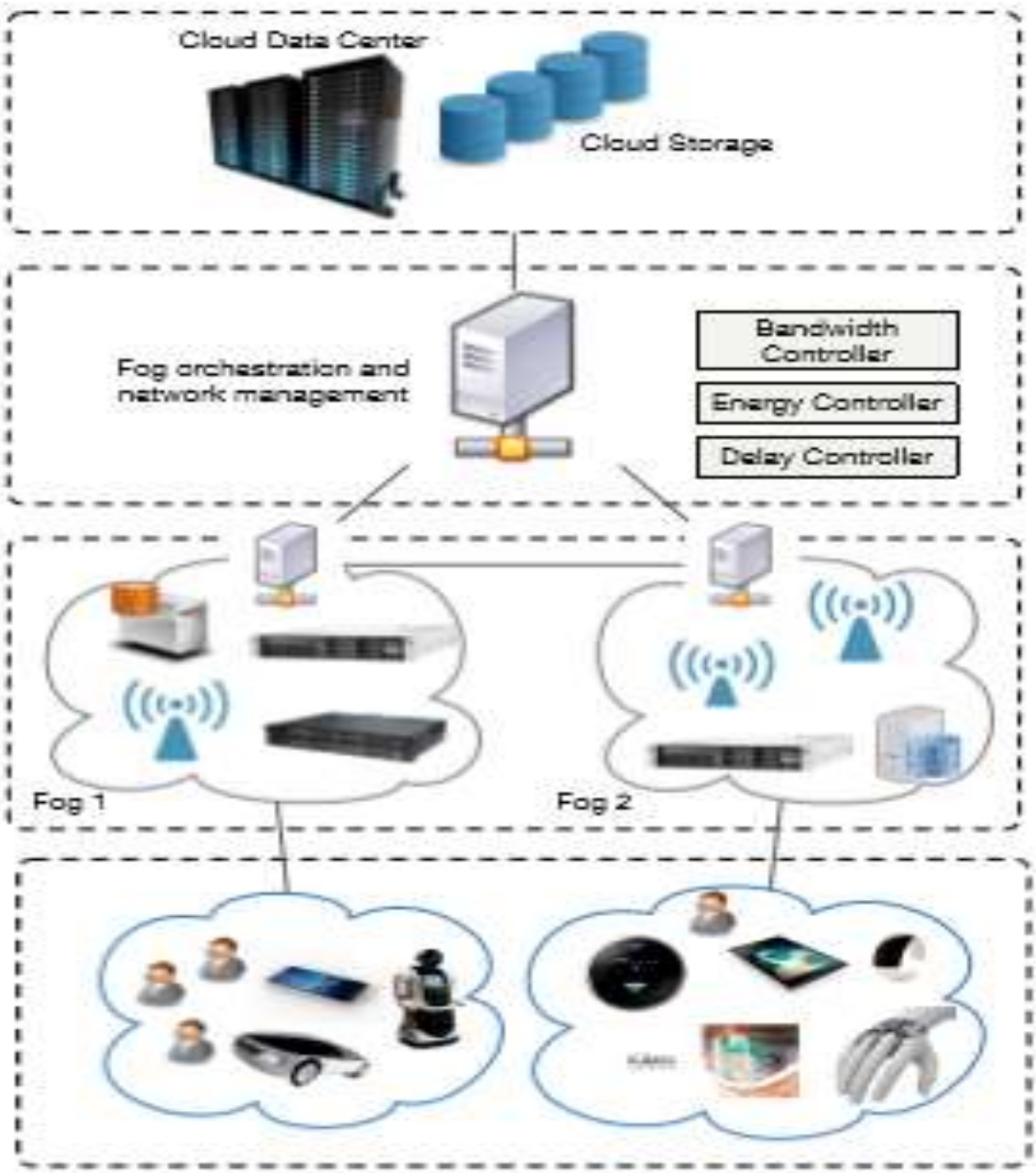

Figure 3: Three-Tier Architecture

To get a better picture of fog computing how it computes, store, and provide quality service at the edge of the network, we will discuss hierarchal architecture, software-defined fog architecture, and radio access network. The basic architecture is 3 tier.

- Tier1: Terminal Nodes: This layer includes all IoT enables devices, handheld devices, mobiles, tablets, wearables, smart cars, etc. All these devices have GPS. They are also called Terminal nodes (TN's).
- Tier2: This layer has all switches, routers, and access points. Also, called fog nodes which have a smaller capacity to store and compute.
- Tier3: It is the topmost layer that has the cloud and data centers with adequate storage and computing capacity. Figure 2 represents 3 tier architecture.

There are also other layers as described by Aazam and Hu named as the virtual and physical layer, monitoring layer, preprocessing layer, temporary storage layer security layer, and transport layer[24]. Table 5 [5] reflects the other additional layers. We already know that fog nodes reduce the time delay to the requests of the EU.

But if there is a request that has some delay constraints then how to handle such requests of us. To tackle this issue [25] Souza et al. purposed another architecture.

- The bottom layer consists of TN's as in a basic architecture that sends requests.
- It contains the first fog-type fog nodes which are low in capacity and directly connected to the TN's with a single hop. That's how it handles delay constraints EU requests. So, it is a good architecture of fog computing for IoT devices that are intolerant to high latency.
- After this, we have a second type of fog node which has fixed nodes. These nodes entertain a medium number of service requests.
- The term "cloud radio access network" (C-RAN) refers to the use of cloud computing to visualise base station functions. This leads in a unique cellular design in
- which a reconfigurable centralised "cloud," or central, unit manages low-cost wireless access points known as radio units or remote radio heads. C-RAN enables operators to save money on the capital and operational costs of deploying and maintaining dense heterogeneous networks.
- The last layer is the cloud layer which has sufficient storage and computing capacity at a higher latency for EUs[26].

Due to the visualization of baseband processing of Remote Radio Heads at a centralized processor the information rate transmitted over a given bandwidth can be improved in Cloud Radio Access Network (C-RAN) because inference management is more efficient[26]. However, F-RAN (Fog Radio Access Network) Boosts a C-RAN by approving RRHs called errors which have to cache and signal processing capacity[46][47][48]. Traffic overhead and latency can be reduced by using a local cache to the errors in F-RANs. All frequently used files can be fetched from errors instead of centralized as shown in figure 3 processor by a frontal. In a hybrid model of H-CRAN (heterogeneous-CRAN) and FogNet, the data can be retrieved in three ways.

- From the users.
- From the cloud network.
- Cached at baseband signal processing unit.

FOG COMPUTING SOFTWARE-DEFINED NETWORK

SDN is a useful way for the configuration and updating of the network[27][43][44][45]. The key feature of SDN is the

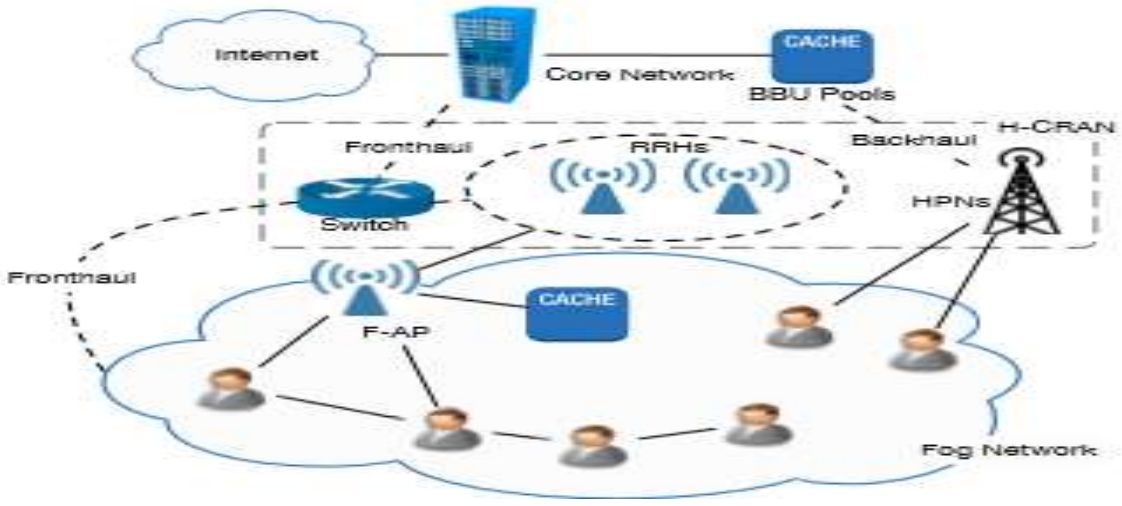

Figure 4: Fog Radio Network

Table 5: Additional Layers

Layered Architecture	
Transport layer	Transfer data to the cloud.
Security layer	Provides security and handles all security issues.
Temporary storage layer	Used to store data temporarily.
Preprocessing layer	This layer helps in preprocessing of data.
Monitoring layer	It monitors and handles requested tasks and also the energy consumption of the underlying physical device.
Physical and Virtual layer	Consists of TN's and other sensor nodes.

physical separation of the control layer and data plane. The senor-nodes do not participate in decision-making for a task rather they are being controlled by the instruction of the centralized controller. Thus we can reprogram easily these sensor nodes without making major hardware changes. SDN controllers are connected to routers by TCP connection. These controllers operate network functions and data forwarding tasks[28]. The limitation of SDN is the delay between routers and the controller. One solution to this problem is to use one controller for one network which will result in increased cost. Although we know fog computing supports latency-sensitive tasks, it could be possible that all the available as As shown in figure 4, resources would not be enough due to the diverse and dynamic infrastructure and mobility issues of TN's.A good idea to handle this issue is to perform some latency-aware tasks by cloud if there are not adequate resources available in the fog layer. SDN has complete knowledge of the states of the network thus enables for the distribution of latency-aware fog tasks.Fog computing can reduce the burden of SDN controllers for computation and transmission.The basic difference between fog-based SDN and 3 tier architecture is that the fog-SDN controller supports dynamic QoS.

RQ2: What are the security and privacy issue which are associated with fog computing?

There are many challenges for fog computing to provide privacy and security to TN's. Here, we will discuss some of the challenges and their solutions to make fog computing more reliable and secure for TN's.

1. IDENTITY AUTHENTICATION:

As we know fog, the cloud is a service provider to the TN's and they consume and provide different services in different domains respectively so, this returns many security hurdles for service providers and the users because it is difficult to ensure that all the bodies are trusted worthy. User authentication is a key to make sure authenticity of the user before accessing the services. Without any proper security Measures, an external attacker can make their target achieve their goals easily by manipulating the resources and infrastructure. So, there is a need for secured techniques for identity authentication.

Although many authentication mechanisms have been introduced to enhance IoT services and provide secured fog-based frameworks[28]. But these procedures do not support the mobility of IoT devices. As a user moves from one place to another with so they connect many different fog nodes for services but there will always be delays to provide service because the authentication process at each fog node will result in high latency.

SOLUTION

To overcome authenticity issues cooperative authentication schemes can reduce authentication overhead**Error! Reference source not found.**. On the other hand, it might possible that users of TN's do not want to expose their location or identity. In such cases, anonymous authentication plays its role in the authenticity of the user e.g. pseudonyms or short signatures **Error! Reference source not found.**.

2. LIGHTWEIGHT PROTOCOL DESIGN

In fog computing fog devices interacts with IoT devices by using hops which makes real-time services suitable. The latency depends on the delay of processing nodes, range, and bandwidth. Due to low computation apacity if fog nodes have to perform complex computation for a user the response time will be very large. To protect users' data and offer reliable services a variety of security protocols should be implemented on the fog node. If these deployed protocols are not effective enough then will not only increase the response delay but will also a large number of computational resources.

Solution: For providing real-time services using fog computation with limited computation capabilities lightweight security protocols are very essential to design to support real-time services for fog-assisted IoT devices.

3. INTRUSION DETECTION:

In fog computing nasty internal or external attackers can attack anyone whenever they want. If the attack is successful it may result in a slowdown of the services etc. This can happen when there is no proper intrusion detection system is deployed to discover these malicious activities. So, there must be a defense mechanism available to protect the whole architecture of fog computing. These detection systems are implemented in the cloud but unfortunately are not available in fog computing.

SOLUTION

The intrusion detection systems might be implemented in fog computing to detect malicious activities [65][66]. But it is not an easy solution as we know fog computing is decentralized. As a fog node can provide services to users locally and as collective as globally so there should be defense mechanisms available to handle both local and global intrusions[67][68].

4. DATA SENSITIVITY DETECTION AND PROTECTION:

In IoT applications, the collected data contains information from different resources[48][50][51]. Some data is considered sensitive data. So, there is a need for the nodes to identify the sensitive data from the collected volume of data before uploading it over the cloud to keep the sensitive data safe and protected. But it is difficult to identify the sensitive data from a large volume because in some cases it be no sensitive data but in some cases, it may be sensitive.

SOLUTION

The first solution is that we can perform some encrypting algorithm on the whole data collected regardless of its sensitivity. But this will add up another extra cost to IoT devices and communication channels. It is a good approach to detect some sensitive data before we process it depending upon the application for which we are using fog computing. It will be helpful to minimize data leakage[52][53][54].

5. **UPDATING IOT DEVICES**

Unfortunately, many IoT devices are still vulnerable to attacks and there is a need for remote software update capabilities to handle security updates[40][41][42]. Vulnerable firmware can leave devices open for attack.

Solution: Updating the billions of devices is a massive task but the geo-distribution characteristic of fog computing can help to supply the IoT device with necessary updates to keep them safe and secure[55][56][57].

6. VERIFIABLE COMPUTATIONS

Fog performs computation to reduce to load to cloud for computations in a distributed way. But there is no such mechanism available to verify if the result computed by the fog nodes is correct or not[62][63]. Normally a user uploads data for computation and gets its result back. But both the fog nodes and cloud cannot be trusted fully because the returned result is correct or not is a huge concern for the user and cloud. There is some mechanism available in the cloud to check the correctness of the result but in fog, there is no such mechanism present to check correctness. But there are some mechanisms proposed for fog computations to verify the result but have not been implemented yet.

SOLUTION

Although there are schemes proposed they are all theoretical approaches to verify the computation privately or publically. In fog, computing computation is done in a distributed way so an error generated by one node will cause an error in the result of another node and so on[58][59]**Error! Reference source not found.**. So all the intermediate results and the final result should be verified to guarantee the correctness of the result and to trace out the fog node putting the fault results[61][62].

RQ3: What are the applications of fog computing in IoT?

To answer this question we explain different application use cases and these use cases are given below.

1. URBAN SURVEILLANCE

The global masses are impelling towards smart cities. According to United Nations Population Funds, more than 50% of the population lived in urban areas and it is expected that this figure will increase up to 70% by 2050[31]. So, many cities are installing video cameras, environmental sensors, and edge computing platforms such as Rasberry pi and fog computing platforms e.g. NVIDIA Jetson TX1 to become a part of the light pole computing pilot. Video surveillance in urban cities is not just good for the safety of the public but it is also helpful for observations around the cities e.g. to observe the violation of parking or to observe any criminal activity with the help of trained deep learning models based on IoT devices in the smart cities.

As we know to train a neural network is pricy and videos at the source i.e. edge device that is also big. It is required hours to train a neural network to perform accurately. As a result, classification using trained models is a good approach but also this GPU-based processing takes hundreds of frames per second.

Hence, we can train the model in batch, then computation and data can move to the fog layer it saving bandwidth. Classification can be done either on fog or edge depending on the need. A night when human safety is more concerned we can collect data of the public's activities in the daytime and then train our model for street cameras to find out any suspicious activity thus these kinds of edge devices can trigger an alert message in nearby smartphones or notify officers. The edge and fog both platforms can also provide services to other IoT devices such as tapping a video streaming or sensor streamers for data analytics[32].In this work, we propose "Cumulus," an open-source platform for low-cost, low-latency edge cloud compute[33].

2. SMART POWER GRID

Over 4 million customers will be served by Los Angeles Smart Grid in the USA[69]. Electricity smart meters are connected via the internet and observe the power supply-demand of households and industries. Then report to electricity companies periodically after a few minutes. These

meters run on a peer-peer model or 2G. Demand–response optimization keep a balance between demand and supply of electricity depending upon the need. It means that demand-response and load control decisions are being performed at multiple levels. The electricity companies observe data of demand and supply that enable them to forecast the demand and depending on such decisions these companies can cut off or supply the electricity. After that, the utility will notify the customers accordingly via edge devices[70-73].

Demand-response loop feedback is tolerant to time from a few seconds to a few minutes but when it comes to loading control it is sensitive to time as it can affect the distribution network. The computational models run on very fine-grained measurements to detect any instability and thus respond quickly accordingly on the edge to avoid the distribution network from malfunctioning. Fog state distribution models are a good example that can take periodic updates to the cloud and also push back from the cloud.

3. INTERNET OF VEHICLES

Internet of Vehicles (IOV) is a distributed network of vehicles that produce data and thus by using that data vehicles communicate in real-time with drivers or with other vehicles. They are connected usually with an edge network. Different support systems in IOV enable vehicles to perform a different set of operations. Autonomous vehicles are a perfect example of IOV where a self-driving car is taking all decisions without human intervention[35][36][37].

IOV is intolerant to time and they have to decide in Nanoseconds to avoid any road contingencies or any road disasters[38]. The IoV's main purpose is to improve the vehicular network's communications and data security. As a result, the chances of sending blockchain packets via a cellular network are slim[34][39].

By using deep learning we can train our models by using the data of the roads but to train a neural network is costly when it comes to computation. Instead of sending our data to the cloud and then training our model, it is a good way to use fog layer or fog nodes to compute and train the model hence it will lower the latency and thus will be helpful for IOV to decide in real-time.

CONCLUSION AND FUTURE WORK

After studying fog computing we concluded that it is providing and supporting some real-time issues of cloud computing such as latency-sensitive tasks, traffic congestion, computation, and storage. Many hybrid architectures are purposed among them fog computing with SDN and fog radio access both showed some promising future of fog computing. Although, fog computing is more reliable than cloud computing if the user's requests are not correlated and fog nodes would not have enough resources in this case the ultimate choice is cloud computing. From a security and privacy point of view, fog computing has more reliability and trust than cloud computing. But there are many challenges which we need to address like location privacy prevention. Security still has space for future work like detection of rouge fog nodes in IoT.

CREDIT AUTHOR STATEMENT

Mansoor Ahmed Rasheed: Conceptualization, Methodology, draft handling and maintain, Abstract, Introduction, Big data governance and its Framework, Figures. **Jabar Saleem:** Introduction, Background, Motivation and Related Studies, Research questions, **Hudabia Murtaza:** Results and analysis, Research questions,Methodology, Irregularity in Data Integrity, Case study presenting big data governance. **Hafiz Abdullah Tanweer:**Methodology,Table making and Editing, Optimize and Compute, Rules and Policies, Data Management, Scope of big data. **Mannan Ahmad Rasheed:** Stakeholder's Selection, Storage of Big Data, Tools for big data governance ,**Mishaal Ahmed:**Opportunities, Improved Data Security and Privacy, Data centralization.

COMPLIANCE WITH ETHICAL STANDARDS

It is declare that all authors don't have any conflict of interest.Furthermore, informed consent was obtained from all individual participants included in the study.

REFERENCES

[1] C. E.-t.-E. I. Analytics, "for Electric Utilities Solution Overview," *URL https://www. cisco. com/c/en/us/solutions/collateral/data-center-virtualization/big-data/solution-overview-c22-740248. html*, 2018.

[2] P. Varshney and Y. Simmhan, "Demystifying fog computing: Characterizing architectures, applications and abstractions," in *2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, 2017: IEEE, pp. 115-124.

[3] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112-116, 2016.

[4] N. Bessis and C. Dobre, *Big data and internet of things: a roadmap for smart environments*. Springer, 2014.

[5] E. Wikström and U. M. Emilsson, "Autonomy and control in everyday life in care of older people in nursing homes," *Journal of Housing for the Elderly*, vol. 28, no. 1, pp. 41-62, 2014.

[6] O. C. A. W. Group, "OpenFog reference architecture for fog computing," *OPFRA001*, vol. 20817, p. 162, 2017.

[7] G. Infrastructure, "Amazon Web Services," *URL: http://aws. amazon. com/aboutaws/global-infrastructure/(visited on 2017-03-14)*, 2018.

[8] S. Krishnan and J. L. U. Gonzalez, "Getting Started with Google Cloud Platform," in *Building Your Next Big Thing with Google Cloud Platform*: Springer, 2015, pp. 13-

[9] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and

research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1826-1857, 2018.

[10] D. M. Vistro, A. U. Rehman, A. Abid, M. S. Farooq, and M. Idrees, "Analysis of cloud computing based blockchain issues and challenges," *Journal of Critical Reviews*, vol. 7, no. 10, pp. 1482-1492, 2020.

[11] H. ElSawy, E. Hossain, and M.-S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147-4161, 2014.

[12] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *IEEE Access*, vol. 7, pp. 156237-156271, 2019.

[13] Gaspar, L. Mendes, M. Matthé, N. Michailow, A. Festag, and G. Fettweis, "LTE-compatible 5G PHY based on generalized frequency division multiplexing," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, 2014: IEEE, pp. 209-213.

[14] E. Bastug, M. Bennis, and M. Debbah, "Living on the edge: The role of proactive caching in 5G wireless networks," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 82-89, 2014.

[15] Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *2014 federated conference on computer science and information systems*, 2014: IEEE, pp. 1-8.

[16] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts," *Applications and Issues Department of Computer Science College of William and Mary Williamsburg, VA, USA https://dl. acm. org/doi/pdf/10.1145/2757384.2757397*, 2016.

[17] K. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *International Journal of Computer Applications*, vol. 122, no. 3, 2015.

[18] L. Rao, X. Liu, L. Xie, and W. Liu, "Coordinated energy cost management of distributed internet data centers in smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 50-58, 2011.

[19] J. Galvão, J. Sousa, J. Machado, J. Mendonça, T. Machado, and P. V. Silva, "Mechanical design in industry 4.0: Development of a handling system using a modular approach," in *International Conference on Innovation, Engineering and Entrepreneurship*, 2018: Springer, pp. 508-514.

[20] M. Mukherjee *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293-19304, 2017.

[21] D. M. Vistro, A. U. Rehman, M. S. Farooq, A. Abid, and M. Idrees, "A SURVEY ON CLOUD COMPUTING SECURITY WITH CROSS PLATFORM," *Journal of Critical Reviews*, vol. 7, no. 10, pp. 1439-1445, 2020.

[22] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*: Springer, 2018, pp. 103-130.

[23] S. G. Wayangankar and P. P. Jorvekar, "Survey on Internet of Things in the Fog," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 2018: IEEE, pp. 80-86. .

[24] F. L. Wang, J. Fong, and M. Choy, "Blended learning for programming courses: A case study of outcome based teaching & learning," *Blended Learning*, p. 30, 2007.

[25] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*: Springer, 2018, pp. 103-130.

[26] V. B. C. Souza, W. Ramírez, X. Masip-Bruin, E. Marín-Tordera, G. Ren, and G. Tashakor, "Handling service allocation in combined fog-cloud scenarios," in *2016 IEEE international conference on communications (ICC)*, 2016: IEEE, pp. 1-5.

[27] O. Simeone, A. Maeder, M. Peng, O. Sahin, and W. Yu, "Cloud radio access network: Virtualizing wireless access for dense heterogeneous systems," *Journal of Communications and Networks*, vol. 18, no. 2, pp. 135-149, 2016.

[28] I. T. Haque and N. Abu-Ghazaleh, "Wireless software defined networking: A survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2713-2737, 2016.

[29] M. S. Farooq and S. Akram, "IoT IN AGRICULTURE: CHALLENGES AND OPPORTUNITIES," *J. Agric. Res*, vol. 59, no. 1, pp. 63-87, 2021..

[30] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE communications magazine*, vol. 46, no. 4, pp. 88-95, 2008.

[31] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. B. Zikria, "Role of IoT technology in agriculture: A systematic literature review," *Electronics*, vol. 9, no. 2, p. 319, 2020.

[32] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," *Journal of urban technology*, vol. 22, no. 1, pp. 3-21, 2015.

[33] R. Ghosh and Y. Simmhan, "Distributed scheduling of event analytics across edge and cloud," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 4, pp. 1-28, 2018.

[34] H. Gedawy, S. Tariq, A. Mtibaa, and K. Harras, "Cumulus: A distributed and flexible computing testbed for edge cloud computational offloading," in *2016 Cloudification of the Internet of Things (CIoT)*, 2016: IEEE, pp. 1-6.

[35] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640-4649, 2018.

[36] S. Coicheci and I. Filip, "Self-driving vehicles: current status of development and technical challenges to overcome," in *2020 IEEE 14th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2020: IEEE, pp. 000255-000260.

[37] W. Schwarting, J. Alonso-Mora, and D. Rus, "Planning and decision-making for autonomous vehicles," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 187-210, 2018.

[38] P. Szikora and N. Madarász, "Self-driving cars—The human side," in *2017 IEEE 14th international scientific conference on informatics*, 2017: IEEE, pp. 383-387.

[39] R. Ghebleh, "A comparative classification of information dissemination approaches in vehicular ad hoc networks from distinctive viewpoints: A survey," *Computer Networks*, vol. 131, pp. 15-37, 2018.

[40] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589-3603, 2010.

[41] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017: IEEE, pp. 551-556.

[42] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34-42, 2017.

[43] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things," *Security response, symantec*, 2015.

[44] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015: Ieee, pp. 1202-1207.

[45] J. C. Nobre *et al.*, "Vehicular software-defined networking and fog computing: Integration and design principles," *Ad Hoc Networks*, vol. 82, pp. 172-181, 2019.

[46] A. Muthanna *et al.*, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 15, 2019.

[47] D. Pliatsios, P. Sarigiannidis, S. Goudos, and G. K. Karagiannidis, "Realizing 5G vision through Cloud RAN: technologies, challenges, and trends," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1-15, 2018.

[48] H. M. Abdel-Atty, R. S. Alhumaima, S. M. Abuelenin, and E. A. Anowr, "Performance analysis of fog-based radio access networks," *IEEE Access*, vol. 7, pp. 106195-106203, 2019.

[49] R. S. Rai, "Performance Analysis of Non-Orthogonal Multiple Access (NOMA) in C-RAN, H-CRAN and F-RAN for 5G Systems," University of Kent, 2019.

[50] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge intelligence in the cognitive Internet of Things: Improving sensitivity and interactivity," *IEEE Network*, vol. 33, no. 3, pp. 58-64, 2019.

[51] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Transactions on Emerging Telecommunications Technologies*, p. e3677, 2019.

[52] N. Tariq *et al.*, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[53] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: Architecture, challenges, and optimization," *IEEE Access*, vol. 5, pp. 25445-25454, 2017.

[54] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for Healthcare 4.0 environment: Opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, pp. 1-13, 2018.

[55] R. K. Naha *et al.*, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE access*, vol. 6, pp. 47980-48009, 2018

[56] M. Mukherjee *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293-19304, 2017.

[57] A. Yousefpour *et al.*, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289-330, 2019.

[58] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for internet of things and analytics," in *Big data and internet of things: A roadmap for smart environments*: Springer, 2014, pp. 169-186.

[59] S. Wang, Y. Ruan, Y. Tu, S. Wagle, C. G. Brinton, and C. Joe-Wong, "Network-aware optimization of distributed learning for fog computing," *IEEE/ACM Transactions on Networking*, 2021.

[60] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, pp. 1-22, 2017..

[61] R. Mahmud, K. Ramamohanarao, and R. Buyya, "Latency-aware application module management for fog computing environments," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 1, pp. 1-21, 2018.

[62] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, 2017.

[63] L. Li, K. Ota, and M. Dong, "Deep learning for smart industry: Efficient manufacture inspection system with fog computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4665-4673, 2018.

[64] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*, 2018: IEEE, pp. 1-8.

[65] N. Mohan and J. Kangasharju, "Edge-Fog cloud: A distributed cloud for Internet of Things computations," in *2016 Cloudification of the Internet of Things (CIoT)*, 2016: IEEE, pp. 1-6.

[66] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Computers & Security*, vol. 74, pp. 340-354, 2018.

[67] S. Raponi, M. Caprolu, and R. Di Pietro, "Intrusion detection at the network edge: Solutions, limitations, and future directions," in *International Conference on Edge Computing*, 2019: Springer, pp. 59-75.

[68] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[69] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of things journal*, vol. 3, no. 6, pp. 854-864, 2016.

[70] Y. Simmhan *et al.*, "Cloud-based software platform for data-driven smart grid management," *IEEE/AIP computing in science and engineering*, vol. 79, 2013.

[71] A. Arooj, M. S. Farooq, T. Umer, and R. U. Shan, "Cognitive internet of vehicles and disaster management: a proposed architecture and future direction," *Transactions on Emerging Telecommunications Technologies*, p. e3625, 2019.

[72] A. Abid, M. F. Manzoor, M. S. Farooq, U. Farooq, and M. Hussain, "Challenges and Issues of Resource Allocation Techniques in Cloud Computing," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, no. 7, pp. 2815-2839, 2020.

[73] I. A. Khawaja, A. Abid, M. S. Farooq, A. Shahzada, U. Farooq, and K. Abid, "Ad-Hoc Collaboration Space for Distributed Cross Device Mobile Application Development," *IEEE Access*, vol. 8, pp. 62800-62814, 2020.

[74] A. Arooj, M. S. Farooq, A. Akram, R. Iqbal, A. Sharma, and G. Dhiman, "Big Data Processing and Analysis in Internet of Vehicles: Architecture, Taxonomy, and Open Research Challenges," *Archives of Computational Methods in Engineering*, pp. 1-37, 2021.

[75] O. Aziz, M. S. Farooq, A. Abid, R. Saher, and N. Aslam, "Research trends in enterprise service bus (ESB) applications: A systematic mapping study," *IEEE Access*, vol. 8, pp. 31180-31197, 2020.

[76] I. Obaid, M. S. Farooq, and A. Abid, "Gamification for recruitment and job training: model, taxonomy, and challenges," *IEEE Access*, vol. 8, pp. 65164-65178, 2020

[77] H. Malik, M. S. Farooq, A. Khelifi, A. Abid, J. N. Qureshi, and M. Hussain, "A Comparison of Transfer Learning Performance Versus Health Experts in Disease Diagnosis From Medical Imaging," *IEEE Access*, vol. 8, pp. 139367-139386, 2020.

[78] R. Tehseen, M. S. Farooq, and A. Abid, "A framework for the prediction of earthquake using federated learning," *PeerJ Computer Science*, vol. 7, p. e540, 2021.

[79] A. Abid, M. S. Farooq, I. Raza, U. Farooq, and K. Abid, "Variants of Teaching First Course in Database Systems," *Bulletin of Education and Research*, vol. 37, no. 2, pp. 9-25, 2015.

[80] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," *arXiv preprint arXiv:1502.01815*, 2015.

[81] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the internet of things: A survey," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 2, pp. 1-41, 2019.

[82] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489-2520, 2020.

[83] A. Ahmed *et al.*, "Fog computing applications: Taxonomy and requirements," *arXiv preprint arXiv:1907.11621*, 2019.

[84] J. Singh, P. Singh, and S. S. Gill, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *Journal of Parallel and*

Distributed Computing, vol. 157, pp. 56-85, 2021.

[85] A. Markus and A. Kertesz, "A survey and taxonomy of simulation environments modelling fog computing," *Simulation Modelling Practice and Theory*, vol. 101, p. 102042, 2020.

[86] A. Markus and A. Kertesz, "A survey and taxonomy of simulation environments modelling fog computing," *Simulation Modelling Practice and Theory*, vol. 101, p. 102042, 2020.