Open access • Journal Article • DOI:10.4018/IJFC.2020010105

# Fog Computing Architecture, Applications and Security Issues — Source link

Rahul Neware, Urmila Shrawankar

**Published on:** 01 Jan 2020

Peer-reviewed version available at International Journal of Fog Computing (IJFC) 2020; doi:10.4018/IJFC.2020010105

# Fog Computing Architecture, Applications and Security Issues: A Survey

**Rahul Neware***

MTech Student; Department of Computer Science and Engineering, G.H. Raisoni College of Engineering Nagpur, Maharashtra, India, 440016; neware_rahul.ghrcemtechcse@raisoni.net

* Correspondence: neware_rahul.ghrcemtechcse@raisoni.net; Tel.: +91-904-939-4357

**Abstract:** The development of Internet of Things (IoT) has triggered a virtual wave of interconnection and intercommunication among enormous number of universal things. This has caused an exceptional surge of colossal heterogeneous information, known as information explosion. Until now, cloud computing has filled in as a proficient method to process and store these data. Still, it came to light that by utilising just cloud computing, pesky issues like, the expanding requests of actual-time or speed-sensitive applications and the restrictions on system transfer speed could not be solved. Consequently, another computing platform, called fog computing has been advanced as a supplement to the cloud arrangement. Fog computing spreads the cloud administrations and services to the edge of the system, and brings processing, communications and reserving and storage capacity closer to edge gadgets and end-clients and, in the process, aims at enhancing versatility, low latency, transfer speed and safety and protection. This paper takes an extensive and wide-ranging view of fog computing, covering several aspects. At the outset is outlined the many-layered structural design of fog computing and its attributes. After that, chief advances like communication and inter-exchange, computing, reserving and storage, asset administration, naming, safety and safeguarding of privacy are delineated, while showing how these back up and facilitate the installations and various applications. Then, numerous applications like augmented reality (AR), healthcare, gaming and brain-machine interface, vehicular computing, smart scenarios etc. are highlighted to explain the fog computing application milieu. Following that, it is shown that how, despite fog computing being a features-rich platform, it is dogged by its susceptibility to several security, privacy and safety concerns, which stem from the nature of its widely distributed and open architecture. Finally, some suggestions are advanced to address some of the safety challenges discussed so as to propel the further growth of fog computing.

**Keywords:** Fog Computing; Cloud Computing; Security and Privacy; Edge Computing; Internet of Things;

## 1. Introduction

The internet has revolutionized the computers, communication and communication technology like nothing has ever before. The internet's invention is one of mankind's most cherished accomplishments. Yet, the seepage of its use and adaptation of technology is changing its terrain rapidly. The specter of new technologies coming together and linking with each other faster has created new paradigms like Cyber-Physical System (CPS) and the Internet of Things (IoT). What is unimaginable is the wireless connection of devices to our physical bodies, to each other and absolutely everything around us at any time [1, 2]. Thus, IoT implies an expansion of Internet through which physical objects are connected virtually, with the ability to provide smart services to its users.

Naturally, this interaction between devices is slated to create gargantuan amounts and diversities of information and data. It is interesting to consider some figures. Cisco predicts that by 2020 some 50 billion devices will be connected to the Internet, and the data and information generated by devices, people, things, appliances etc. will amount to 500 zettabytes. And by 2019, out of this, 45

percent of data generated by IoT will be interpreted, processed, analysed and saved at the network's edge [3,4].

Along with the mushrooming of data, the pace of data creation is fast increasing, too. For instance, findings related to healthcare services show that 30 million users create about 25,000 tuples data per second[5] with respect to healthcare-linked IoT communication. This means the data storage and processing mechanisms that we have in place at present are unable to keep up with what is expected[6]. And traditional computing versions, like distributed computing etc. are failing to handle this deluge.

But the advent of cloud computing has emphatically altered the scenario of information technology. By getting rid of such factors like proportional expenses, scalability, getting rid of upfront IT investment etc., it has brought in substantial advantages for IT users[7-11].

Thus, owing to its potent computational power and capacity to store [12,13], cloud computing emerged as an effective method for data processing. At the same time, though, there are some inherent issues with cloud computing. For one, cloud computing is a consolidated, centralized computing representation that performs computations in the cloud. This means that all the data, information, requests and what have you have to be dispatched to the cloud. And while the pace of processing of data has increased swiftly, the bandwidth of network has not kept equal pace.

So for massive amounts of data, bandwidth of network is turning out to be a hindrance in cloud computing. And this is causing long latency, the duration of time it takes for data to go from point to another. And the issue is compounded when increasing number of devices are linked to Internet because applications that are sensitive to latency begin to face grave problems of long delays. For instance, systems in some IoT applications, such as emergency response[14], smart healthcare[15,16], traffic light system in smart transportation, smart grids[17] and other latency-sensitive applications[18] may perforce need an extremely short response time and support of mobility. In short, it was found that these challenges stemming from the unprecedented growth of IoT, with respect to latency, bandwidth of network, mobility support, dependability, location awareness, security etc., could not be effectively tackled by the model of cloud computing.

And thus emerged a new paradigm named Fog computing, to surmount the issues listed above [19][20]. Fog computing, it is established, effortlessly facilitates working between center of cloud and devices that are at the network edge, and thus morphs as a better solution to tackle the problems presented by cloud computing. Bonomi et al. [21] describe Fog computing "as a geographically distributed, highly virtualized architecture where diverse multifarious devices at the brink of network are universally linked in conjunction to offer communication, flexible computation and storage facilities" [22].

It is worth noting that both cloud and fog computations deliver to end users application services, computation, storage and data[23]. But certain telling features distinguish fog from cloud. Fog is a platform that locally processes huge amounts of data, enables installation of software on diverse hardware[24], has dense geographical distribution, offers support for mobility[25] and is decentralized and close to end users.

A case in point displaying and proving the aspect of latency is a system of traffic lights. In a system of traffic lights not based on Fog, between the cloud server and monitoring probes there might be 3 to 4 jumps or hops. This makes it difficult to make actual-time decisions and the problem of network latency pops up. If the system is Fog-based, however, monitoring probe serves like a sensor and the traffic lights as actuator. The Fog node can transmit a normal condensed video which can exist in the cloud for some duration. The Fog can take an instantaneous decision to turn green the related traffic lights when it records headlights of an ambulance flashing, to enable the health-care vehicle to pass through without holding it. Still, what is to be noted is that the Fog is only an adjunct; it can supplant the Cloud.

The most noteworthy facet of fog computing is that it extends the services of cloud to the brink of the network. By gathering the local resources, it brings in close proximity such features as communication, control, storage and computation to end clients. The topographically dispersed

devices at the edge of network absorb all the information and data. The net result is that the time of data transmission and the volume of network transfer is immensely curtailed[26].

Thus the Fog platform can keep up with the requirements of applications that need latency and also, in the process, smooth hindrances in bandwidth of network. Moreover, for users Fog is accessible from any location, at any time, through any device that is linked to the network of Fog. It's no wonder then that Fog computing has found increasing favor in such areas as healthcare [27-30], smart city [31-33] and others. Also, thanks in due parts to its quick response and small energy expenditure [34,35], it can offer enhanced Quality of Service (QoS).

As for the fog system itself, it is made up of what are called fog nodes, which incorporate various devices that are at the edge of network and systems of management imbedded in the devices. It also includes some simulated edge of centers of data[36]. Fog computing serves to work as a connecting link between cloud and edge users. This is accomplished by fog nodes by conjoining end appliances and devices and users through the use of wireless connection platforms like Wi-Fi, Bluetooth, 4G etc., to make available services such storage, computation and computing. At the same time, to fully utilize the cloud's loaded storage and computing resources, fog nodes can also be linked, through Internet, with cloud [37]. Thus the fog computing system facilitates speedy evaluation of data and the process of decision making.

It must, however, be borne in mind that fog computing is just an adjunct of cloud computing. It does neither replace nor substitute cloud computing. Edge devices and sensors create data and fog nodes simply save and process the data. After this, the leftover significant data is shifted over the cloud server for either further processing or saving.

Fog computing, undoubtedly, is a dynamic, versatile resources-rich platform. Still, it's widely dispersed and open structural design renders it vulnerable to various kinds of attacks, endangering the safety and security of its operation. For instance, in IoT fog nodes are frequently the primary group of processors that data or information meets, and have the assets to execute a full hardware root of trust. This root of trust can be stretched to all applications and procedures operating upon them, and thereafter to the Cloud [38]. If a hardware root of trust is missing, different assault situations can hobble the fog's software frameworks, permitting the assaulters to establish their sway. Thus, with the ascent of the fog, newer dangerous issues relating to trust and safety have sprung forth[39]. As it happens, however, because of the fog's attributes of diversification, mobility and wide universal dispersion, the available current techniques are inadequate to counter the security threats[40]. This paper specifically dwells on the issues of safety, security and trust pertaining to fog computing. This paper also undertakes an extensive survey of fog computing. It details various aspects of fog computing, including its design and architecture, main technologies involved, the applications where fog computing can be put to effective use and the security and trust issues and other challenges.

The survey paper's first chapter gives a general introduction to fog computing. In chapter 2, the architecture and attributes and characteristics of fog computing are enumerated. Chapter 3 dwells on the main technologies involved in fog computing. Chapter 4 focuses on certain prominent applications vis-a-vis fog computing. Chapter 5 shines a light on the challenges, security and trust issues dogging fog computing. And the conclusion is presented in chapter 6.

## 2. Architecture of Fog Computing

Fog computing, a new platform that complements cloud computing, shifts the conventional cloud jobs like computing and services to the brink of network. At the network's edge, it offers to end users communication, storage, services, controlling and computation. The prominent feature of fog computing is its decentralization. In its design and architecture fog computing is at variance with other traditional models of computation. Below, we take a look at the architecture and design and attributes and characteristics that are the hallmark of fog computing.

*2.1. The Hierarchical Architecture of Fog Computing*

Since its advent, for fog computing several designs have been propounded. But the majority of them have invariably relied on a three-tier architecture. As has been mentioned earlier, fog computing shifts cloud services to the network's brink. It accomplishes this by injecting a layer of fog between the cloud and end appliances.

The stratified structure of fog computing stems from the following three tiers:

Terminal tier: This tier is the nearest in proximity to the end user and physical world. It encompasses different IoT segments such as cell phones, sensors, smart cards, smart vehicles etc. Generally, these devices are dispersed widely and sense and capture the feature information of actual happenings or objects and then transfer the sensed information to the tiers above, either for saving or processing.

Fog tier: Situated at the network's edge, this tier comprises many fog nodes, such as switchers, routers, access points, gateways fog servers, base stations etc. Between the cloud and end devices these fog nodes are dispersed widely, for instance, locations such as shopping malls, bus depots, cafes, parks, streets, etc. Whatever their position, whether moving on vehicles or fixed at a location, the fog nodes facilitate connectivity with end devices to deliver services. They possess the power to transfer, quantify and save the data received through sensing. It is in the fog tier where latency-sensitive functions and actual-time analysis takes place. Additionally, through IP core network, fog nodes can link with the centre of cloud data and work jointly and interact with cloud to acquire more enhanced strengths for saving and processing.

Cloud tier: Consisting mainly of various high-geared servers and storage niches, cloud computing tier is responsible for offering diverse services of applications, such as smart transportation, smart factory, smart home, smart office etc. This tier possesses mammoth capabilities for storage, saving and computing and therefore executes wide-ranging computation analysis and stores and saves eternally huge amounts of data and information[41].

In this design, wired connection or wireless access technologies, such as Wi-Fi, 3G, Local Area Network, 4G, Bluetooth, ZigBee and others help link each smart item or end device with fog nodes. Wireless or wired communication technologies also help fog nodes to link and communicate among themselves. On top of that, through IP core network, each fog node remains connected with the cloud.

Thus, this architecture, in essence, has the capability to offer technical backing to IoT, Mobile internet and CPS to ensure competent storage facilities and processing of data. To control and monitor the devices and objects that are in the physical world [42], CPS blends the competencies of communication, storage and computing. Fog computing can enhance quality of service and proficiency of CPS, especially in the present scenario of data proliferation.

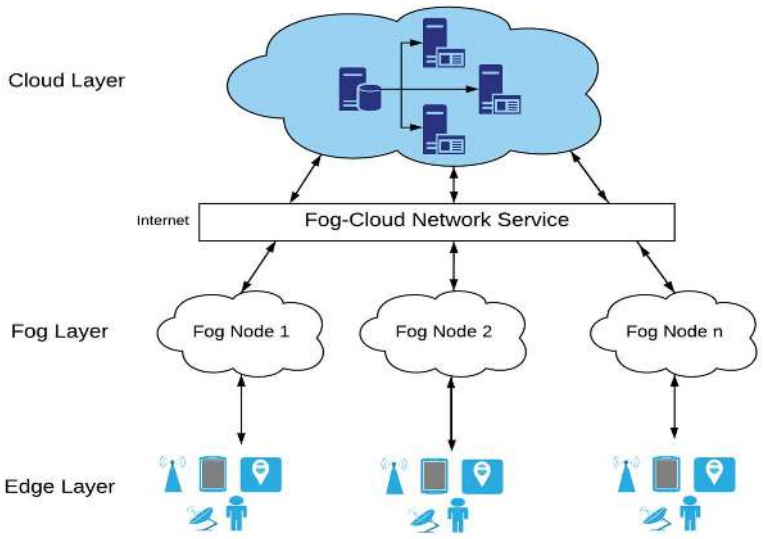


**Figure 1.** Hirarchical Architecture of Fog Computing

*2.1. Charesteristics of Fog Computing*

Fog computing performs its jobs of communication, storage and computation on devices on network that are close to users. This means that for end users computing's services are close at hand. This assumes the most crucial attribute of fog computing. It is also the most pivotal benefit of fog computing in comparison to other models of computing. Enumerated below are some prominent characteristics and benefits of fog computing:

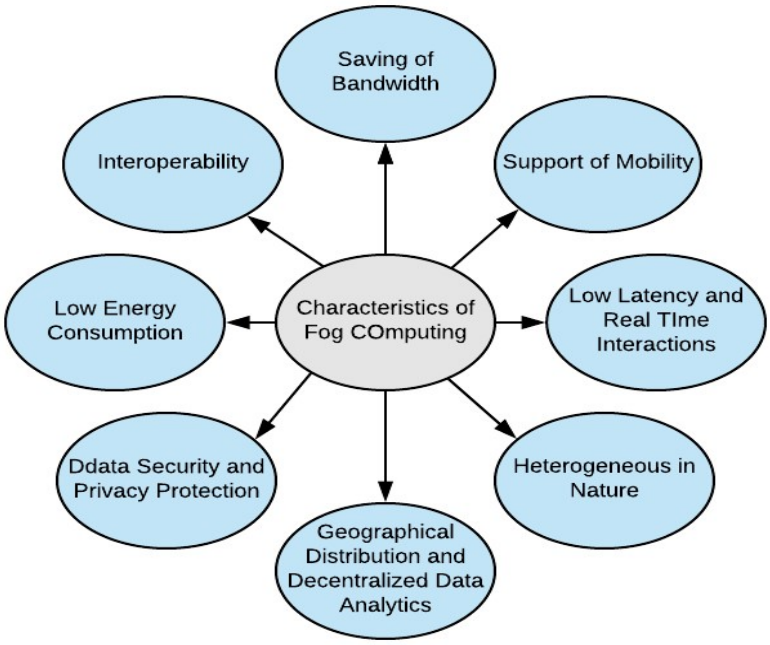


**Figure 2.** Characteristics of Fog Computing

2.1.1. Saving of Bandwidth

As noted earlier, to store and process data between cloud and end nodes, fog computing shifts to the edge of the network storage and its computation capabilities, while some jobs are executed locally, jobs like getting rid of redundancy, pre-processing of data, extracting of important information, filtering and sprucing up of data etc. That is the benefit of locally performed jobs. A major part of data is not needed to be transferred to cloud, only a significant segment of data has to be transferred. For instance, in the experiment of Hu et al.[43] with respect to fog computing related face recognition and identification, fog nodes managed to transfer just the identifiers of face to the cloud.
Thus, fog computing could substantially curtail the volume of network transmission and in consequence salvage bandwidth. Also, fog nodes, in the working of certain applications, execute decision making locally, rather than shifting the process to cloud and, in effect, saving bandwidth considerably.

2.1.2. Support of Mobility

Fog computing gives backing for mobility. Mobile devices, such as smart vehicles, smart watches, smart phones, are intrinsically linked with fog computing, generating at the terminal tier regular spatial mobility. At the same time, certain devices like cameras monitoring street traffic, can stay fixed and static. In fog tier fog node can serve as both a static or mobile computing resource base.

Especially at locations such as coffee outlets, airports or on moving trains and cars [44-46] this fog node can be extensively used. Thus it becomes imperative for fog computing to interact and communicate straight-forwardly with mobile appliances. Fog computing design can back mobility demands generated from locations, equipping managers and administrations to have sway over

mobile gadgets and their users' locations and the manner in which they obtain data[47]. This contributes to enhancing quality of service and the system's performance.

#### 2.1.3. Low Latency and Real Time Interactions

Sensors and devices create data that is absorbed by fog nodes situated at the edge of network, and save and process data from devices at network edge in local area network. This results in substantial saving of movement of data over Internet, offering accelerated blue-ribbon services that are localized and backed by end points. Thus, for applications that demand latency and quick time [25], it facilitates low latency and fulfils the need of actual-time interactions.

This was borne out by Sarkar et al. [41] who showed that latency of service linked to a protocol incorporating fog computing was lower than the one linked to cloud computing. Similar result was obtained by Hu et al. [43] when they employed fog computing in the field of face recognition and resolution. Their experiment found that the response period from the system was much reduced as compared to cloud computing.

#### 2.1.4. Heterogeneous in Nature

Fog nodes, generally, assume two forms, virtual or physical notes and are used in diverse environments. They normally comprise gateways, edge routers, base stations, high-executing servers, access points and others. Possessing varying degrees of storage and computation potential, these hardware components operate different types of operating systems (OS) and upload a number of diverse software applications. In fog computing, being a well-simulated or virtualised programme, certain virtual network nodes and virtual computing nodes can also double up as fog nodes [37]. This clearly establishes the diversity or heterogeneity of fog nodes.
Further, fog computing's infrastructure of network incorporates wireless access technologies, such as ZigBee, Wi-Fi, 3G, WLAN, 4G [48] etc., and also faster connections linking to data centre. This also points to diversity or heterogeneity of fog computing's network infrastructure.

The fog computing's design, from the brink to the core, emanates from a multi-layered hierarchical structure. To fulfil the demands of low latency of applications that are widely dispersed, in certain IoT applications like smart home, Internet of Vehicles, smart transportation etc., service interfaces and resources of fog nodes are exceedingly forceful and diversified at varied stages of the design hierarchy [49].

#### 2.1.5. Geographical Distribution and Decentralized Data Analytics

Fog computing comprises many nodes that are universally dispersed. Hence, they possess the power to keep watch over and figure out the locations of end gadgets to back mobility. Thus the design and services of fog computing foster geographically dispersed use. The prominent feature of fog computing is decentralisation which enables the data and information to stay close to the end user. This attribute helps in providing improved location-related services, potent competencies to execute actual-time decisions and quicker analysis of big data.

Especially in IoT with its universal computing scenario, the main aim is to accomplish faster interworking and interlinking between gadgets that are widely dispersed and massive in numbers. These requirements can be fulfilled because of fog computing's attributes of decentralised information analytics and geographical distribution capabilities. For instance, fog computing is able to offer an array of different IoT related services in the area of Internet of Vehicles - services such as feedback on conditions prevailing in urban areas and on streets, entertaining related data, traffic security etc., emanating from the linking and communication between vehicle to vehicle and vehicle to access doors [50].

#### 2.1.6. Data Security and Privacy Protection

The prominent feature of fog computing is that it delivers services in close proximity to end users. This has beneficial implications in terms of safeguarding of privacy and safety of data. It can simply

safeguard data through isolation and encryption by offering integrity checks, policy of access control, isolation techniques and schemes of encryption. Additionally, it can prevent the glitches and risks arising out of upgradation of system. Unlike the remote upgrade that takes place in conventional devices, only the updating of micro applications and algorithms at the fog end is required and not the Over-the-Air Technology (OTA) rmware system of upgradation employed in remote upgradation.

#### 2.1.7. Low Energy Consumption

Since fog nodes in fog computing structure are spread topographically, it does not create too much heat that might otherwise have resulted from concentration, and hence it does not require any extra cooling method. Moreover, the usage of communication energy is also curtailed [51] because certain mobile nodes optimally manage energy and because of communication mode's short range. Thus it serves to curtail use of power, conserves energy and reduces the costs, making fog computing a green computing platform.

That fog computing acted as a greener computing system was shown by Sarkar et al. [41] through a theoretical specimen of the structure of fog computing. The outcome of the experiment showed that the fog computing structure expended 40.48% less average energy than the regular traditional model of cloud computing.

#### 2.1.8. Interoperability

Fog computing is diversified and heterogeneous in nature in which end gadgets and fog nodes are supplied by various providers located at different locations and the fog nodes end up being employed in different scenarios. So, it becomes imperative for fog nodes to interlink, cooperate and interconnect with a wide variety of providers so as to be able to deliver and support a wide array of services [54].

A case in point is the fog computing-backed streaming service that necessitates working together of various providers, in which services end up being allocated across different locations and domains [25]. Here, consider the scenario of the fog computing related system of smart transportation. In this, with vital transfer of data among smart vehicles, fog nodes and applications, traffic lights and signals, what is needed is quick analysis of actual-time data. Therefore, to make sure that there is safe cooperation and collaboration and interoperability between various resources employed in fog computing. [52,53}, a scheme of management of resources in the form of a policy has been propounded.

## 3. Main Technologies Supporting Fog Computing

In order to be able to deliver applications and services, fog computing relies on certain technologies. These technologies chiefly comprise storage and communication technologies, computing, privacy and security protection, naming, resource management etc. These technologies are fully aligned with fog computing's properties and fulfil its requirements of applications. Below are listed the main technologies that support the fog computing platform.

### *3.1 Computing Technologies*

Fog computing is an intuitive dynamic computing platform in which fog nodes freely fulfil the demands of end users for data processing and computation. In order to deliver the capabilities of fast turnaround and low-latency, it requires the backing of certain computing technologies.

#### 3.1.1. Latency Management

In fog computing any latency management's main aim is to curtail the time of response of any end service within a pre-decided parameter. This parameter is the upper limit up to which latency can be accepted with respect to a request of service or requirement of any application's service quality.

In an effort to achieve management of latency, Oueis et al. [54] put forth an effective induction protocol in which several nodes working with each other complete computation jobs jointly within the parameters of latency. In a separate study, for management of latency Intharawijitr et al. [55] propounded a fog computing design geared to achieve low-latency. To resolve the delay in communication and computing, they proposed a mathematical formula to help guide the choice and selection of nodes in the network of fog that could offer the least delay.

#### 3.1.2. Computational Offloading

The mechanism of computation offloading, which executes the shifting of computational jobs to an external entity, can surmount the limitations of resources inherent in edge gadgets and devices particularly when it comes to computation-sensitivity laden tasks. This can also facilitate in enhancing the operation and preserving the life span of battery[56]. Gao [57] put forth a contingency computation offloading model for computation offloading among companions of fog nodes.

This model, to save energy and curtail time of computation, could offload segments of tasks to the neighbour nodes. It was found that the offloading decision was mainly driven by the neighbour nodes' level of energy, power of computation and the chance of linking between them at a later time. The offloading of the task to the neighbour nodes happened successfully when energy usage and time period could be lessened post offloading and the new node finished the task on time.

### *3.2 Communication Technologies*

The architecture of fog computing, dynamic, decentralised, multi-layered, resource-rich, is unlike that of any other computing mode. In this design, fog nodes act as an in-between networking constituent that links with the cloud, end devices and users as well as with other fog nodes. It houses and makes possible three types of connections: a) wireless connections between fog nodes and edge devices, b) wired and wireless connections between fog nodes, c) wired and wireless connection between centre of cloud data and fog nodes. These technologies of wireless communication that sustain the fog applications, particularly the mobile fog computing encompass Wireless Local Area networks (WLAN), 3G, Bluetooth, WiFi, 4G, ZigBee. The fog computing architecture also supports other communication technologies, which are enumerated below:

#### 3.2.1. Network Function Virtualization

NFV provides a novel method to create, manage and deliver networking services. The prominent feature of NVF is that it detaches network function from owned hardware gadgets and appliances through virtualisation and technology of device abstraction. This makes it possible for resources to be shared flexibly and totally, ensuring quick growth and delivery of new service [58].
Because NFV incorporates IT virtualisation, several components like rewalls, gateways and switches can be virtualised and kept on fog nodes. It can help in easily managing resources such as storage, communication, computing and, in the diversified and geographically dispersed fog network, harmonise various functions[59].

#### 3.2.2. Software Define Networking

An emerging networking platform, SDN's design allows it to be centrally and intuitively controlled and programmed through the use of software applications. Its architecture enables it to delink the control part from the data part. A centralised server executes control and also decides the communication route of node[60]. Its structure enables it to be scalable, flexible and capable of being programmed. It removes dependence on embedded network gadgets and devices such as switches, rewalls, routers etc., and can also rid the differences stemming from diverse network devices. It empowers users to lay down their own rules of network transmission and routing, which gives flexibility to communication[61].

SDN can play a versatile role in fog computing. SDN can competently manage diverse fog networks [62] and find solutions for recurring problems of high packet loss rate, collisions and

uneven connectivity[63]. For instance, SDN can surmount the above problems in fog computing vehicle's network. Truong et al. [64] have suggested an SDN and fog computing- propped-up novel ad hoc network design named FSDN for vehicles, which will solve the problems of poor and uneven connectivity and those related to flexibility and scalability. Additionally, by merging with fog computing, SDN can lessen latency and optimise the use of resources.

3.2.3. The Fifth Generation (5G) Wireless Communication Network

The latest generation of mobile communication technology is on the horizon, bringing benefits like never seen before: high network speed, wide signal coverage, enhanced mobility, a dazzling array of applications, high flux density and others. 5G is geared to achieve 1000 times more growth of system capacity, 10 times more of energy efficiency, 5 times more of latency curtailment and 25 times more of throughput than compared with the present version, 4G[65].

With resource-constricted mobile terminals, 5G technology would allow several challenging services and applications[66]. For mobile users in fog computing, especially, it promises to surmount the glitch of resource constraint and offer extensive resources-studded services [67]. It will also make available an array of dazzling services such as low latency, high-speed data applications and premier-quality wireless communication.

To offer advanced energy and spectral efficiency, Peng et al. [68] has suggested a fog computing-propped-up radio access network that would merge fog computing into diversified cloud radio access network. Besides solving the conventional problems of centralised baseband unit pool and cloud radio access network in the constricted front haul, it will make available actual-time collaboration between flexible cooperative radio resource management and radio signal processing at the devices that are at the edge.

2.3.4. Long-Reach Passive Optical Network(LRPON)

Long Reach Passive Optical Networks (LR-PON) technology has been advanced as a cost-saving solution for deploying fiber for use in office, home buildings, pavements etc. It is better than the conventional PON because it stretches the network reach up to 100 km, using several optical amplifiers. It makes it easy to consolidate the network process over a huge area[69]. In fog computing LRPON has special uses, in terms of giving backing to applications that are bandwidth- and -latency-sensitive, such as smart industry services and smart home. To enhance the design of network, Zhang et al. [70] have suggested that LR-PON and fog computing should be assimilated.

2.3.5. Content Distributed Network(CDN)

CDN, an Internet-based cache network, is the bulwark that is responsible for delivering content, which it does through its proxy servers, located the Internet's edge. CDN's system takes into account such factors as user and load distance of each node and status of connection, and then transmits the content to its proxy servers that are in proximity to the users. Thus, readers and users, in getting information, are able to curtail the download period of contents from faraway sites and enhance response speed [71-72].

Synching with the attributes of fog computing, CDN can confer many benefits; it can lessen expenses and costs, expend less usage of bandwidth, make available more content and can lessen network congestion. Fog computing entrenched with CDN can deliver to end users outstanding services, particularly when aligned with context aware technology.

*3.3 Naming, Identification and Resolution*

Fog computing is a resource-studded centre that houses huge number of devices, gadgets and things and also numerous applications that operate and offer diverse services. Computer networks have the domain name system (DNS). Fog computing, too, has to have a platform of identification, naming and resolution. This would meet the requirements associated with manging and controlling objects, data communication, verification of identity, discovery of services and objects etc.

Among diversified devices, gadgets and things, for collaboration and communication, a competent and established naming mechanism is a must. In fog computing, conventional naming mechanisms like DNS and Uniform Resource Identifier (URI) that are employed extensively in present networks, can meet requirements of applications up to a limit. But the location of most devices, gadgets and things at the edge renders them decidedly mobile and restricted in resources.

This, in turn, renders these mechanisms inflexible in some situations to be in sync with the vibrant fog computing platform. Also, the popular IP-based naming system could not be employed because of cost considerations. Consequently, some novel naming methods have been put forth that would be in sync with fog computing's features. These novel methods, for instance, are called Data Networking(NDN) [73-74] and Mobility First[75].

DN: A growth of IP design, it takes into account "the contents (What) rather than the addresses (Where)." With tier-layered data, NDN packets summon names rather than source and destination location and address. It has the ability to give monikers to anything, whether computers, humans, books, sensors etc. Its chief aim is to enhance the competence, scalability and safety and stability of the prevailing internet paradigm, making it appropriate for fog and edge computing.

MobilityFirst: It aims to tackle the glitches pertaining to wireless access and mobility to fulfil in the present mobile Internet the requirements of naming protocols. Unlike the current system, it detaches names from addresses on network. Currently, both the Global Unique Identification (GUID) and Global Name Resolution Service (GNRS) are employed to affix name and addresses together. In MobilityFirst, though, the API service focuses on names of destination or source network objects, instead of on addresses of network. To accomplish scalability, it employs combined name/address embedded routing. For fog computing that houses devices that move, this naming method delivers excellent results.

As for the technology for identification of devices, applications and things, it is categorised in three segments: physical object identification, communication identification and application identification.

Physical object identification: Chiefly availed to identify devices, gadgets and things, this kind of identification embraces, as identifiers, natural property and ID code. The natural property identifier uses behaviour attributes, biometric, information about space and time or other attributes as identifier[76-77]. This is also termed non-ID verification. On the other hand, the ID code identifier comprises alphabets or numbers with some rules attached to them, such as ubiquitous ID (uID) [78], European Article Number(EAN), Electronic Product Code (EPC) [79] etc.

Communication identification: This one is employed to verify the identity of devices, gadgets or network nodes, especially those that have the capability to deal in communication. Among these, the popular forms are: IP address [80], MAC address, E.164 number, etc. Application identification: In fog platform this one is concerned with identifying the different applications, such as uniform resource locator (URL), domain name etc.

In terms of resolution technology, the Object Name Service (ONS), which is part of EPC global network is the most popularly used resolution service [81]. In fog computing, ONS is in sync and supports the mobility attribute. In their study, Hu et al. [43] advanced a fog computing entrenched framework of identification and resolution. It was found that it identified and resolved persons from their faces and, in the process, also preserved bandwidth and enhanced efficiency of processing. The method could also double up as a reference for non-ID verification.

### *3.4 Storage Technologies*

Let us look at the role pre-cache technology plays in fog computing to cater to the requirements of low-latency property. First, fog nodes anticipate the user's demand, then intuitively choose the most significant content to stash in the nodes that are geographically dispersed. Thus, the delay in downloading of contents from faraway websites or data centres can be substantially curtailed, enabling, in turn, applications on fog to fully exploit the storage resources to deliver to users optimum services [45].

In 5G wireless networks Bastug et al. [82] have propounded an ardent dedicated caching mechanism that would energetically, on its own, stash the sought-for information even prior to users asking for it. If this pre-catch scheme and stratagem can be incorporated in fog computing, it can come in handy in smart vehicular and traffic applications. The system could anticipate proactively the demands of drivers and stash them in edge devices and at base stations, thus significantly lessening traffic demands at peak times.

Additionally, it is worth noting that edge devices have constricted capacity for storage. So to enhance fog computing's overall service strengths, the technology of storage extension can prove very beneficial. In their study, Hassan et al. [47] have come up with the new concept of leveraging personal storage in mobile gadgets, as a method for storage extension that is secure and competent.

*3.5 Security and Privacy Protection*

Devices that use fog nodes, being near to end users, are carried to locations that may not be secure. Such devices could become vulnerable to unwarranted vicious assaults [83-84]. For instance, in the man-in-the-middle attack, essentially a data hijacking strategy, fog node devices could be switched virtually to being fake ones. This problem, though, could be effectively dealt with decryption and encryption approaches.

Another sensitive issue is the integrity and confidentiality of data. This issue arises because in fog computing, a widely dispersed platform, devices at the edge create huge volumes of data which, incidentally, have to be transmitted to fog nodes for storing and saving as well as for computing. Moreover, the fog nodes have to often interact with edge gadgets and data pools in cloud computing. All these complex operations render the data vulnerable to exposure and hacking. There is, however, a solution to tackle this problem. It is to simply employ masking techniques or light-weight encryption algorithms [85].

Additionally, in fog computing there are scores of areas where collaboration takes place. This can give rise to problems pertaining to privacy and safety. These problematic areas comprise authentication and authorisation, identity management, resource access control, securely distributed decision enforcement and collaboration, quality of security and service, sharing policy of information etc. [86-87]. To resolve the above issues, Dsouza et al. [60] put forth the idea of a resource management and access control system based on policy that would ensure among the diversified resources sought by users a safe partnership and interoperability between resources.

*3.5 Security and Privacy Protection*

Management of resources deserves paramount importance in fog computing, for arranging and leveraging fog services and resources. As has been noted, fog nodes and devices at the edge normally remain restricted in terms of energy. Therefore, how resources are managed and allocated has a direct impact on the performance and durability of fog network. To facilitate the process of mobility and low-latency in fog computing, the techniques of how resources are arranged and managed needs to be focused on, especially such factors as migration, placement, fog nodes, strengthening of devices and gadgets at edge, tasks, applications modules etc.

These factors have an adverse effect on periods of decision making and processing of latency. As against this, some solutions are suggested. For one, virtualisation of resources of fog nodes could spell a competent management way. For another, context-awareness technology can help in the leveraging of services and resources competently in fog computing. Moreover, the management of resources and energy within the ambit of context-awareness technology can ensure better use of resources and conserve energy [88].

In fog computing, resource discovery and sharing is crucial for the enhancement of performance of applications. It can naturally alternate between centralised and flooding modes, thus conserving energy in diversified networks. Liu et al. [89] propounded a robust way for resource discovery in mobile cloud computing. It can automatically transform between centralised and flooding strategies to save energy in diversified networks.

## 4. Applications

It is now established that fog computing especially serves well those applications that thrive on low latency [37,90]. That's why, in several areas that mandate low latency, such as urgent services, cyber physical systems, healthcare etc. fog computing has found enthusiastic favour. Below are listed certain applications that embrace fog computing:

### *4.1 Smart Environment*

Network forms the basis of IoT applications and smart dwelling scenarios. Without network both just cannot exist. IoT applications are created out of a number of processors and smart objects. Controllers, sensors, inter-connectors, processors and actuators all are classified as smart objects. In the network, it is the processors that manage, communicate and track smart objects.

Smart scenarios and environments such as smart home, smart city, main rely on cloud computing for their operation. Cloud servers facilitate smart objects to work in concert and to correlate and cooperate. The prominent feature of smart objects, however, is that they are universally dispersed. This gives rise to a crucial concern: speed or latency of data transfer between smart objects and the cloud, more so for applications that are finely attuned to latency needs. In order to surmount this glitch, the industry recently put forth the fog computing protocol that facilitates actual-time interaction among location-related services. Especially, the fog computing's local processing mode decreases substantially the amount of data being sent to the cloud.

To buttress the smart living scenario, Li et al [91] created a data-entrenched fog platform, which evaluates and administers the flow of data of similar applications such as smart office, smart healthcare, smart safety, smart entertainment, smart energy and others. Comparing how the applications performed in fog related and cloud related structures, they have confirmed that in applications of smart environment the fog related structure establishes ascendency. In their work, Jannuzzi et al [92], too, point out that for seamless operation of IoT the fog computing platform will be the most fitting structure. This is mainly because of some inherent and compounded demerits of cloud computing which is hobbled by concerns relating to scalability, dependable control and mobility.

### *4.2 Healthcare*

Healthcare is the one area in which fog computing based applications have been cited most often. In the past few years, a wide range of healthcare services and works relating to diagnosis, detection, health illnesses etc. have been propounded.

Talking about the attributes of fog computing, M. Yannuzzi et al. [16] and [93] stress on areas in healthcare where fog computing can be profitably employed.

In their work, Cao et al. [15] have put forth a system called FAST which in reality is a system of distributed analytics backed by fog computing to keep track of fall alleviation. In this protocol, they have included algorithms for identifying fall, and the system disseminates the analytics across the network through the separation of identifying task between the server and devices at the edge, which are basically phones that users carry.

In another initiative, M. Ahmad et al. [94] displayed Health Fog, a model in which fog computing is put to use as a connection link between the cloud and end users. The structure of Health Fog is

such that it lessens the cost arising out of added communication. In systems that are similar, this cost works out much higher.

### *4.3 Vehicular Fog Computing*

Smart vehicular systems rely on many sophisticated programmes and one of the pivotal amongst them is Vehicular Ad-hoc Networks(VANET). VANET ensure traffic efficiency, driving safety and convenience by exchanging valuable information. Basically, VANET excel in information exchange, and bring with it several benefits, such as driving safety, convenience, efficiency etc. VANET facilitate several mobile services which, among others, include data dissemination service that comes in handy during critical situations like emergencies, content-distributions applications that are useful for media, entertainments, advertisements etc.

In the past few years, VANET have witnessed phenomenal growth, no doubt aided by the advent of novel breakthroughs and development of equipment and technologies. At the same time, though, this advancement of technologies gave rise to a new concern: a mushrooming demand for information communication and greater capacity for computation. Newer applications have fostered expectations and demands. For instance, applications like self-driving, augmented reality (AR) that are based on processing of data and complicated storage workings now need more advanced degrees of communication, computational processes and storage capabilities.

Consequently, a new computing platform called Vehicular Fog Computing (VFC) has been advanced [95,54,25], precisely to fulfil the requirements of the above applications that have distinct additional needs of low latency, location pin-pointing and mobility.

Basically, VFC treats vehicles as a framework to effect computation and communication. As an architecture, VFC employs a shared collection of end-user clients or near-user edge devices and gadgets to effect communication and computation, utilising better each vehicle's individual in-built resources of computation and communication[21,25]. VFC incorporates the usual cloud features of storage, applications, computing as services to end clients. What, however, makes it distinctly different from other protocols is its backing for mobility, solid universal distribution and closeness to end users [25].

### *4.4 Augmented Reality, Brain Machine Interface and Gaming*

Augmented reality is a technology that combines virtual reality with the real world in the form of live video imagery that is digitally enhanced with computer-generated graphics. AR can be experienced through headsets that people wear and through displays on mobile devices.

Nowadays, scores of businesses are adopting Augmented Reality (AR) technology to sell their products and also produce eye-catching marketing and advertising strategies. Applications that rely on AR technology invariably require high bandwidth to transfer data, and high power computation to deliver live video streaming. This is mainly because even a very short duration delay or buffering like interruption can spoil the presentation for users and invite censure.

Thus for AR using applications, like some brain related ones in healthcare, low-latency is a must, and fog computing happens to be the best platform that could meet this condition. With fog computing's rich-resources and versatility, AT technology in conjunction with fog computing could curtail latency in transmission and process of computing, leading to the optimisation of throughput.

In their study, Zao et al [96] created a fog computing based computer interaction game that linked brain with data. As the person is playing, the data created by EEG head-set reveals the state of the player's brain and, in effect, serves to save time because the data does not have to be transmitted to main servers for processing. The system uses a blend of cloud and fog servers, allowing for non-stop actual-time processing and categorisation.

*4.5 Smart Energy Grid*

The energy grid is a power dissemination network; it uses smart meters at different areas to quantify the ongoing status data, as far as energy production, conveyance, utilisation and charging are concerned. Smart energy alludes to the utilisation of systems' administration advancements and IoT to progressively disseminate energy with a specific end goal to limit their cost and also expand energy, which includes basic leadership in terms of decision-making and a subsystem of action performing.

A main consolidated server called supervisory control and data acquisition (SCADA) framework accumulates and dissects the status data. Then, to balance the power grid, it transmits orders to react to any request for change or crisis. For instance, in the example of the biggest open utility in the US, the Los Angeles Smart Grid will cater to more than 4 million clients [44]. Smart meters linked to the Net keep a watch on power consumption in homes and factories and report them back intermittently, like clockwork, to the main controlling utility.

Thus, the smart grid, embedded in fog computing will transform into a many-layered structured framework with the interchange between the SCADA and the fog. In such framework, a fog is responsible for a miniaturised-grid and interacts with nearby fogs and at higher levels. The higher the layer, the bigger the latency, and the more extensive the geo-physical the reach.

*4.6 Fog in IoT and Cloud of Things*

The rise of IoT has made it hard to manage information in a powerful and proficient approach to generate helpful services. Diverse gadgets create distinctive kinds of information with various frequencies and distinctive sizes. Consequently, a combination of IoT and distributed computing, called as Cloud of Things (CoT) has recently been advocated[37].

On its part, CoT is found to encourage and help the administration of developing media content and other information. Other than this, highlights like benefit revelation, asset provisioning, pervasive access and administration creation assume a huge part, which accompanies CoT. Human services like crisis management, healthcare and services that depend on speed and accuracy mandate constant and actual-time reaction.

Likewise, it is imperative to choose what kind of information is to be transferred to the cloud, without over-burdening the system data transmission and the cloud. Therefore, Fog computing is relied upon to assume an essential part to achieve this job. Fog computing dwells fundamentally in-between the cloud and IoT. Its chief activity is to oversee assets, pre-processing, information filtration, and safety efforts.

For this reason, Fog needs a successful and effective asset administration system for IoT. A distinctive utilisation of fog computing lies in the Industrial Internet of Things (IIoT). Here, the machines and different sensors, gateways and actuators embedded in a production website can be utilised as fog system to expand the productivity [97].

*4.7 Storage Technologies*

The fog computing platform also serves as an extremely favourable mode for Urgent computing, such as, for instance, in providing backing for disaster related occurrences that require immediate evaluation, help and reactions. In this regard M. Aazam et al. [98] built up a support framework for making flood related decisions. This system employs fog nodes to process the obtained genuine information and trigger alerts in the event of flood occurrence.

Also, M. Aazam, E.-N. Huh et al. [99] exhibited E-HAMC (Emergency Help Alert Mobile Cloud) program that endeavours to react expeditiously to a demand of a client in the event of an emergency circumstance. Fog computing has been put to another use in the optimisation of web [100]. Any request made by the user on the web is initially processed through the fog or edge servers, which secure them later from the centre system or network where the web servers are located and then alter and locally store these documents. Thus, fog gadgets or devices can possibly be utilised as local storing and reserving points.

## 5. Security Issues and Challenges in Fog Computing

Fog computing gadgets and devices may confront genuine framework security concerns, since fog gadgets are normally used in places that are outside the ambit of safeguarding and observation. Subsequently, they wind up exposed to malicious assaults like information seizing and listening in that may jeopardise the working and systems of fog gadgets. Cloud computing is fortunately lucky to have myriad solutions, which might not be effective in case of fog computing, as the gadgets and devices that rely on fog computing operate at network's brink. This paper surveys some of the following security issues and challenges facing fog computing.

*5.1 Trust*

Trust assumes a noteworthy part in encouraging relations in light of past associations among fog nodes and edge gadgets. A fog node is regarded as the most crucial part as it is responsible for guaranteeing security and namelessness for end clients [28]. Additionally, this part should be trusted for carrying out its task, as they should be guaranteed that the fog node actualises the worldwide covering process on their discharged information and unleashes only non-threatening actions. This requires a certain degree of trust among all nodes that operate within the network of fog.

5.1.1. Collusion Deception

In their study, Wang et al. [101] contemplate about the trust plan in fog computing that incorporates what is called a system of public-subscribe (PSS) [102], to safeguard trust against concerted collusion assaults. In several big crucial systems like monitoring and checking of traffic, PSS has generally been used on a large-scale. Here, a non-specific broker based PSS protocol is presented[126], which shows a broker's part as being an essential piece of a PSS.

Brokers perform their work by interacting with publishers and subscribers, and harmonising the appropriate demands of users and then transferring the information of users [103]. They can be employed to separate interplay of users and offer communications that are not in sync. A malignant subscriber or publisher node that is programmed to retain other nodes' data content or encryption key hidden would intentionally release to the opposed brokers the hitherto concealed key.

Below are listed the ways in which malignant nodes and brokers are able to conspire with each other and divulge secrets:

- A malignant node offers crucial information of other users to a noxious broker that evaluates this information and
- The malignant broker offers information of other nodes to its colluders, so as to befool other users into thinking that the colluders are the appropriate entity.

Thus, it can be inferred that the brokers might be noxious and the fog faces conniving assaults. To diminish the security dangers and vulnerabilities, the examination [101] suggests content related PSS with varying protection in a fog setting that would guarantee the reliable working and delivery of publish and subscribe.

#### 5.1.2. Trust Middleware and Specimen

In their work, Elmisery et al. put forth a fog-based middleware, in which trust operators compute the estimated relational trust between the cloud and a fog node [28]. The calculation of trust is performed in a decentralised manner through the use of definition of entropy as spelt out in [104]. To obtain privacy for user, the nearby covering operator executes the neighbourhood camouflage procedure. The worldwide covering operator, just existing in a fog node, performs the worldwide disguise process on the collected client profile. To enhance and control trust [28], an administration and service tier is incorporated in the fog structure.

In their study, Soleymani et al. indicate that, to ensure dependability and integrity of applications, it is crucial to set up trust among vehicles [105]. In vehicular situations, a protected trust paradigm is able to manage vulnerabilities and taking of risks, arising out of untrustworthy data. But it is found that cars and other vehicles often accumulate, in addition to ambulatory and non-ambulatory obstacles, data that is simply wrong, deficient, uncertain and error-filled.

Thus, to beget a safe vehicular network, a fuzzy trust paradigm consolidated on involvement, experience and credibility is propounded [105]. It performs a progression of safety checks to guarantee the accuracy of data got from approved vehicles. Additionally, fog nodes are affiliated as an instrument to assess the degree of precision of the area of an occasion or event.

In this context, Koo et al. has presented a mixed secure paradigm that eliminates duplication by considering false fog saving and reserving scenarios [106]. For safeguarding of privacy, this work interjects a trusted third party (TPP) in the operation [107]. Pernicious assaults can render sensor interchanges deceptive and questionable. That's why, a trust assessment technique is a must to guarantee an unwavering quality relationship among sensors to oppose noxious assaults. Fog nodes are incorporated to enable the framework to figure out trust values [108].

#### 5.1.3. Area Based Trust

In the fog various physical gadgets exist at diverse areas having varied communication kinds and networking structures. Still, to deliver quicker reactions, fog nodes are equipped to offer both regional and local computation services. So, the question of how to achieve these objectives in concert with fog's attributes forms a study area for the future. To effect trust based interaction and communication between fog nodes at widely spread locales, Dang et al. have advanced a trust paradigm based on areas [109].

In this scenario, a fog node is chosen to designate computational asset administration and job execution in a locale. For instance, if node 2 in area A and node 4 in area B are chosen as designates, separately, designated nodes are utilised to figure out trust estimations or values for nodes in a similar area. So, for instance, if node 1 needs to get the trust estimation of node 3, it needs to acquire

it by means of node 2 in region A. And if node 1 desires to secure the trust value of node 5, it is required to get it through node 4 in area B. At the same time, they can also figure out their area trust estimations and transmit them to the cloud.

*5.2 Assault*

Devices and gadgets with fog nodes are carried to all sorts of places including those where protection is weak or absent. Hence they may face malevolent assaults [110]. Also, a noxious client can either record wrong or false readings, spoof IP locations and addresses or alter its own smart meter [111].

5.2.1. Malignant Nodes and their Assaults

Assaults from malignant Fog nodes: Lee et al. have analysed the parts and singular threats against security of IoT in fog [95]. As one of the potential dangers, the concern of a malignant fog node is far from trivial. Their study shows that fog nodes process in the fog the dense workload that is segmented into different tasks.

In their exploration, the substantial workloads in the Fog are separated into a few occupations and prepared by fog nodes. In the event that a portion of these nodes is assaulted by malignant clients, it is difficult to guarantee the security of the information. But the authors did not advance a solution about how to take care of such an assault. Z. Li, X. Zhou et al. [34] studied the growth of malignant nodes in the fog. They first probed, as a non-agreeable differential game, how malignant nodes and susceptible nodes interacted. Then they evaluated, broke down and figured out the process of decision making.

Assaults from malevolent edge gadgets of clients: For protection of information in the fog, it is crucial to pinpoint the edge gadgets and devices that have turned malignant. Still, it is hard to ward off the assault in view of the specific benefits conceded to them to utilise and process the information. In this context, Sohal et al. have suggested a structure by employing a Markov model, interruption identification framework and virtual honeypot gadget to take care of the issue [112].

5.2.2. MitM Assault

All the traffic and interaction between fog nodes and edge gadgets and devices are safeguarded by transfer channels that are safe and secure. Still, an outside attacker can spy on or change a client's discharged information before the fog node executes a worldwide disguising process [28]. MitM is such an endemic sort of assault.

The outside assailant effectively disturbs the OpenFlow channel and controls the entryway after executing the four stratagems mentioned below:

- For a gadget inside the IoT LAN, the outside aggressor can usurp control of it by propelling firmware upgrading assault, as the embedded smart gadgets are defenceless against assaults.
- The smart gadget then injects a customer endorsement in the fog node, falsely asserting that the fog node has to utilise this testament to reveal its identity in later interchanges.
- After the fog node implants the customer certificate, the outside aggressor severs the association between it and the controller.
- Finally, the aggressor executes MitM assault on the OpenFlow control channel.

In their research, C. Li, Z. Qin et al. [113] have discussed the safety concern of an OpenFlow channel between the controller and its operators in IoT fog. Since all the controller charges are sent through this channel, once assaulted, the system is totally manipulated by an aggressor. For both the

providers of network services and their clients it is a calamity. In this context, I. Stojmenovic et al. [114] advanced the antidote of utilising the Bloom filter to recognise MitM assault. In their study, Stojmenovic et al. have probed MitM assault and its covert features through the investigation of fog gadget's memory consumption and CPU [110]. One can likewise take care of the issue by making use of encryption and decryption [115].

*5.3 Access Control*

5.3.1. Quality Encryption

The fog evolves from and is a significant expansion of cloud computing. It is therefore natural that it acquires numerous safety difficulties relating to privacy of cloud computing. But many of the usual solutions of cloud computing come in handy in fog computing. For instance, the calculations, Rivest Shamir Adleman and Advanced Encryption Standard [116], the encryption solutions normally favoured, can be employed.

In their work, Fan et al. have called attention to the fact that, to gain control of data access in both cloud and fog platforms, Cipher content attribute based encryption (ABE) can come in handy [117].

Consequently, they propound a plan of entry control propped on outsourced multi-authority that can be verified. Cryptography based on attributes works as an outstanding innovation to ensure information secrecy and to control entry to fine-tuned information. The work [118] propounds a safe plan for control of fine-tuned data access combined with computation outsourcing and Cipher text update for IoT in fog computing. It can lessen cost of computation and ensure safe control of information access.

The framework comprises cloud servers, characteristic head, fog nodes and clients. For each fog node and server the attribute head generates a public key. It produces a hidden key, too, for each gadget and device at the edge from clients. The communication information is rendered in Cipher content for fog-to-fog and fog-to-cloud, while it is limited Cipher content for edge-to-fog.

Smart meters can encode and send the information to a fog gadget, like, for instance, a gateway of home-area network, then assemble the outcomes and lastly transmit them to the cloud, if required. Here, Jiang et al. call attention to the fact that some bothersome circumstances and the infringement of an entrance control approach can show up on the grounds that a client can produce another private key for the entrance right [119]. To take care of the issue, they suggest a technique to determine this issue by formalising security necessities and developing a characteristic based encryption (ABE) plan to fulfil the new security prerequisites.

To facilitate bona fide and personal communication among a bunch of fog nodes, Alrawais et al. put forth a proficient key trading paradigm formed on Cipher text-policy characteristics-based encryption (CP-ABE) to set up secure interchanges among members [119]. They fused together digital signature and CP-ABE protocols, to accomplish validation, privacy, access control and irrefutability. Together with a server that creates a key, the structure comprises segments like the key creating server, the cloud, IoT gadgets and fog nodes. The key creating server is employed to produce and circulate the keys among the included segments. The Cloud characterises an entrance structure to all fog nodes and executes the encryption to get Cipher content [120].

5.3.2. Behaviour Profiling

In their research, Mandlekar et al. draw attention to the fact that unapproved entry should be identified and genuine information ought to be preserved without getting hacked [40]. Subsequently, to match a user's behaviour with that of regular users for verification, they take recourse to the technology of behaviour profiling and decoy information.

*5.4 Safe Communication*

In communications there are two types [105] : 1) Communications between constricted-IoT gadgets or devices and fog nodes; and 2) Communications between fog nodes. There might be sham messages during communication when assaulters in the network send false data [121]. Mukherjee et al. aver that safety features ought to be powerful and adaptable in an asset-constricted fog scenario while data is being transmitted from the edge to the cloud [122]. For fog to cloud interactions and conversations they outline an irregular and adaptable end-to-end safety system for communications between fog and cloud.

It can manage problematic system associations and accomplish safety setups befitting various application requirements. In their work, Wang et al. suggest a plan to safeguard the identities of edge gadgets through the use of aliases and to ensure information concealment using a similar in form encryption method while transferring information from edge gadgets to the cloud [106].

*5.5 Privacy Safeguarding*

Privacy safeguarding is absolutely essential in the light of users' numerous worries about their delicate information [27]. Diverse protection safeguarding approaches, plans and techniques are put forth, particularly in healthcare area [28-30,123]. In the light of various advances, outlined below are certain related works.

5.5.1. Area Privacy Safeguarding

In the fog area privacy concerns remain a test [123]. With the assistance of the fog, area-based services, which are favoured by many, can accomplish low-latency. J. Kang, R. Yu et al. [124] in their study examined a privacy safeguarding protocol related to areas. In their work, Kang et al. dwell on area privacy concerns relating to fog backed Internet of Vehicles (IoV) that aspires to surmount problems like huge latency and mind-boggling expenses [107].

Consequently, a privacy safeguarding alias is introduced for management of viable nom de plume. The work [125] acknowledges directional privacy safeguarding propped up on the fog for cloud area services. The paper [126] exhibits a superfluous fog-circle based plan to safeguard the source-node area privacy and accomplish in the fog energy capability. The examination [124] suggests a positioned cryptography convention for saving area privacy. Fog nodes are particularly able to fulfil the necessities for area-particular applications and area-aware information administration, like in vehicular provisional networks [107, 125].

5.5.2. Other Privacy Safeguarding

In their work Du et al. point to the privacy issue that is in-built in a fog stage, and propose a differential privacy-based questionnaire model [127]. Wang et al. advance a privacy safeguarding plan by utilising differential privacy in the fog, which can at the same time guarantee clients' confidentiality and privacy [165].

On the other hand, R. Lu, K. Heung et al. [128] point out that most privacy saving information conglomeration plans bolster information aggregation for diversified IoT gadgets only and are not able to combine total hybrid IoT gadgets' information into a single unit. Consequently, a lightweight privacy saving information total plan for the fog-upgraded IoT is advanced.

In their study, Elmisery et al. examine and uncover the revelation limit amongst publicity and privacy as also between oneself and others [28]. On the other hand, Hu et al. advance a privacy protecting plan for distinguishing face by utilising the fog [129]. Fog-entrenched vehicular provisional network is another protocol that is beneficial for the fog and vehicular cloud, for which a safe and privacy-safeguarding navigation plan is propounded [130].

### *5.6. Others*

Service accessibility: It incorporates how to lessen denial of service (DOS). At the point when there are a large number of client demands for the same service, DOS happens if hackers exploit the situation for assaulting [131]. It is suggested that a novel plan for shielding DOS assaults [132] ought to be sought. Newer techniques should be thought of to prevent needless utilisation and wastage of resources and provide adequate reserving capacities to enhance the accessibility of services.

Secure applications: Meanwhile, Khan et al. abridge the potential security concerns found in the below listed fog applications: web advancement, virtualised radio access, smart meters, 5G portable systems, vehicular systems and street safety, medicinal services frameworks, sustenance traceability, observation video handling, discourse information, management of asset and resources, enlarged brain-PC interface, catastrophe response, energy decrease and unfriendly environments [21].

Because not all fog nodes are replete with resources, heavy applications that need resource-constricted nodes are not exactly simple as contrasted with traditional information centrals. Such hot applications chiefly centre around vehicles [124,105,133-134] and healthcare [135,27]. Encoding critical information can enhance the safety of the applications while conjuring APIs. At the same time, if an excessive number of APIs are conjured and conveyed, they may devour an excessive number of assets, thus adversely impacting typical access to them and even causing the application system to become immobile.

Secure sharing innovation: This happens when the data is shared among numerous websites [28], such as harmonious coordination between fog nodes and services. For sharing of services in the fog social networks can be innovatively utilised. In the social fog, to endorse security services correctly together with a mechanism that facilitates crowd sensing, an innovative model of provision of security service has been advanced [136].

## 6. Conclusion

Fog computing is a vibrant computing protocol that assumed prominence and witnessed fast growth with the advent of mobile internet, CPS and Internet of Things (IoT). An exceptionally virtualised fabric, fog computing is not deemed as a substitution for cloud computing. Fog computing is the platform that spreads from the outer brinks of where information is produced to the point where it will ultimately be saved and stored. The information might end up getting stored in a user's information centre or in the cloud itself.

Fog computing is a multi-tier distributed network platform for edge gadgets and devices. This makes it possible for an increasing number of services, uses and applications to be shifted from the

cloud. For devices that are at the edge and for conventional depositories of cloud computing information, fog computing makes available several services, such as networking, saving and storage and data processing [137]. In its working fog computing confers myriad benefits: it enormously lessens the time of information exchange and the volume of system transmission. It also more than adequately fulfils the requirements of actual-time or latency-demanding applications and renders barriers related to bandwidth of networks easy to surmount [138].

For all its positive features, though, fog computing becomes susceptible and defenceless against security dangers and attacks, precisely because of the nature of its dispersed and open architecture. This comprehensive and wide-ranging survey takes a detailed look at fog computing, encompassing its several prominent features, from its architecture, characteristics, relevant technologies involved to various applications it supports to the security, trust and other issues linked with it. As has been noted earlier, unlike the cloud which is a centralised entity, fog computing, because of its vulnerable features of wide distribution and remote operability, can become exposed to newer security threats and challenges.

In view of the above, it is pertinent to take note of certain recommendations. Firstly, we require new techniques. Fog is a widely dispersed platform. Therefore, executing safety and security protocols to achieve integrity of data might adversely impact to a large extent its quality of service (QoS). Consequently, we have to discover new techniques to enhance the security and trust issues of the Fog.

Secondly, we require newer interfaces. Since fog nodes are required to collaborate with various hardware entities supplied by various sellers, new interfaces are a must to guarantee computing processes that can be relied upon.

Thirdly, we need new conventions or protocols. There are already some protocols designed and put in place, like the ones in [139-141]. But new protocols that would on their own discover instances of trust and safety endangerments are sorely missing in the current structure of the fog. Hence, it is imperative to come up with a new set of counter-steps to guard against trust and safety related breaches [142].

## References

1. L. Atzori, A. Iera, G. Morabito. The internet of things: A survey. *Computer Networks*. **2010,** 54 (15), 2787–2805, doi:10.1.1.719.9916.
2. H. Ning, H. Liu, J. Ma, L. T. Yang, R. Huang. Cybermatics: Cyber physical social thinking hyperspace-based science and technology. *Future Generation Computer Systems*. **2016,** 56, 504–522, doi: http://dx.doi.org/10.1016/j.future.2015.07.012.
3. D. Evans. The internet of things: How the next evolution of the internet is changing everything. CISCO White Paper 1, **2011**, 1–11.
4. Cisco global cloud index: Forecast and methodology. **2016-2018** white paper.
5. R. Cortes, X. Bonnaire, O. Marin, P. Sens. Stream processing of healthcare sensor data: Studying user traces to identify challenges from a big data perspective. Procedia Computer Science. **2015,** 52 (1), 1004–1009, doi: 10.1016/j.procs.2015.05.093.
6. Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, Y. Li. Cost-efficient strategies for restraining rumor spreading in mobile social networks. *IEEE Transactions on Vehicular Technology*. **2017**, 66 (3), 2789–2800, doi: 10.1109.TVT.2016.2585591.
7. M. H. Ghahramani, M. C. Zhou, and C. T. Hon. Toward Cloud Computing QoS Architecture: Analysis of Cloud Systems and Cloud Services. *IEEE/CAA Journal of Automatica Sinica*. **2017**, Vol. 4, No. 1, pp. 5-17, doi: 10.1109./JAS.2017.7510313.

8. Y. Xia, M. Zhou, X. Luo, and Q. Zhu. Stochastic Modeling and Quality Evaluation of Infrastructure-as-a-Service Clouds. *IEEE Trans. on Automation Science and Engineering*. **2015**, 12(1), pp. 160-172, doi: 10.1109./TASE.2013.2276477.
9. H. Yuan, J. Bi, W. Tan, M. C. Zhou, B. H. Li, and J. Li. "TTSA: An Effective Scheduling Approach for Delay Bounded Tasks in Hybrid Clouds." *IEEE Transactions on Cybernetics*. **2017**, vol.47, no. 11, , pp. 3658– 3668, doi:10.1109/TCYB.2016.2574766.
10. P. Y. Zhang and M. C. Zhou. Dynamic Cloud Task Scheduling Based on a Two-stage Strategy. *IEEE Transactions on Automation Science and Engineering*. **2018**, 15(2), 772-783, DOI: 10.1109/TASE.2017.2693688.
11. W. B. Zheng, M. C. Zhou, Y. N. Xia, L. Wu, Xin Luo, S. C. Pang, and Q. S. Zhu. Percentile performance estimation of unreliable IaaS clouds and their cost-optimal capacity decision. *IEEE ACCESS*. **2017**, Vol. 5, pp. 2808 – 2818, doi:10.1109/ACCESS.2017.2666793.
12. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica. A view of cloud computing. *Comm of the Acm*. **2010**, 53 (4), 50–58, doi:10.1145/1721654.1721672.
13. N. Fernando, S. W. Loke, W. Rahayu. Mobile cloud computing: A survey. *Future Generation Computer Systems*. **2013**, 29 (1), 84106.1070, doi: https://doi.org/10.1016/j.future.2012.05.023.
14. T. Qiu, R. Qiao, D. Wu. Eabs: An event-aware backpressure scheduling scheme for emergency internet of things. *IEEE Transactions on Mobile Computing*. **2017,** 17(1), 72-84, doi:10.1109/TMC.2017.2702670.
15. Y. Cao, S. Chen, P. Hou, D. Brown, Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation, in: IEEE International Conference on Networking, Architecture and Storage, **2015**, pp. 2–11, doi: 10.1109/NAS.2015.7255196.
16. V. Stantchev, A. Barnawi, S. Ghulam, J. Schubert, G. Tamm. Smart items, fog and cloud computing as enablers of servitization in healthcare. *Sensors & Transducers*. **2015**, 185 (2), 121–128.
17. T. Qiu, K. Zheng, H. Song, M. Han, B. Kantarci. A local-optimization emergency scheduling scheme with self-recovery for smart grid. *IEEE Transactions on Industrial Informatics*. **2017**, 13(6), 3195-3205, doi:10.1109/TII.2017.2715844.
18. H. R. Arkian, A. Diyanat, A. Pourkhalili. Mist: Fog-based data analytics scheme with cost-efficient resource provisioning for iot crowdsensing applications. *Journal of Network & Computer Applications*. **2017**, 82, 152–165, doi:10.1016/j.jnca.2017.01.012.
19. G. Luo and Y. Pan, ZTE Communications Special Issue on Cloud computing, Fog computing, and Dew computing. *ZTE Communications*. **2017,** 15(1) 2.
20. T. H. Luan, L. Gao, Z. Li, L. Sun. Fog computing: Focusing on mobile users at the edge, arXiv preprint arXiv:1502.01815. **2015**.
21. F. Bonomi. i Connected vehicles, the Internet of Things, and Fog computing, in Proc. VANET, Las Vegas, CA, USA, **2011**, 13-15.
22. S. Yi, Z. Hao, Z. Qin, Q. Li. Fog computing: Platform and applications, in: 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies, **2015**, pp. 73–78.
23. S. Ivan and W. Sheng. The Fog Computing Paradigm Scenarios and Security Issues, in Proc. of the 2014 Federated Conference on Computer Science and Information Systems. **2014**, 1-8.
24. S. Khan, S. Parkinson, and Y. Qin. Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing: Advances, Systems and Applications*. **2017**, 6(19), DOI 10.1186/s13677-017-0090-3.
25. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the Internet of Things, in Proc. of MCC'12. **2012**,13-15.
26. S. K. Datta, C. Bonnet, J. Haerri. Fog computing architecture to enable consumer centric internet of things services, in: International Symposium on Consumer Electronics, **2015**, pp. 1–2
27. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog computing Facility with Pairing-Based Cryptography. IEEE Access. **2017**, 5, 22313-22328 DOI:10.1109/ACCESS. 2017.2757844.
28. A. M. Elmisery, S. Rho, and D. Botvich. A Fog Based Middleware for Automated Compliance with OECD Privacy Principles in Internet of Healthcare Things. *IEEE Access*. **2016**, 4, 8418-8841, doi:10.1109/ACCESS.20162631546.
29. S. R. Moosavia, T. N. Gia, E. Nigussie, A. M. Rahmania, S. Virtanen, H. Tenhunena, and J. Isoaho. End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Systems*. 2016, 64, 108-124, doi:https://doi.org/10.1016/j.future.2016.02.020.
30. X. Liu, R. H. Deng, Y Yang, H. N. Tran, and S. Zhong. Hybrid Privacy-preserving Clinical Decision Support System in Fog-cloud Computing. *Future Generation Computer Systems*. 2018, 78, 825-837, 2018, doi:https://doi.org/10.1016/j.future.2017.03.018.

31. B. Tang, Z. Chen, G. Hefferman, S. Pei, T. Wei, H. He, and Q. Yang. Incorporating Intelligence in Fog computing for Big Data Analysis in Smart Cities. *IEEE Trans. on Industrial Informatics*. **2017**, 13(5), 2140-2150, doi:10.1109/TII.2017.2679740 .
32. B. Molina, C. E. Palau, G. Fortino, A. Guerrieri, and C. Savaglio. Empowering smart cities through interoperable Sensor Network Enablers, in Proc. of 2014 IEEE International Conference on Systems, Man and Cybernetics (SMC), IEEE. **2014** ,7-12.
33. F. Cicirelli, A. Guerrieri, G. Spezzano, and A. Vinci. An edge-based platform for dynamic Smart City applications, *Future Generation Computer Systems*. **2017**, Volume 76, pp. 106-118, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2017.05.034, 2017.
34. Z. Li, X. Zhou, Y. Liu, H. Xu, and L. Miao. A Non-Cooperative Differential Game-Based Security Model in Fog computing. *China Communications*. **2017**, 14(1), 180-189, doi:10.1109/CC.2017.7839768.
35. V. Sharma,J. D. Lim, J. N. Kim, and I. You. SACA: Self-Aware Communication Architecture for IoT Using Mobile Fog Servers. *Mobile Information Systems*. **2017**, 1-17, https://doi.org/10.1155/2017/3273917.
36. H. Zhang, Y. Xiao, S. Bu, D. Niyato, R. Yu, Z. Han. Fog computing in multi-tier data center networks: A hierarchical game approach, in: 2016 IEEE International Conference on Communications (ICC), **2016**, pp. 1–6.
37. M. Aazam, E. N. Huh. Fog computing: The cloud-iot/ioe middleware paradigm. *IEEE Potentials*. **2016**, 35 (3), 40–44, doi:10.1109/MPOT.2015.2456213.
38. G. Fortino, A. Guerrieri, W. Russo, and C. Savaglio. Integration of agent-based and cloud computing for the smart objects-oriented IoT, in Proc. of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design, IEEE. **2014**.
39. C. C. Byers. Architectural Imperatives for Fog computing: Use Cases, Requirements, and Architectural Techniques for Fog-Enabled IoT Networks. *IEEE Communications Magazine*. **2017**, 55(8), 14-20, doi:10.1109/MCOM.2017.1600885.
40. M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar. Security and Privacy in Fog computing: Challenges. *IEEE Access*. **2017**, 5, 19293-19304, DOI:10.1109/ACCESS.2017.2749422.
41. S. Sarkar, S. Misra. Theoretical modelling of fog computing: a green computing paradigm to support iot applications. *IET Networks*. **2016**, 5 (2), 23–29, doi:10.1049/iet-net.2015.0034.
42. J. Shi, J. Wan, H. Yan, H. Suo. A survey of cyber-physical systems, in: 2011 International Conference on Wireless Communications and Signal Processing (WCSP), **2011**, pp. 1–6.
43. P. Hu, H. Ning, T. Qiu, Y. Zhang, X. Luo. Fog computing based face identification and resolution scheme in internet of things. *IEEE Transactions on Industrial Informatics*. **2017**, 13 (4), 1910–1920.
44. P. Varshney, Y. Simmhan. Demystifying fog computing: Characterizing architectures, applications and abstractions. arXiv preprint arXiv:1702.06331. **2017**, 1–23.
45. T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, L. Sun. Fog computing: Focusing on mobile users at the edge. *Computer Science*. arXiv.1502.01815. **2015**, 1–11.
46. M. S. Hossain, M. Atiquzzaman. Cost analysis of mobility protocols. *Telecommunication Systems*. **2013**, 52 (4), 2271–2285, doi: https://doi.org/10.1007/s11235-011-9532-2.
47. M. A. Hassan, M. Xiao, Q. Wei, S. Chen. Help your mobile applications with fog computing, in: IEEE International Conference on Sensing, Communication, and Networking - Workshops, **2015**, pp. 1–6
48. F. Bonomi, R. Milito, P. Natarajan, J. Zhu. Fog Computing: A Platform for Internet of Things and Analytics. Springer International Publishing. **2014**.
49. K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwlder, B. Koldehofe. Mobile fog: a programming model for large-scale applications on the in ternet of things, in: ACM SIGCOMM Workshop on Mobile Cloud Computing, **2013**, pp. 15–20.
50. K. Kang, C. Wang, T. Luo. Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues. *Journal of China Universities of Posts & Telecommunications*. **2016**, 23 (2), 56–96, doi: https://doi.org/10.1016/S1005-8885(16)60021-3.
51. Y. Zhang, D. Niyato, P. Wang, I. K. Dong. Optimal energy management policy of mobile energy gateway. *IEEE Transactions on Vehicular Technology*. **2016**, 65 (5), 3685–3699, doi:10.1109/TVT.2015.2445833.
52. F. Bonomi, R. Milito, P. Natarajan, J. Zhu. Fog Computing: A Platform for Internet of Things and Analytics, Springer International Publishing, **2014**, 169-186, doi:10.1007/978-3-319-05029-4_7.
53. C. Dsouza, G. J. Ahn, M. Taguinod. Policy-driven security management for fog computing: Preliminary framework and a case study, in: IEEE International Conference on Information Reuse and Integration, **2015**, pp. 16–23.

54. J. Oueis, E. C. Strinati, S. Sardellitti, S. Barbarossa. Small cell clustering for efficient distributed fog computing: A multi-user case, in: 2015 IEEE 82nd Vehicular Technology Conference (VTC Fall), **2015**, pp. 1–5.
55. K. Intharawijitr, K. Iida, H. Koga. Analysis of fog model considering computing and communication latency in 5g cellular networks, in: IEEE International Conference on Pervasive Computing and Communication Workshops, **2016**, pp. 1–4.
56. X. Zheng, Z. Cai, J. Li, H. Gao. A study on application-aware scheduling in wireless networks. *IEEE Transactions on Mobile Computing*. **2017**, 16 (7), 1787–1801 doi:10.1109/TMC.2016.2613529.
57. W. Gao, Opportunistic peer-to-peer mobile cloud computing at the tactical edge, in: IEEE Military Communications Conference, **2014**, pp. 1614–1620.
58. R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*. **2015**, 18 (1), 236–262, doi:10.1109/COMST.2015.2477041.
59. B. Han, V. Gopalakrishnan, L. Ji, S. Lee. Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*. **2015**, 53 (2), 90–97, doi:10.1109/MCOM.2015.7045396.
60. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*. 16 (3) (2014) 1617–1634, doi:10.1109/SURV.2014.012214.00180.
61. D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, S. Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*. 2014, 103 (1), 10–13, doi:10.1109/JPROC.2014.2371999.
62. H. Kim, N. Feamster. Improving network management with software defined networking. *IEEE Communications Magazine*. **2013**, 51 (2), 114–119, doi:10.1109/MCOM.2013.6461195.
63. A. Natraj. fog computing focusing on users at the edge of internet of things. *International Journal of Engineering Research*. **2016**, 5 (5), 1004–1155.
64. N. B. Truong, G. M. Lee, Y. Ghamri-Doudane. Software defined networking-based vehicular adhoc network with fog computing, in: IFIP/IEEE International Symposium on Integrated Network Management, **2015**, pp. 1202–1207.
65. M. Peng, Y. Li, Z. Zhao, C. Wang. System architecture and key technologies for 5g heterogeneous cloud radio access networks. *IEEE Network*, **2014**, 29 (2), 6–14, doi:10.1109/MNET.2015.7064897.
66. M. Chen, Y. Zhang, Y. Li, S. Mao. Emc: Emotion-aware mobile cloud computing in 5g. *IEEE Network*. **2015**, 29 (2), 32–38, doi:10.1109/MNET.2015.7064900.
67. D. Amendola, N. Cordeschi, E. Baccarelli. Bandwidth management vms live migration in wireless fog computing for 5g networks, in: IEEE International Conference on Cloud Networking, **2016**, pp. 21–26.
68. M. Peng, S. Yan, K. Zhang, C. Wang. Fog-computing-based radio access networks: issues and challenges. *IEEE Network*. **2015**, 30 (4), 46–53 doi:10.1109/MNET.2016.7513863.
69. R. P. Davey, D. Grossman, M. Rasztovitswiech, D. B. Payne, D. Nesset, A. E. Kelly, A. Rafel, S. Appathurai, S. H. Yang. Long-reach passive optical networks. *Journal of Lightwave Technology*. **2009**, 27 (3), 273–291.
70. W. Zhang, B. Lin, Q. Yin, T. Zhao. Infrastructure deployment and optimization of fog network based on microdc and lrpon integration. *Peer-to-Peer Networking and Applications*. **2017**, 10 (3), 579–591, doi:10.1007/s12083-016-0476-x.
71. C. Papagianni, A. Leivadeas, S. Papavassiliou. A cloud-oriented content delivery network paradigm: Modeling and assessment. *IEEE Transactions on Dependable & Secure Computing*. **2013**, 10 (5), 287–300, doi:10.1109/TDSC.2013.12.
72. Coile, D. In, D. O'Mahony. Accounting and accountability in content distribution architectures: A survey. *ACM Computing Surveys*. **2015**, 47 (4), 59:1–59:35, doi:10.1145/2723701.
73. Z. U. A. Jaffri, Z. Ahmad, M. Tahir. Named data networking (ndn), new approach to future internet architecture design: A survey. *International Journal of Informatics and Communication Technology*. **2013**, 2(3), 155–165, doi: http://dx.doi.org/10.11591/ij-ict.v2i3.5122.
74. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Clafy, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang. Named data networking. *Acm Sigcomm Computer Communication Review*. **2014**, 44 (3), 66–73.
75. D. Raychaudhuri, K. Nagaraja, A. Venkataramani. MobilityFirst: a robust and trustworthy mobility-centric architecture for the future internet. *AcmSigmobile Mobile Computing & Communications Review*. **2012**, 16 (3), 2–13, doi:10.1145/2412096.2412098.
76. P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, A. K. Sangaiah. A unified face identification and resolution scheme using cloud computing in internet of things. *Future Generation Computer Systems*. **2018**, 81, 582-592, doi:10.1016/j.future.2017.03.030.

77. H. Ning, Y. Fu, S. Hu, H. Liu. Tree-code modeling and addressing for non id physical objects in the internet of things. *Telecommunication Systems*. **2015**, 58 (3), 195–204, doi: https://doi.org/10.1007/s11235-014-9867-6.
78. N. Koshizuka, K. Sakamura. Ubiquitous id: standards for ubiquitous computing and the internet of things. *IEEE Pervasive Computing*. **2010**, (4), 98–101, doi:10.1109/MPRV.2010.87.
79. D. L. Brock, The electronic product code (epc), Auto-ID Center White Paper MIT-AUTOID-WH-002. **2001**, 1–21.
80. S. Hong, D. Kim, M. Ha, S. Bae, S. J. Park, W. Jung, J.-E. Kim. Snail: an ip-based wireless sensor network approach to the internet of things. *IEEE Wireless Communications*. **2010**, 17(6), 34–42, doi:10.1109/MWC.2010.5675776.
81. B. Ning, G. Li, Y. Chen, D. Qu. Distributed architecture of object naming service, in: Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009), **2012**, pp. 251–257.
82. E. Bastug, M. Bennis, M. Debbah. Living on the edge: The role of proactive caching in 5g wireless networks. *IEEE Communications Magazine*. **2014**, 52 (8), 82–89, doi:10.1109/MCOM.2014.6871674.
83. P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, X. Yao. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal*. **2017**, 4(5), 1143-1155, doi:10.1109/JIOT.2017.2659783.
84. T. Qiu, A. Zhao, F. Xia, W. Si, D. O. Wu. Rose: Robustness strategy for scale-free wireless sensor networks. *IEEE/ACM Transactions on Networking*. **2017**, 25(5), 2944-2959, doi:10.1109/TNET.2017.2713530.
85. K. Lee, D. Kim, D. Ha, U. Rajput. On security and privacy issues of fog computing supported internet of things environment, in: International Conference on the Network of the Future, **2015**, pp. 1–3.
86. U. S. Premarathne, I. Khalil, M. Atiquzzaman. Secure and reliable surveillance over cognitive radio sensor networks in smart grid. *Pervasive & Mobile Computing*. **2015**, 22(C), 3–15, doi:10.1016/j.pmcj.2015.05.001.
87. N. Yaakob, I. Khalil, H. Kumarage, M. Atiquzzaman, Z. Tari. By-passing infected areas in wireless sensor networks using bpr, *IEEE Transactions on Computers*. **2015**, 64 (6), 1594–1606, doi:10.1109/TC.2014.2345400.
88. V. Sharma, F. Song, I. You, M. Atiquzzaman. Energy efficient device discovery for reliable communication in 5g-based iot and bsns using unmanned aerial vehicles. *Journal of Network and Computer Applications*. **2017**, 97, 79-95, doi:https://doi.org/10.1016/j.jnca.2017.08.013.
89. W. Liu, T. Nishio, R. Shinkuma, T. Takahashi. Adaptive resource discovery in mobile cloud computing. *Computer Communications*, **2014**, 50 (13), 119–129, doi:10.1016/j.comcon.2014.02.006.
90. A. V. Dastjerdi, R. Buyya. Fog computing: Helping the internet of things realize its potential, *Computer*. **2016**, 49 (8), 112–116, doi:10.1109/MC.2016.245.
91. J. Li, J. Jin, D. Yuan, M. Palaniswami, K. Moessner. Ehopes: Data centered fog platform for smart living, in: Telecommunication Networks and Applications Conference, **2015**, pp. 308–313.
92. M. Yannuzzi, R. Milito, R. Serral-Gracia, D. Montero. Key ingredients in an iot recipe: Fog computing, cloud computing, and more fog computing, in: IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, **2014**, pp. 325–329.
93. Y. Shi, G. Ding, H. Wang, H. E. Roman. The fog computing service for healthcare, in: International Symposium on Future Information and Communication Technologies for Ubiquitous Healthcare, **2015**, pp. 70–74.
94. M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong, S. Lee. Health fog: a novel framework for health and wellness applications. *Journal of Supercomputing*. **2016**, 72 (10), 3677-3695, doi: doi:10.1007/s11227-016-1634-x.
95. X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, S. Chen. Vehicular fog computing: A viewpoint of vehicles as the infrastructures. *IEEE Transactions on Vehicular Technology*. **2016**, 65 (6), pp.3860–3873, doi:10.1109/TVT.2016.2532863.
96. J. K. Zao, T. T. Gan, C. K. You, E. C. Cheng, Y. T. Wang, T. Mullen, T. P. Jung. Augmented brain computer interaction based on fog computing and linked data, in: International Conference on Intelligent Environments, **2014**, pp. 374–377.
97. T. Zhu, S. Dhelim, Z. Zhou, S. Yang, H. Ning. An architecture for aggregating information from distributed data nodes for industrial internet of things. *Computers & Electrical Engineering*. **2017**, 58, 337–349, doi: https://dx.doi.org/10.10.1016/j.compeleceng,2016.08.018.
98. R. Brzoza-Woch, M. Konieczny, B. Kwolek, P. Nawrocki, T. Szyd lo, K. Zielin´ski. Holistic approach to urgent computing for flood decision support. *Procedia Computer Science*. **2015**, 51, 2387–2396.
99. M. Aazam, E.-N. Huh. E-hamc: Leveraging fog computing for emergencyalert service, in: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), **2015**, pp.518–523.

100. J. Zhu, D. S. Chan, M. S. Prabhu, P. Natarajan, H. Hu, F. Bonomi. Improving web sites performance using edge servers in fog computing architecture, in: 2013 IEEE Seventh International Symposium on Service Oriented System Engineering, **2013**, pp. 320–323
101. Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin. PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme With Differential Privacy in Fog computing. *IEEE Access.* 5(2017)17962-17986, doi:10.1109/ACCESS.2017.2748956.
102. C. Esposito and M. Ciampi. On security in publish/subscribe services: A survey. *IEEE Commun. Surveys Tuts*. **2014**, 17 (2), pp. 966-997, doi:10.1109/COMST.2014.2364616.
103. E. Onica, P. Felber, H. Mercier, and E. Riviére. Confidentiality-preserving publish/subscribe: A survey. *ACM Comput. Surv*. **2016**, 49(2), 1-41, doi:10.1145/2940296.
104. H. D. Kim. Applying consistency-based trust definition to collaborative filtering. *KSII Trans. Internet Inf. Syst*. **2009**, 3(4), 366-374.
105. S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi. A Secure Trust Model based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog computing. *IEEE Access*. **2017**, 99, 1-10, doi:10.1109/ACCESS.2017.2733225.
106. D. Koo, Y. Shin, J. Yun, and J. Hur. A Hybrid Deduplication for Secure and Efficient Data Outsourcing in Fog computing, in Proc. of 2016 IEEE 8th International Conference on Cloud Computing Technology and Science. **2016**, 285-293.
107. T. Wang, J. Zeng, M. D. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong. Trajectory Privacy Preservation Based on a Fog Structure for Cloud Location Services. *IEEE Access*. **2017**, 5, 7692-7701, doi:10.1109/ACCESS.2017.2698078.
108. T. Wang, Y. Li, Y. Chen, H. Tian, Y. Cai, W. Jia, and B. Wang. Fog-Based Evaluation Approach for Trustworthy Communication in Sensor-Cloud System. *IEEE Communications Letters*. **2017**, 14(8), 1-4, doi:10.1109/LCOMM.2017.2740279.
109. T. D. Dang, D. Hoang. A Data Protection Model for Fog Computing. 2017 Second International Conference on Fog and Mobile Edge computing (FMEC). **2017**, pp.32-38.
110. P. Hua, S. Dhelima, H. Ning, and T. Qiu. Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications*. **2017**, 98, 27-42.
111. I. Stojmenovic and S. Wen. The Fog computing paradigm: Scenarios and security issues, in Proc. 2014 Federated Conference on Computer Science and Information Systems (FedCSIS). **2014**.
112. 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*. **2017**, 1-15, doi: http://dx.doi.org/10.1016/j.cose.2017.08.016.
113. C. Li, Z. Qin, E. Novak, and Q. Li. Securing SDN Infrastructure of IoT-Fog Network from MitM Attacks. *IEEE Internet of Things Journal*. **2017**, 1-8, doi:10.1109/JIOT.2017.2685596.
114. I. Stojmenovic, S. Wen, X. Huang, and H. Luan. An overview of Fog computing and its security issues, Concurrency and Computation: Practice and Experience. **2015**, 28(10), 2991-3005, doi:10.1002/cpe.3485.
115. H. W. Kim, J. H. Kim, J. H. Park, and Y. S. Jeong. Time pattern locking scheme for secure multimedia contents in human-centric device. *The Scientific World Journal*. **2014**, 1-9, DOI:10.1155/2014/796515.
116. K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang. A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing. *Sensors*. **2017**, 17(7), 1965, DOI:10.3390/s17071695.
117. Q. Huang, Y. Yang, and L. Wang. Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog computing for Internet of Things. *IEEE Access*. **2017**, 12941-12950, doi:10.1109/ACCESS.2017.2727054.
118. Y. Jiang, W. Susilo, Y. Mu, and F. Guo. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*. **2018**, 78(P2), 720-729, doi:10.1016/j.future.2017.01.026.
119. A. Alrawais, C. Hu, and X. Cheng. An Attribute-Based Encryption Scheme to Secure Fog Communications. *IEEE Access*. 2017, 5, doi:10.1109/ACCESS.2017.2705076.
120. V. G. Mandlekar, V. K. Mahale, S. S. Sancheti, and M. S. Rais. Survey on Fog computing Mitigating Data Theft Attacks in Cloud. *International Journal of Innovative Research in Computer Science & Technology*. **2014**, 2(6), 13-16.
121. B. Mukherjee, R. L. Neupane, and P. Calyam. End-to-End IoT Security Middleware for Cloud-Fog Communication. 2017 IEEE 4th International Conference on Cyber Security and Cloud computing. **2017**, 151-156.
122. H. Wang, Z. Wang, and J. Domingo-Ferrer. Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Generation Computer Systems*. **2018**, 78, 712-719, doi:10.1016/j.future.2017.02.032.

123. X. Yang, F. Yin, and X. Tang. A Fine-Grained and Privacy-Preserving Query Scheme for Fog computing-Enhanced Location-Based Service. *Sensors*. **2017**, 17(7), 1-14, DOI:10.3390/s17071611.
124. J. Kang, R. Yu, X. Huang, and Y. Zhang. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles. *IEEE Trans. on Intelligent Transportation Systems*. **2018**, 19(8), 2627-2637, doi:10.1109/tits.2017.2764095.
125. M. Dong, K. Ota, and A. Liu. Preserving Source-Location Privacy through Redundant Fog Loop for Wireless Sensor Networks, 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous computing and Communications; Dependable, Autonomic and Secure computing; Pervasive Intelligence and computing. **2015**, pp.1835-1842.
126. R. Yang, Q. Xu, M.H. Au, Z. Yu, H. Wang, and L. Zhou. Position based cryptography with location privacy: A step for Fog computing. *Future Generation Computer Systems*. **2018**, 78, 799-806.
127. M. Du, K. Wang, X. Liu, S. Guo, and Y. Zhang. A Differential Privacy-based Query Model for Sustainable Fog Data Centers. *IEEE Transactions on Sustainable computing*. **2017**, 1-1, doi:10.1109/tsusc.2017.2715038.
128. R. Lu, K. Heung, A. Lashkari, and A. Ghorbani. A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog computing-Enhanced IoT. *IEEE Access*. **2017**, 5, 3302-3312, doi:10.1109/ACCESS.2017.2677520.
129. P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao. Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog computing in Internet of Things. *IEEE Internet of Things Journal*. 2016, 4(5), 1143-1155, DOI 10.1109/JIOT.2017.2659783.
130. L. Wang, G. Liu, and L. Sun. A Secure and Privacy-Preserving Navigation Scheme Using Spatial Crowdsourcing in Fog-Based VANETs. *Sensors*. **2017**, 17(4), DOI:10.3390/s17040668.
131. R. Rios, R. Roman, J. A. Onieva, and J. Lopez, From Smog to Fog: A Security Perspective, 2017 Second International Conference on Fog and Mobile Edge computing (FMEC). **2017**, 56-61.
132. J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen. Secure intelligent traffic light control using fog computing. *Future Generation Computer Systems*. **2018**, 78(P2), 817-824, doi:10.1016/j.future.2017.02.017.
133. S. Basudan, X. Lin, and K. Sankaranarayanan. A Privacy-Preserving Vehicular Crowdsensing-Based Road Surface Condition Monitoring System Using Fog computing. *IEEE Internet of Things Journal*. **2017**, 4(3), 772-782, doi:10.1109/JIOT.2017.2666783.
134. J. Ni, A. Zhang, X. Lin, and X. Shen. Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing. *IEEE Access*. 2017, 5, 19293-19304, DOI:10.1109/ACCESS.2017.2749422.
135. J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan. FCSS: Fog-computing-based Content-Aware Filtering for Security Services in Information-Centric Social Networks. *IEEE Transactions on Emerging Topics in computing*. **2017**, 1-1, DOI:10.1109/TETC. 2017.2747158.
136. Cloud Security Alliance, Top Threat to Cloud computing V1.0, **2010**.
137. J. Wu, Z. Su, S. Wang, and J. Li. Crowd Sensing-Enabling Security Service Recommendation for Social Fog Computing Systems. *Sensors*. 2017, 17(8), 1744, DOI:10.3390/s17081744.
138. F. Bonomi, R. Milito, P. Natarajan, and J. Zhu. Fog computing: A Platform for Internet of Things and Analytics, In: Bessis N., Dobre C. (eds), Big Data and Internet of Things: A Roadmap for Smart Environments. Studies in Computational Intelligence, Springer, Cham, New York. **2014**, 546, 169-186.
139. X. Guan, B. Yang, C. Chen, W. Dai, and Y. Wang. A Comprehensive Overview of Cyber-Physical Systems: From Perspective of Feedback System. *IEEE/CAA Journal of Automatica Sinica*. **2016**, 3(1), 1-14, doi:10.1109.JAS.2016.7373757.
140. W. Fang, W. Zhang, J. Xiao, Y. Yang, and W. Chen. A Source Anonymity-Based Lightweight Secure AODV Protocol for Fog-Based MANET. *Sensors*. **2017**, 17, DOI:10.3390/s17061421.
141. Y. Zhang, Y. Xiang, W Wu, and A. Alelaiwi. A variant of password authenticated key exchange protocol. *Future Generation Computer Systems*. **2018**, 78, 699-711, doi:10.1016/j.future.2017.02.016.
142. M. Frustaci, P. Pace, G. Aloi, and G. Fortino. Evaluating critical security issues of the IoT world: Present and Future challenges. *IEEE Internet of Things Journal*. 2018, 5(4), 2483-25-95, DOI:10.1109/JIOT.2017.2767291.