Journal of Communications Technology, Electronics and Computer Science, Issue 24, 2019
ISSN 2457-905X

Fog Computing Architectures, Privacy and Security Solutions

Wasswa Shafik
Computer Engineering Department, Yazd University, Yazd, Iran
wasswasshafik@stu.yazd.ac.ir
Seyed Akbar Mostafavi
Computer Engineering Department, Yazd University, Yazd, Iran
a.mostafavi@yazd.ac.ir

Abstract
Fog computing is a promising computing paradigm that extends cloud computing to the edge of networks where it provides services closer to users characterized by closer proximity to end-users and bigger geographical distribution, local resource pooling, latency reduction and backbone bandwidth savings. Fog computing supports vertically-isolated, latency-sensitive applications by providing ubiquitous, scalable, layered, federated, and distributed computing, storage, and network connectivity. In this paper, we have comprehensively surveyed and identified fog computing bottlenecks by showing the research gaps, classification of insights on fog computing corresponding state-of-earth resolutions. The Fog situates between the devices that can be connected on Internet known as Internet of Things (IoT) like electronics to allow connectivity, interaction and exchange data and the cloud. This paradigm faces security and privacy challenges for instance intrusion, cyber-crimes in design, implementation, operation or internal control. Besides, those inherited from cloud computing for instance integrity, confidentiality, availability, trust and reputation, authentication among others were studied in early standards.

Keywords: Fog Computing; Internet of Things; Security; Fog Privacy; Strategic Access

1. Introduction

Fog computing is denoted to as fogging or edge computing that extends cloud computing towards the edge of networking where it facilitates the operation of storage, computation, and networking services between end devices and data centres [1]. Edge computing is characteristically denoted to be a location where services are instantiated, fog computing implies easy computation, and storage resources and services close to devices and systems in the control of end-users.

Fog computing allocates the universal framework where selected services and processes are directed at the edge of the network by an IoT device, but still leaves other applications to be managed via the cloud that brings linkage of data [2]. To cloud computing, it offers storage, data and various applications for users but on a larger geographical scale, Fog paradigm accelerates operations and distributes communication and computation services to devices controlled by end-users often serves as a complement to cloud computing [3]. The core awareness in Fog computing is to improve efficiency and reduce the amount of data transported to the cloud for processing, analysis and storage.

Nonetheless, it also used for security, performance and logical reasons, it has an extra layer of an edge which supports and similar to that of cloud computing and the IoT applications [4]. More importantly provision of low latency in the network, paradigm emphasizes proximity, geographical distribution, local resource pooling, latency reduction, and bandwidth reserves to achieve a better quality of services via contribution services at the edge of the network, or even end devices resulting in superior user-experiences [5]. Due to its wide geographical distribution capabilities, it is well situated for real-time big data, and real-time analytics, the devices are distributed over heterogeneous platforms, spanning multiple management domains, unlike cloud computing.

A fog computing environment network partakes two planes, a control plane and a data plane. The control plane looks offers an overview of the network structure. The data plane occasionally referred to as a forwarding plane that determines what happens to the data packets as they arrive. The data plane allows computing resources to be placed anywhere on the network [6].

This distributed approach to handling information is becoming more widespread as the number of Internet of Things devices increases. The reason for this is that IoT devices generate large amounts of data and transmitting all of this directly to a cloud service can consume large amounts of bandwidth and create problems with latency. If the data is part of a control system, for machinery, for example, this can lead to performance problems and lack of responsiveness [7]. Fog computing allows IoT data to be processed in a data hub or smart device closer to the sensor that's generating it.

The significance of using this effectively lies in prioritizing the data packets and routing them

consequently. The most critical data is analysed on a fog node closest to the device generating it, the node itself can pledge actions that need to be carried out quickly, such as opening a valve or tripping a switch. Data that can wait a little longer is passed additional the line as resources and bandwidth permit to an aggregation node, examples of this might be in smart metering where data from individual meters would be passed to a local sub-station [8]. Data that's basically for ancient or big data analytics will be conceded reliably to the cloud or a data centre as resources allow.

The main impressions of this paradigm, including security, scalability, openness autonomy, programmability, reliability, availability, serviceability etc. There are some concerns surrounding the use of a fog model. Numerous concern securities, it's easier to secure data when it kept together, accordingly uncertainty sensitive information is distributed among many devices there are more points where it's vulnerable. It's therefore important that fog nodes are subject to appropriate security controls [9]. Another issue is that the fog adds a further layer of complexity which may make some enterprises wary of adopting it in the short term.

The fog architecture strategies are the vital components and are alienated into three layers like heterogeneous physical resources, fog abstraction layer and fog Service orchestration Layer. Cloud Service Providers famines to expand the Cloud up to the Edge also may build the Fog infrastructure. Remarkably, cloud computing is Internet or network without which the entire network collapses and there is no way uncertainty connecting to the cloud servers whereas fog computing has different applications ranging from an IoT to Human-Machine Interactions ranging wide applications[10].

Autonomic computing mechanizes the process through which the user can provision resources access through minimizing user involvement, automation speeds up the process, reduces labour costs and reduces the possibility of human errors and a good fit for small and medium-sized dealings who need on-demand access to company information from anywhere in the world without hardware or expensive equipment where allows for flexibility within reasonable through featuring a pay-as-you-go structure when security and privacy issues considered [11].

The implement measures to reduce your network's vulnerability to unauthorized access or damage. It may not be possible, otherwise cautiously practical, to eradicate all vulnerabilities, so performing an evaluating risk like data loss, security breaches, malicious attacks including hacking and viruses is significant in deciding what measures to implement [12]. Preventive measures embrace security devices such as firewalls and anti-virus software, security settings in the router or the operating system, data encryption systems for sensitive data, data backup, including the use of off-site backup, checking access to the network infrastructure to authorized personnel only, training staff in the safe and secure practice of the equipment [13].

Privacy and anonymity are supreme to users, particularly as e-commerce continues to gain traction. According to studies, privacy violations and threat risks are standard considerations for any website under development and the existing one's privacy links [14]. Notably, privacy in a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. When measured through qualitative and quantitative privacy and security assessments, file and resource sharing, sharing a single internet connection, increasing storage capacity [15].

Current intelligences on issues like device synchronization, device trust, authentication, integrity, secure data storage, confidentiality, secure and private data computation, availability with privacy factors comparable data, usage and location privacy, access control, intrusion detection shows that there is a need to expansively analyse security and privacy in relation to interconnection and computing as a whole.

From the identified issues instantaneously above, this authenticates this study to understand the insights of fog computing security and privacy research gaps, categorizing of sensitivities as well as proposing solutions to identified fog computing bottlenecks that have not been well studied based on the current and existing studies. Certifying functional and operational performance has gained paramount reputation exclusively once the number of devices connects to IoT have been growing tremendously having in mind that physically and functionally intermediate between nodes and centralized clouds [16].

Fog computing bids a way of allotting that workload in order to reduce the strain on infrastructure whilst delivering results more hurriedly. It also permits easier and more cost-effective scaling. For IoTs that require a rapid response time or for remote locations where fast networking isn't accessible, it offers a useful alternative to both the cloud and more traditional models [17]. Basing on the observation, they would need to have big processing rates increase in network and data centre capacity.

The rest of this article is structured as follows. In section 2, we summarized the current related work about fog computing, the classification of modern paradigms including jungle, cloud, edge, fog together with the characteristics of fog computing. In section 3, we illustrate fog taxonomy, discussion on fog architecture including the traits of fog and the interplay between the fog, edge and the cloud and the difference that cut across. In section 4, we elaborated security and privacy issues within the domain of Fog computing paradigm. The following

section 5 takes a close look at the investigation of security and privacy against the state of earth solutions. We conclude by depicting identified and persisting encounters as well as discussing future work perspectives.

2. Related Work

Security partakes consistently a major issue in technology advancement, in this section will review the most current work in the fog computing environment, it develops predominantly stern because the data is located in different places even in all the sphere. Security and privacy protection are the two main factors of the user's concerns about cloud technology [16]. Nevertheless, many techniques on the topics in fog computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the forthcoming progress of fog computing technology in government, industry, and business [17]. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

Focusing on converging characteristics towards a common definition of a fog node, while we remain cognizant of the ongoing evolution that is distorting the differences between clouds, fogs, and edge devices as the services become more oblivious of the infrastructure used. For instance, the effects of fog computing on cloud computing and big data systems may vary however, a common aspect is a limitation inaccurate content distribution, an issue that has been tackled with the creation of metrics that attempt to improve accuracy, gives the cloud a companion to handle the two Exabyte of data generated daily from the IoT [18]. Processing data closer to where it is produced and needed to unravels the challenges of ignition data volume, variety, and velocity.

Fog networking comprises of a control and data plane for example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-centre. Fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction and backbone bandwidth savings to achieve quality and grade and edge analytics mining, resulting in superior user-experience and redundancy [18].

The fence and footraces toward the rapid growth of fog computing are data security and privacy issues including Reducing data storage and processing cost is a mandatory requirement of any organization [19], while analysis of data and information is always the most important tasks in all the organizations for decision making [20]. Consequently, no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers.

2.1 Computing Paradigms Classification

The evolution of IoTs has amplified the high performance of embedded systems that can be utilized in locally and over the wider platform to enable resolutions for computing paradigm chucks and gateways within the fog platforms. Since of advances in big data and network computing, to examine the security and privacy levels, several new distributed computing paradigms have arisen. In the section, we present four new distributed computing paradigms including Jungle Computing, Cloud Computing and Edge Computing, Fog Computing.

2.1.1 Jungle Computing

Jungle computing form of high-performance computing that allocates computational tasks across clusters with increased complexity provides a range of choices beside traditional supercomputers and clusters. Jungle computing cartels several distributed and high-performance computing systems to reduce programming complexity that makes it different from Fog and Cloud computing.

2.1.2 Cloud Computing

The term "cloud" is a set of dissimilar types of hardware and software that work jointly to deliver many parts of computing to the end-user as an online service. Cloud Computing involves the use of hardware and software to deliver a service over a network (classically the Internet). The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs and helps the users focus on their core business instead of being impeded by technical impediments [21].

Currently, many companies are moving to a Hybrid Cloud Computing model. With this model, companies are given the flexibility of storing sensitive data securely in a private cloud while storing public data in a public cloud. Both infrastructures are kept as separate, unique entities, this provides reduced costs like establishing, and running a data centre is expensive, flexibility, mobility, scalability, no need for a backup plan, data security, and improved collaboration among others in the merits.

2.1.3 Edge Computing

This is stimulating progress in the ongoing search for network infrastructure resolutions that deliver speed and reliability across a wide range of industries has quickly become the newest trend for companies looking to break beyond the limitations imposed by traditional cloud-based computing architecture. Though enterprise-level data centres continue to play a vital role in modern networks, the exciting possibilities offered by IoT devices adept of processing the data they collect closer to the source is

persuasive everyone to reconsideration their tactic to the network infrastructure[22].

The scalable nature of edge computing also makes it an ideal solution for fast-growing, agile firms, especially if they are already making use of colocation data centres and cloud infrastructure. Importantly, this computing focuses on speed, it has the capability to increase network routine by contending latency. Edge data centres allow them to service end-users efficiently with little physical distance or latency thus incredible versatility. Security is other concern about IoT devices is that they could be used as a point of entry for cyber-attacks, allowing malware or other intrusions to infect a network from a single weak point. Tranquil, it offers a far less expensive route to scalability allowing companies to expand their computing capacity through a blend of IoT devices and edge data centres and reliability as well [23].

2.1.4 Fog Computing

To analyse the security and privacy of network on significant data is transferred through globally connected channels alongside lots of gigabytes of other users' info. The Fog computing is known as fog fogging defined as decentralized computing infrastructure in which data, computer, and applications are distributed in the most logical, efficient place between the cloud, data sources and local data sources. Fog computing fundamentally extends cloud computing and services to the edge of the network. The system is vulnerable to cyber-attacks or data loss, the problem can be partially solved with the help of hybrid or private clouds [24].

Fog nodes are fundamental processing rudiments that enable high-compute operations in close proximity to end nodes. Once these high-level requirements are well understood, the design of the network and its elements can commence. Fog offers unique partitioning options for multifaceted software-based systems using a hierarchy of processing, networking and storage resources from the cloud to IoT endpoints. With several layers of fog nodes potentially in a deployment, finding a balance of the optical layer in the hierarchy to host functions is an interesting challenge [25].

2.2 Characteristics of Fog computing

Issues including edge location, location awareness together with low latency support for endpoints with the finest services at the edge of a network. Within this section, we are discussing various computing characteristics, some of them are briefly explained below.

2.2.1 Heterogeneity

Compute, storage, and networking resources are the building blocks of both the Cloud and the Fog. This implies that Fog nodes cannot be deployed in a variety of environment.

2.2.2 Mobility Support

It is vital for a number of Fog applications to interconnect unswervingly with mobile devices, and therefore support mobility techniques, with a different protocol, that decouple host identity from location identity, and require a distributed directory system.

2.2.3 Edge location:

The backgrounds of the Fog computing are traced to early proposals to sustenance endpoints with rich services at the edge of the network, including applications with low latency requirements basic examples include video streaming, augmented realities.

2.2.4 Distribution geographically

In sharp contrast to the more centralized Cloud, the Fog will play an active role in delivering high-quality streaming to moving vehicles, through proxies along highways and tracks. This depicts that the services and application objective of fog is widely distributed.

2.2.5 Interactions Based on Real-Time

Fog applications and services involve real-time interactions rather than batch processing. Fog requires real-time interactions for great speedy services.

3. Fog Computing Taxonomy

The operations within this fog archetype state the entire processing happen inside a data hub on a smart mobile device on the edge of the network in a smart router or another gateway device. For instance, in figure 1, in IoT, this technique is quite convenient as the amount of data twisted by the sensors is immense where Cisco that refers to encompassing cloud computing to the edge of an enterprise's network [26]. Notably, Edge Computing or fogging, fog computing facilitates the operation of computing, storage, and networking services between end devices and cloud computing data centres.

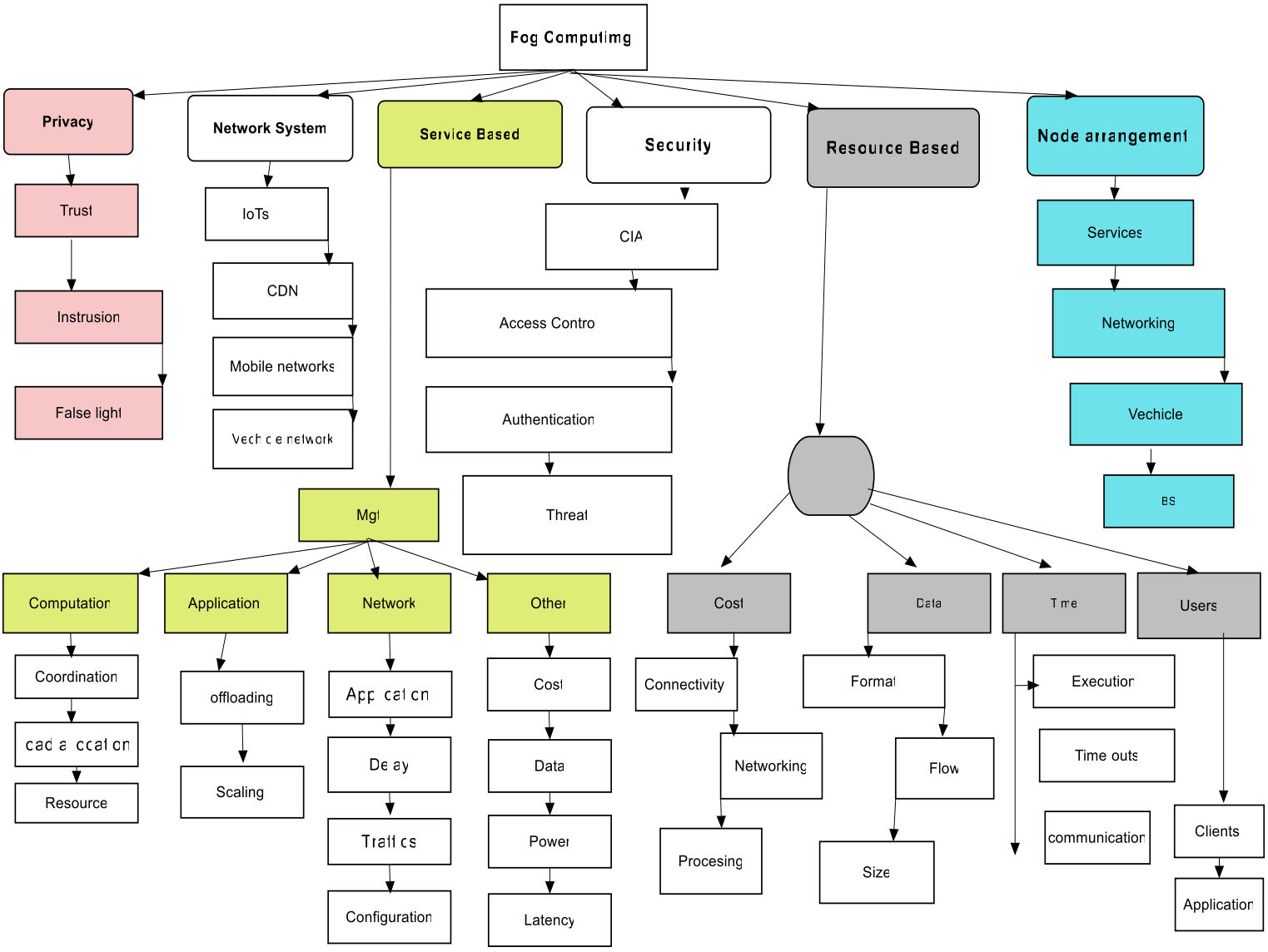

Fig. 1 Fog computing taxonomy

In distribution perspectives for fog computing entities permits the deployment of fog services, and formed by at least one or supplementary physical devices with processing and sensing capabilities instance a computer, mobile phone, smart edge device, car, among others. It is worthy to note that physical devices of a fog node are connected by dissimilar network technologies both wired and wireless and aggregated and abstracted to be viewed as one single logical entity, which is the fog node, able to seamlessly execute distributed services, as it were on a single device [27, 28]. Fog computing is physically and functionally intermediate between edge nodes and centralized clouds.

3.1 Fog Architecture

This emerged as an auspicious technology that can bring the cloud applications closer to the physical IoT devices at the network edge among which a fog node is, usually in relation to a specific edge device, a specific use case or an application. This section, we describe the architecture of fog in fog computing. Considering edge devices, sensors, and applications generate an enormous amount of data on a daily basis. The data producing devices are often too simple or don´t have the resources to perform necessary analytics or machine-learning tasks [29]. They just produce information to the cloud. The Cloud has the power and ability to manage these computing tasks. But

the cloud is often too far away to process the data and respond in time. Connecting all the endpoints directly to the cloud is not an option, though sending raw data over the internet can have privacy, security and legal implications [30].

Currently, in the Fog Computing architecture, the layer of fog is described basing on the perspective of Things like discussed in [31]. It can be a raspberry, a gateway, a router, amongst others. Where the software reduces the amount of data sent to the cloud and takes action depending on the business logic applied in the Fog Node. The Fog Computing architecture is used for applications and services within various industries such as industry IoT, vehicle networks, smart cities, smart buildings and so forth as depicted in figure 2 below.

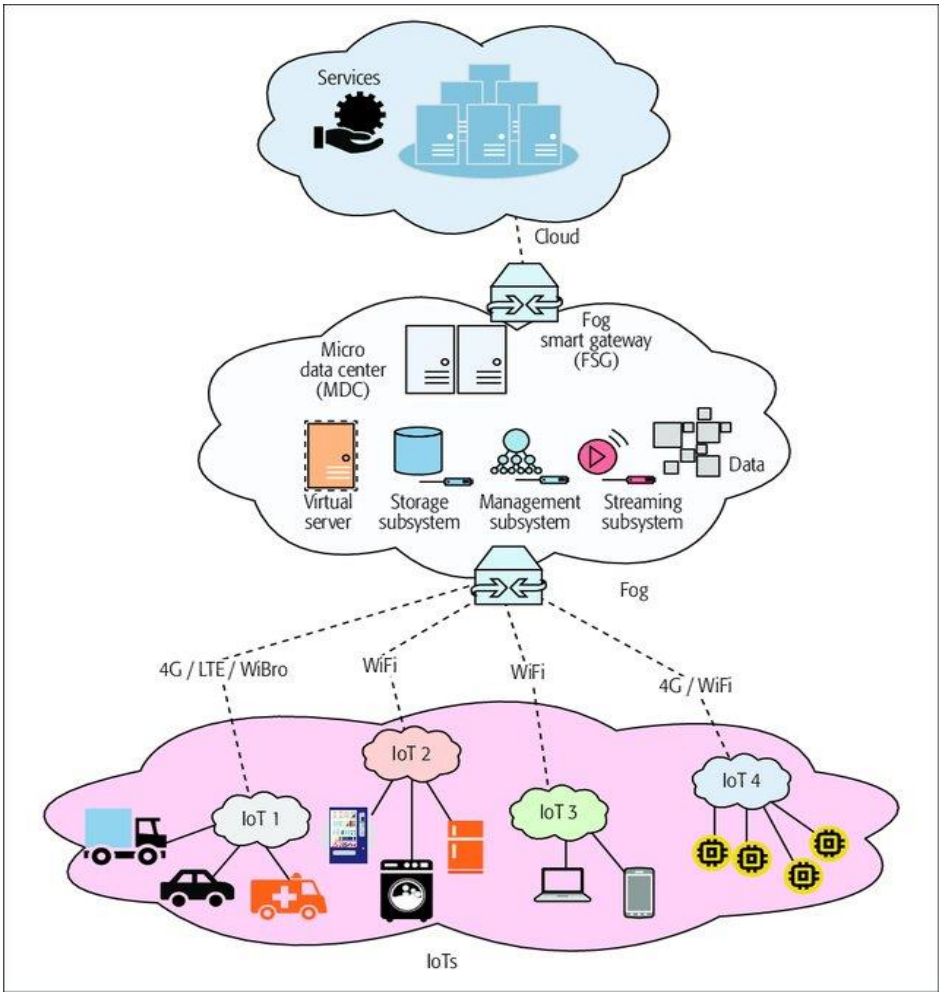

Fig. 2 Architectural Interconnectivity of fog components

The encourage with fog paradigm by that storage, computing, handle and media power can exist anyplace across the structure, possibly from data centres, the cloud computing, advantage devices like gateways or routers, and advantage equipment itself as for instance, a system, or even from detectors and it has mainly five layers through which it does its operation, it is also vibrant that within these, three important echelons are silenced as illustrated in figure 2 from the end-user of the device to the last layer where data were widely manged [31].

3.1.1 Data management centre layer

This is the last layer of last computing like fogging, here the core emphasis is on the storage and management of large data. This service model layer in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). Users normally pay for their cloud data storage on a per-consumption depending, when it comes to storing and accessing massive amounts of data by an organization, cloud data services are a cost-effective alternative to setting up and running a data centre [32, 33]. A data centre customarily refers to server hardware on your premises to store and access data through your local network.

3.1.2 Intermediate computing node layer

A node is a basic approach, are devices or data points on a larger network. Devices such as a personal computer, cell phone, among others are nodes. When defining nodes on the Internet, a node is anything that has an IP address. These nodes may contain a value or condition or possibly serve as another independent data structure. Nodes are represented by a single parent node [34]. The highest point on a tree structure is called a root node, which does not have a parent node, but serves as the material of all of the nodes below it in the hierarchy. The height of a node is determined by the total number of edges on the path from that node to the furthest leaf node, and the height of the tree is equal to the height of the root node and this level, intermediate computing is done through this node layer [35].

3.1.3 Edge computing layer

Edge computing layer by definition is a layer where optimization of applications or cloud computing systems by taking some portion of an application, its data, or services away from one or more central nodes "core" to the other logical extreme "edge" of the Internet which makes contact with the physical world or end-users. It locally and fundamentally optimizes the processing and manages sensors of the IoT networks for better computing and close to the user [36].

3.1.4 Sensor network

Once IoTs are known at first layer, then the focus of devices put on whether it may be picked censored from the limited capacity of network nodes for data storage, computing and accessing. While at this level layer, resource utilization, the availability of sensors and fog nodes and network elements are monitored noting that variety of tasks performed by nodes too to certify better quality data and resource basic management [37].

3.1.5 Physical layer

This is the first layer on the fogging stages where we diagnose logical connections of IoT devices, noticing behaviours. This contracts with every single "thing" that is capable of connecting to the Internet or even maybe to a network and generating data. It encompasses nodes, devices like vehicles, smartphones, and smart things in general as illustrated in a detailed figure above showing layers within different capacities and some related samples [38].

4. Security and Privacy Challenges

Furthermore, under this section, we denote different challenges from the tradition IoT-cloud architectures, millions of smart fog devices are wildly distributed and located in different areas, which can be easily compromised by some malicious parties. These compromised fog devices may temper the data collected by smart health IoT devices, and these fake data may mislead the data user or even threat people's lives [39]. To address these arising challenges and opportunities different from traditional cloud-based architecture, we supplementary elaborated security and privacy differences and similarities, we focused on the fog computing issues and challenges, to begin with, is a clear definition of this terms [40].

4.1 Security and Privacy definition

Fog paradigm requires security in the cloud environment by reducing the rate of data loss through supporting vertically isolated, latency-sensitive applications by providing ubiquitous, scalable, layered, federated, and distributed computing, storage, and network connectivity protecting data transported through the IoT devices [41]. Privacy can be defined as the protection, is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues may arise in response

to information from a wide range of sources. Notably, the challenge is to use data while protecting an individual's privacy preferences and their personally identifiable information[42]. In details, we discussed the main privacy issues that we identified.

4.2 Location of Privacy

Several approaches have been proposed for protecting location privacy of a user. The fundamental idea behind all techniques is to prevent the revelation of unnecessary information and to explicitly or implicitly control what information. There is an inherent trade-off between the utility and quality of services that users wish to receive and the location privacy they are ready to compromise. Privacy policies define restrictions that regulate the release of the location of a user to third parties [43]. User's needs for privacy are satisfied by restricting the ability to manage locations and disclosing information. The biggest disadvantage of policy-based measures is the lack of policy enforcement specified by a service provider.

4.2.1 Usage and data privacy

Briefly, data protection is about securing data against unauthorized access. Data privacy is about authorized access who has it and who defines it. Another way to look at it is this: data protection is essentially a technical issue, whereas data privacy is a legal one. IoTs vary in the levels of privacy offered virtual credentials consists of the birth date, current address, and telephone number(s). Some sites also allow users to provide more information about themselves such as interests, hobbies, favourite books or films, and even relationship status. These distinctions matter because they are woven deeply into the overarching issues of privacy and cybersecurity, both of which loom large in businesses, politics and culture [44]. For industries subject to compliance standards, there are crucial legal implications associated with privacy laws. In addition, ensuring data protection may not adhere to every required compliance standard leading to trust from the technology.

4.2.2 Technology to Trust Privacy

In diminutive, no number of technological precautions can eradicate the central role of trust in guaranteeing data privacy. Technology is still implicated in data privacy, exactly because the attributed users of technology have an obligation to the privacy law. All of this goes double for those involved in file transfers. Data authorizations through Web nodes as the equivalent of obsolete postcards. Any server that handles a packet can read the message as well as the forwarding Internet Protocol address. At some very basic level, there is no confidentiality and not much security for anything sent across the open Web [45].

4.3 Challenges

Theory of computing challenges provides computer avail concepts as in models, and formalisms to help reason about these concepts and models. Software and efficient algorithms are the base of today's technology and of technology to come. We substantiate these points in two ways. First, we describe five areas that pose major technologically foundational research and theoretical research that is focused on individual applications are needed in this endeavour. We provide a summary of the challenges in all three-dimensions as follows.

4.3.1 The legal dimension

While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals [46]. The former, forensic, relates to a discussion or examination performed in public. Because trials in the ancient world were typically held in public, it carries a strong judicial connotation. This legal, which is derived from the Latin word for knowledge and is today closely tied to the scientific method, a systematic way of acquiring knowledge.

The main information manipulation techniques within the legal aspects of data reduction and data mining. Forensic investigators currently use data reduction methods involving known file filters and hash sets, but these are limited in both scope and performance. Data mining employs a combination of machine learning, statistical analysis and modelling techniques to extract relevant information from large data sets [47]. This dimension just begins to find applications in digital forensic investigations, and numerous research opportunities exist in this area.

4.3.2 The organizational dimension

The objective of the organizational dimension is to develop knowledge of theories, skills, techniques, and strategies needed to accomplish the mission. The Organizational Dimension falls into three sections. The headings appearing in the first section illustrate organizational leadership, executive-level strategy, and the characteristics of leaders within an organization [48]. The relationship between leadership principles and the nature of organizations is also addressed. Integration answering enquires like to what degree the organizational structure results in an integrated approach that crosses division. Evaluation and resource allocation focusing on the consistent financial resources to support organizational oversight for the duration.

4.3.3 The technical dimension

The technology element is composed of all of the tools, applications and infrastructure that make processes more efficient. Following the process includes formal and informal mechanisms (large and small, simple and complex) to get things done. Design defines how the organization implements its strategy [49]. Processes, culture and architecture are important in determining the design. The model is independent of any particular technology or technological changes over time.

Traditionally, IoTs focuses much on confidentiality followed by integrity and availability. The persistent problem here is that the business is often unaware of threats that come with the technologies fuelling their innovation. Companies want to reap the rewards of innovation in exchange for sacrificing security operations. That being said, the picture is changing. Cybersecurity education, as well as the oft-lamented argument that the entire leadership sphere should be vigilant about cybersecurity, is showing results. Below we share the four main discovered problems that need quick attention in fog computing at cut across the entire three discussed dimensions [50].

In perspective of security, the same security concerns that apply to current virtualized environments can before see to affect fog devices hosting applications. This is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information it has a threat to the data, and protocols this is so due to the presence of secure sandboxes for the execution of droplet applications poses new interesting challenges like trust with Privacy. The fog will allow applications to process user's data in a third party's hardware or software [51].

Security focuses preventative, detective, and responsive on the Controls like documented processes and countermeasures like firewalls must be implemented as one or more of these previous types, or the controls are not there for the purposes of security. Shown in another triad, the principle of defence in depth dictates that a security mechanism serves a purpose by preventing a compromise, detecting that a compromise or compromise attempt is underway, or responding to a compromise while it's happening or after it has been discovered [52]. Below are persisting issues within the computing paradigms that have come through ages before table 1.

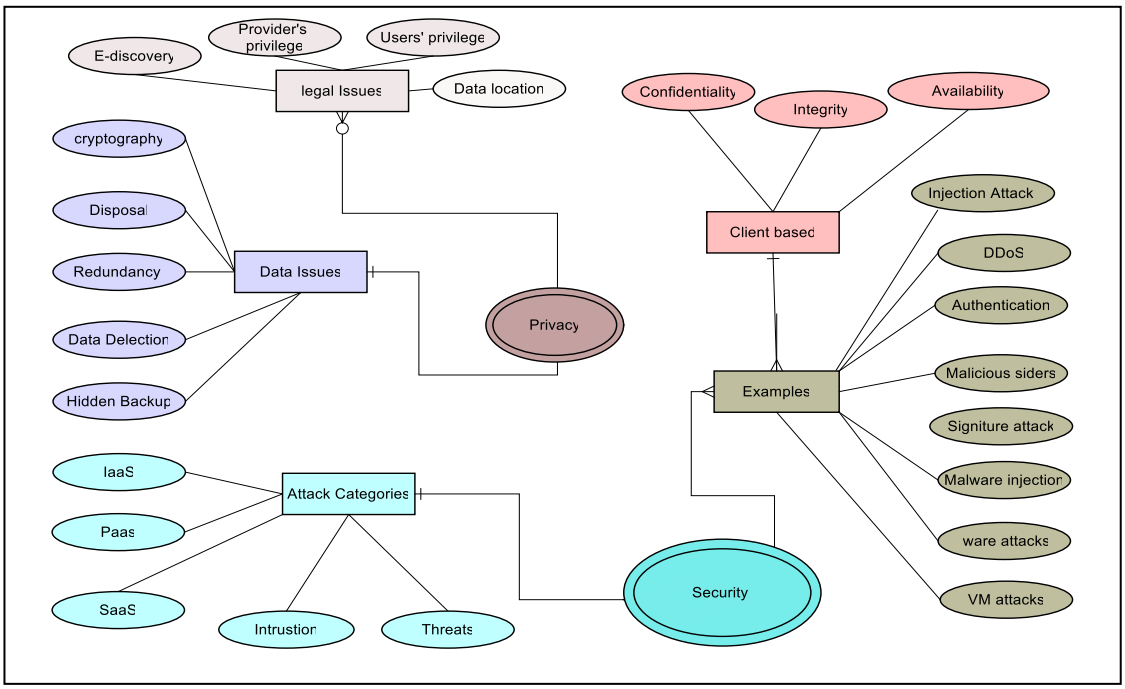

Fig. 3 security and privacy Analysis

4.3.3.1 Computing or Storage limitation

In appreciation of the current trends, there have been efforts that were looking at improving this fact with smaller. Kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed Controllers should only store personal data for as long as is necessary for the specific purpose for which it was

obtained. As per the current Data Protection Act, the storage limitation principle does not apply to personal data cannot be re-associated with the particular data subject.

4.3.3.2 Standardization and Privacy

Today no standardized mechanisms are attainable so each member of the network apparatuses can publicize its obtainability to host other software mechanisms. Nethermost, many protection officers in the file transfer security community would tell you that it is a private security risk. It poses the privacy risk of a security breach that could put you in your personally identifiable data in danger of identity theft and for others to send it their software to be run as and privacy as well.

4.3.3.3 Programmability

Monitoring solicitation lifecycle is by this time a challenge in Fog environments. A redundant term, because what varieties IoTs that it follows a set of directives. Many IoT devices perform only one operation, but they are still following instructions that reside permanently in the unit. The presence of small functional units in more locations like devices calls for the right abstractions to be in place so that programmers do not need to deal with these difficult issues.

5. State-of-the-art Solutions

In this section, we classify in table 1 each problem in accordance to the solution so that available researchers can concentrate on them and address them the identified issues

5.1 Authenticity

Nevertheless, such a third-party authentication only ensures to verify whether a node initiated a request, which is indeed a legitimate node. Even then, the compromised node cannot be detected since it may be a legitimate, third-party certified device. Spoofing of addresses is easy because such addresses are practically unlimited. In various levels of hierarchy in Fog nodes, authentication is essential. As already stated above, Public Key Infrastructure (PKI) may not be feasible. Near-Field Coins (NFC) can be used effectively in Fog Computing to simplify authentication procedures. Biometric-based authentication can also be effectively used in the Fog Computing ecosystem. Authentication becomes important at various levels of gateways or at the level of the device itself.

to make the fog authenticity regardless of the current efforts, these security and privacy problems are still persistent as discussed.

5.2 Synchronization and discovery

IoT devices running on devices may require either some agreed with the way of loading applications, updates, and changes to their operating systems or settings. Uniform devices capable of wireless networking must have some way of loading software if only to load what is needed to create a wireless connection in the first place [53]. Some devices can synchronize over the Internet or wireless networks this centralized point like to establish an upstream backup. Wireless sync eliminates the need for the device to be physically connected to the computer, but it is usually slower than a direct physical connection.

5.3 Management

Having potentially billions of IoT devices to be configured which sends out the management commands to the mobile devices, and a client component, which runs on the managed devices, receives and, implements the management commands. In some cases, a single vendor provides both the client and the server, while in other cases the client and server come from different sources. The fog will heavily rely on decentralized instance scalable management mechanisms that are yet to be tested at this exceptional scale.

5.4 Multi-tenancy

In a multi-user (multi-tenancy) environment in a Fog ecosystem, many complex issues arise. Issues of identity management, monitoring, performance, scalability, security issues including insider management, among others multifactor authentication mechanisms based on end-user role or identity should be implemented in Fog Computing environment, based on analysis of administrators and tenants. A secure reliable networking platform can offer a programmable environment for fine-tuning of topology, allocation of bandwidth and policies of traffic management.

5.5 Failure Recovery

A procedure that allows for a restart of a failed system in a way that either eliminates or minimizes the number of incorrect system results. As done is any backup and recovery system, in Fog environment also we require to provide a reliable data backup and recovery mechanism. The data on the site should be copied and mirrored to

offsite on a regular basis. Depending on specific application requirements, a Fog platform will have a high frequency of data throughput and relatively small sizes of data storage requirement. For the effectiveness in backup and recovery processes, we require to focus on developing policies and strategies for data selecting, mapping, testing and accessibility roles during the recovery process.

Table 1. Fog computing State of the art solutions

Main Identified Challenges	**Identified loopholes**	**Proposed Solutions**
Limitation of bandwidth	A five-layer fog cloud-assisted IoT-based was proposed basing on the stress monitoring framework [53]. A two-stage Temporal Dynamic Bayesian Network (TDBN) model was formed resulting to alert generation mechanism [54]. Fibre Channel (FC) switch based on a field-programmable gate array (FPGA) is designed [55].	An Embedded (Temporal Dynamic Bayesian Network) TDBN predictive model may be developed with generation parameters.
Logging	Storing at the time the multicast - broadcast single frequency network measurement is made, cell measurement results [56, 57]. Novel design and implementation of an instrument for shaft sinking by drilling (ULISSD) [58]. Unpredictability and lack of central authority are further enhanced by a virtual personality [59].	Novel microprocessors and microcontroller devices available for this technical application.
Legal issues	The augmented reality device from a network security appliance receives dynamic network security information [60]. Capturing, by an augmented reality device, a real image of a network object associated with a private network [61].	Hardware or software data communication encryption may be employed to provide increased confidentiality and security, legal Trust Model.
Discovery/Synchronization	Approached on Independent Process, Cooperative Process leading Execution of one process affects the execution of other processes [62].	Virtual Tape Library Models for material backed as well as the classical software-based solution to the critical section problem.
Dependability on the chain	Ensure real-time monitoring to detect vulnerabilities, security threats and abnormal behaviours [63].	Authentication input-output-related system model, material provenance in Fog.
Programmability	Tried on the excessive exploitation of fog resources and management through proposing scalable Vehicular Networks [64].	Embedding energy, efficient Multicast routing protocol based on Software-defined networks and Fog computing for Vehicular computing.

5.6 Backup Mechanisms

In the case of mobile and wireless Fog ecosystems, a backend recovery system based on mobile and on-site arrangements, consistency is required and mechanisms include shared Backup Router Resources, High-density Distribution and Rake Technology, Techniques for Parity Cloud Service, cold and hot Backup Service Replacement Strategy, Efficient Routing Grounded on Taxonomy among others, large bandwidth-based offsite backup and recovery mechanisms should be provided [65].

6. Conclusion

In this paper, we discussed numerous breaches privacy and security vulnerabilities while using analysis method to bring the attention of the researchers' environment as well as security issues in the context of fog networks, which is a new computing paradigm to provide mutable properties at the edge of a network to nearby end-users [66]. The scope of Fog computing is quite huge that include IoTs, applications, standards, protocols, devices, technologies, security, reliability, response requirements, performance, latency, energy, environmental conditions, among others is to be considered. We classified those issues based on the layers that make up IoT and discussed numerous in the broad sense.

We have also surveyed and examined the literature on the existing methods to protect and detect the security infrastructure and summarized these security methods and state of earth solutions on how to address the security issues in the fog computing. To have privacy and security requires a holistic cybersecurity framework casing all concept layers of heterogeneous IoT systems and across platform boundaries. Between all the things security and privacy of network devices are crucial [67, 68]. It is significant to touch out all disputes that affect this kind of computing that's why we are working on model focusing on fog forensic analytics, live, big data investigation techniques, and best practices in multi-tenant and multi-jurisdictional fog computing environments.

References

[1] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 workshop on mobile big data*, 2015, pp. 37–42.

[2] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for the internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, p. 116, 2019.

[3] S. Deep, X. Zheng, and L. Hamey, "A survey of security and privacy issues in the Internet of Things from the layered context," *arXiv preprint arXiv:1903.00846*, 2019.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[5] G. Choudhary and V. Sharma, "A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks," in *5G Enabled Secure Wireless Networks*, Springer, 2019, pp. 69–102.

[6] R. Kumar, P. Kumar, and V. Singhal, "A Survey: Review of Cloud IoT Security Techniques, Issues and Challenges," *Issues and Challenges (March 12, 2019)*, 2019.

[7] A. Yousefpour *et al.*, "All one needs to know about fog computing and related edge computing paradigms: a complete survey," *Journal of Systems Architecture*, 2019.

[8] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[9] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, p. 32, 2017.

[10] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the internet of things: A Survey," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 2, p. 18, 2019.

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

[12] D. Puthal, S. P. Mohanty, S. A. Bhave, G. Morgan, and R. Ranjan, "Fog Computing Security Challenges and Future Directions [Energy and Security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

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

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

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

[16] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International conference on wireless algorithms, systems, and applications*, 2015, pp. 685–695.

[17] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of network and computer applications*, vol. 98, pp. 27–42, 2017.

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

[19] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, “Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis,” in *Proceedings of the Workshop on Fog Computing and the IoT*, 2019, pp. 56–63.

[20] P. Hu, S. Dhelim, H. Ning, and T. Qiu, “Survey on fog computing: architecture, key technologies, applications and open issues,” *Journal of network and computer applications*, vol. 98, pp. 27–42, 2017.

[21] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[22] S. Yi, Z. Qin, and Q. Li, “Security and privacy issues of fog computing: A survey,” in *International conference on wireless algorithms, systems, and applications*, 2015, pp. 685–695.

[23] R. Mahmud and R. Buyya, “Modelling and Simulation of Fog and Edge Computing Environments using iFogSim Toolkit,” p. 35.

[24] J. Pereira, L. Ricardo, M. Luís, C. Senna, and S. Sargento, “Assessing the reliability of fog computing for smart mobility applications in VANETs,” *Future Generation Computer Systems*, vol. 94, pp. 317–332, May 2019.

[25] N. di Pietro, M. Merluzzi, E. C. Strinati, and S. Barbarossa, “Resilient Design of 5G Mobile-Edge Computing Over Intermittent mmWave Links,” *arXiv:1901.01894 [cs, math]*, Jan. 2019.

[26] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, “Green and Sustainable Cloud of Things: Enabling Collaborative Edge Computing,” *IEEE Communications Magazine*, vol. 57, no. 1, pp. 72–78, Jan. 2019.

[27] M. R. Bosnia and S.-H. Jeong, "Efficient Content Delivery for Mobile Communications in Converged Networks," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–12, Jan. 2019.

[28] L. E. Chatzieleftheriou, M. Karaliopoulos, and I. Koutsopoulos, “Jointly Optimizing Content Caching and Recommendations in Small Cell Networks,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 125–138, Jan. 2019.

[29] Y. Lai, L. Zhang, F. Yang, L. Zheng, T. Wang, and K.-C. Li, “CASQ: Adaptive and cloud-assisted query processing in vehicular sensor networks,” *Future Generation Computer Systems*, vol. 94, pp. 237–249, May 2019.

[30] M. Rath, B. Pati, and B. K. Pattanayak, “Mobile Agent-Based Improved Traffic Control System in VANET,” in *Integrated Intelligent Computing, Communication and Security*, vol. 771, A. N. Krishna, K. C. Srikantaiah, and C. Naveena, Eds. Singapore: Springer Singapore, 2019, pp. 261–269.

[31] M. Min, D. Xu, L. Xiao, Y. Tang, and D. Wu, “Learning-Based Computation Offloading for IoT Devices with Energy Harvesting,” *arXiv:1712.08768 [cs]*, Dec. 2017.

[32] U. Lee *et al.*, “Intelligent Positive Computing with Mobile, Wearable, and IoT Devices: Literature Review and Research Directions,” p. 57.

[33] P. LAN, K. Li, and Z. Yu, "Computer implementation of piecewise cable element based on the absolute nodal coordinate formulation and its application in wire modelling," *Acta Mechanica*, Jan. 2019.

[34] C. Talnikar and Q. Wang, "A two-level computational graph method for the adjoint of a finite volume-based compressible unsteady flow solver," *Parallel Computing*, vol. 81, pp. 68–84, Jan. 2019.

[35] S. E. Mahmoodi, K. Subbalakshmi, and R. N. Uma, “Cognitive Cloud Offloading Using Multiple Radios,” in *Spectrum-Aware Mobile Computing*, Cham: Springer International Publishing, 2019, pp. 23–33.

[36] L. Xiao, W. Zhuang, S. Zhou, and C. Chen, “Learning While Offloading: Task Offloading in Vehicular Edge Computing Network,” in *Learning-based VANET Communication and Security Techniques*, Cham: Springer International Publishing, 2019, pp. 49–77.

[37] S. Ha, J. Zhang, O. Simeone, and J. Kang, “Coded Federated Computing in Wireless Networks with Straggling Devices and Imperfect CSI,” *arXiv:1901.05239 [cs, math]*, Jan. 2019.

[38] H. Yang and J. Lee, “Secure Distributed Computing With Straggling Servers Using Polynomial Codes,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 141–150, Jan. 2019.

[39] S. Reif, L. Gerhardt, K. Bender, and T. Hönig, "Towards Low-Jitter and Energy-Efficient Data Processing in Cyber-Physical Information Systems," p. 8.

[40] M. Iturbide *et al.*, “The R-based climate4R open framework for reproducible climate data access and post-processing,” *Environmental Modelling & Software*, vol. 111, pp. 42–54, Jan. 2019.

[41] D. Zhang, F. Haider, M. St-Hilaire, and C. Makaya, “Model and Algorithms for the Planning of Fog Computing Networks,” *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[42] J. Angela Jennifer Sujana, M. Geethanjali, R. Venitta Raj, and T. Revathi, "Trust Model-Based Scheduling of Stochastic Workflows in Cloud and Fog Computing," in *Cloud Computing for Geospatial Big Data Analytics*, vol. 49, H. Das, R. K. Barik, H. Dubey, and D. S. Roy, Eds. Cham: Springer International Publishing, 2019, pp. 29–54.

[43] B. Suri, S. Taneja, H. Bhardwaj, P. Gupta, and U. Ahuja, “Peering Through the Fog: An Inter-fog Communication Approach for Computing Environment,” in *International Conference on Innovative Computing and Communications*, vol. 56, S. Bhattacharyya, A. E. Hassanien, D. Gupta, A. Khanna, and I. Pan, Eds. Singapore: Springer Singapore, 2019, pp. 73–81.

[44] M. Aazam, S. Zeadally, and K. A. Harris, "Fog Computing Architecture, Evaluation, and Future Research Directions," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46–52, 2018.

[45] Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, “EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[46] A. Rial and G. Danezis, “Privacy-preserving smart metering,” p. 12.

[47] W. Wei, F. Xu, and Q. Li, “MobiShare: Flexible privacy-preserving location sharing in mobile online social networks,” in *2012 Proceedings IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 2616–2620.

[48] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, “Location privacy in database-driven Cognitive Radio Networks: Attacks and countermeasures,” in *2013 Proceedings IEEE INFOCOM*, Turin, Italy, 2013, pp. 2751–2759.

[49] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement," in *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Chengdu, China, 2009, pp. 717–722.

[50] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[51] J. Valenzuela, J. Wang, and N. Bissinger, “Real-time intrusion detection in power system operations,” *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[52] Y. Shi, S. Abhilash, and K. Hwang, “Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks,” in *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, CA, USA, 2015, pp. 109–118.

[53] S. A. Bragadeesh and U. Arumugam, “A Conceptual Framework for Security and Privacy in Edge Computing,” in *Edge Computing*, F. Al-Tudjman, Ed. Cham: Springer International Publishing, 2019, pp. 173–186.

[54] L.-L. Cheng, X.-S. Zhan, J. Wu, and T. Han, “An Optimal Tracking Performance of MIMO NCS with Quantization and Bandwidth Constraints,” *Asian Journal of Control*, 2019.

[55] H. Lu *et al.*, “Wide tunable laser based on electrically regulated bandwidth broadening in polymer-stabilized cholesteric liquid crystal,” *Photonics Research*, vol. 7, no. 2, pp. 137–143, 2019.

[56] H. Bhattacharya, S. Chattopadhyay, M. Chattopadhyay, and A. Banerjee, “Storage and Bandwidth Optimized Reliable Distributed Data Allocation Algorithm,” *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 10, no. 1, pp. 78–95, 2019.

[57] S. Zhou, N. Liu, L. Zhang, T. He, B. Yu, and J. Li, "Realization of an infrared detector free of bandwidth limit based on quartz crystal tuning fork," *Optics & Laser Technology*, vol. 113, pp. 261–265, 2019.

[58] S. Preussler, F. Schwartau, J. Schoebel, and T. Schneider, “Photonically synchronized large aperture radar for autonomous driving,” *Optics Express*, vol. 27, no. 2, pp. 1199–1207, 2019.

[59] C. Kottke, C. Schmidt, V. Jungnickel, and R. Freund, “Performance of Bandwidth Extension Techniques for High-Speed Short-Range IM/DD Links,” *Journal of Lightwave Technology*, 2019.

[60] S. Qiao, J. Wu, X. Zhan, and T. Han, “Performance limitation of networked control systems with networked delay and two-channel noises constraints,” *Systems Science & Control Engineering*, vol. 7, no. 1, pp. 28–35, 2019.

[61] Z. Meng *et al.*, "Multimode fibre spectrometer with scalable bandwidth using space-division multiplexing," *AIP Advances*, vol. 9, no. 1, p. 015004, 2019.

[62] Q. Zhang, A.-X. Chen, Y. Zhang, L. Li, and W.-X. Yang, “Enhanced Kerr nonlinearity with a single quantum dot coupled to a gain cavity under weak-excitation limitation,” *Laser Physics Letters*, vol. 16, no. 2, p. 025204, 2019.

[63] K. Liu, S.-Y. Tsai, and Y. Zhang, “ATP: a Datacenter Approximate Transmission Protocol,” *arXiv preprint ar X iv:1901.01632*, 2019.

[64] A. Gonzalez-Monge and A. M. Behie, “6 The Effects of Selective Logging on the Habitat Use of the Annamese Silvered Langur (Trachypithecus margarita) in Northeast Cambodia,” *Primate Research and Conservation in the Anthropocene*, vol. 82, p. 101, 2019.

[65] K. Sammallahti and J. Nurmi, “11. BALING LOGGING RESIDUES ON INTERMEDIATE THINNINGS,” *FOREST OPERATIONS RESEARCH IN THE NORDIC BALTIC REGION*, p. 16, 2020.

[66] M. Cao, H. Liang, D. Fan, Y. Wang, H. Jiang, and N. Sun, “Ultrasonic logging instrument for shaft sinking by drilling,” *Measurement*, vol. 132, pp. 344–349, 2019.

[67] J. Chen, W. Berkman, M. Bardoux, C. Y. K. Ng, and M. Allman-Farinelli, "The use of a food logging app in the naturalistic setting fails to provide accurate measurements of nutrients and poses usability challenges," *Nutrition*, vol. 57, pp. 208–216, 2019.

[68] B. T. Bawono and A. Mashdurohatun, “Penegakan Hukum Pidana Di Bidang Illegal Logging Bagi Kelestarian Lingkungan Hidup Dan Upaya Penanggulangannya,” *Jurnal Hukum*, vol. 26, no. 2, pp. 590–611, 2019.

Wasswa Shafik hails from Kampala Uganda where he received his Bachelors of Sciences in Information Technology at Ndejje University, Kampala, Uganda in 2016. He is currently pursuing the Masters of Sciences in Computer Engineering (Networks) at Yazd University, Yazd, Iran. His research area includes 5G and Beyond, Network Science, Quantum communicaation, UAVs and Machine Learning.