DTU Library

Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog

De Donno, Michele; Tange, Koen Pieter; Dragoni, Nicola

[Link back to DTU Orbit](#)

Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog

MICHELE DE DONNO[1], KOEN TANGE[1], and NICOLA DRAGONI[2]
[1]DTU Compute, Technical University of Denmark, Denmark (e-mail: mido@dtu.dk, kpta@dtu.dk)
[2]DTU Compute, Technical University of Denmark, Denmark, and Centre for Applied Autonomous Sensor Systems (AASS),
Örebro University, Sweden (e-mail: ndra@dtu.dk)

Corresponding authors: Michele De Donno (e-mail: mido@dtu.dk) and Nicola Dragoni (e-mail: ndra@dtu.dk).

ABSTRACT In the last few years, Internet of Things, Cloud computing, Edge computing, and Fog computing have gained a lot of attention in both industry and academia. However, a clear and neat definition of these computing paradigms and their correlation is hard to find in the literature. This makes it difficult for researchers new to this area to get a concrete picture of these paradigms. This work tackles this deficiency, representing a helpful resource for those who will start next. First, we show the evolution of modern computing paradigms and related research interest. Then, we address each paradigm, neatly delineating its key points and its relation with the others. Thereafter, we extensively address Fog computing, remarking its outstanding role as the glue between IoT, Cloud, and Edge computing. In the end, we briefly present open challenges and future research directions for IoT, Cloud, Edge, and Fog computing.

INDEX TERMS Fog Computing, Cloud Computing, Edge Computing, Internet of Things, Mobile Cloud Computing, Mobile Edge Computing

I. INTRODUCTION

In the last decade, we have witnessed a significant evolution of computing paradigms. The most known and consolidated one is surely Cloud computing, a paradigm born from the necessity of using "computing as a utility" [1], thus allowing easy development of new Internet services. Cloud computing has been an extremely popular research topic until an overwhelming spread of smart devices and appliances, namely Internet-of-Things (IoT), has pointed out all the limitations of such a centralized paradigm.

The IoT revolution has opened new research perspectives, leading to an increase of interest in decentralized paradigms. In this light, Edge computing made its way [2], with the idea of providing the power of the Cloud at the network edge, tackling most of the new challenges that Cloud computing alone cannot address, such as bandwidth, latency, and connectivity. As a result, several implementations of the Edge computing principles have been proposed [3], [4], amongst others: Mobile Cloud Computing (MCC), Cloudlet Computing (CC), Mobile Edge Computing (MEC).

In this Edge computing fashion, Fog computing emerged from the crowd representing the highest evolution of the Edge computing principles. Indeed, Fog computing aims at representing a complete architecture that distributes resources horizontally and vertically along the Cloud-to-Things continuum [5]. As such, it is not just a trivial extension of the Cloud, rather a new actor interacting with Cloud and IoT to assist and enhance their interaction. However, research related to Edge and Fog computing is still in the early stages and new different perspectives on these paradigms continuously appear in the literature, making it difficult to have a clear idea about their foundations. A lot of effort has still to be done to put these emerging computing paradigms in practice.

Contribution of the Paper. What is Fog computing? How does it differ from Edge computing? How these paradigms relate to Cloud computing and IoT? What are the foundational characteristics of these computing paradigms and their different implementations (such as MCC, CC, MEC)?

In this paper, we aim at answering all these questions by providing an analysis of the foundations and evolution of major modern computing paradigms, namely Cloud computing, IoT, Edge computing, and Fog computing. The focus of the paper is not to propose yet another survey about a single computing paradigm, but to highlight the foundational dif-

ferences between all these paradigms and how they relate to each other in terms of evolution of the computing paradigm. With this aim in mind, terms like Mobile Cloud Computing, Cloudlet Computing, and Mobile Edge Computing will also be framed.

In particular, the contribution of the paper can be summarized as follows:

- *Roadmap and statistics related to computing paradigms:* we provide an analysis of research trends related to the main modern computing paradigms: IoT, Cloud computing, Edge computing, and Fog computing. The analysis is conducted by providing a roadmap of the evolution of each term and a discussion about causes and consequences related to their evolution;
- *Definition and clarification of keywords:* we define and clarify the difference between the following terms: IoT, Cloud computing, Edge computing, Mobile Cloud Computing (MCC), Cloudlet Computing (CC), Mobile Edge Computing (MEC), and Fog computing.
- *Manifest of Fog computing:* we clearly locate Fog computing in respect with other similar paradigms, marking the difference between them and explaining why Fog computing can be considered the glue between IoT, Cloud, and Edge computing; thus, what are the main benefits it drags in.
- *Open Challenges:* we briefly discuss some of the key challenges that are still open in IoT, Cloud, Edge, and Fog computing, in order to highlight some significant research directions for those who are interested in the field.

Ultimately, the paper aims at providing the groundwork for those interested in Edge and Fog computing who cannot find their way in the jungle of keywords and definitions available in the literature. Indeed, we give a clear and structured picture of those paradigms, based on a careful analysis and comparison with other existing computing paradigms and related concepts. To the best of our knowledge, this represents the key novelty of the paper, filling a gap in the related literature.

Outline of the paper. The paper is organized as follows. Section II presents an analysis of research trends related to IoT, Cloud computing, Edge computing, and Fog computing. Section III and Section IV provide background concepts related to Cloud computing and Internet of Things, respectively. Section V analyses the emergence of IoT that brings us to the post-Cloud era. Section VI describes Edge computing and clarifies its main related concepts: MCC, CC, MEC. Section VII extensively discusses Fog computing, pointing out its main benefits. Section VIII shortly outlines open challenges and research directions for IoT, Cloud, Edge, and Fog computing. Finally, Section IX wraps up and concludes the paper.

II. THE ROADMAP FOR COMPUTING PARADIGMS

In this section, we present a roadmap that drives us through first appearance and research trends related to the main topics addressed in this paper: IoT, Cloud computing, Edge computing, and Fog computing.

A. METHODOLOGY

The results presented in this section have been obtained according to specific criteria. Manuscripts were filtered based on the presence or absence of keywords in the title of the document. Keywords of interest were: Cloud computing, Internet of Things, Edge computing, and Fog computing. IEEE Xplore Digital Library (DL) [6] and ACM Digital Library (DL) [7] have been used as data sources.

The reason behind these choices is that we aim at giving an idea of research trends related to specific keywords, rather than providing a comprehensive and detailed statistical analysis of the literature. Thus, we assume that the results highlighted from the analysis of the aforementioned main databases reasonably reflect common trends of the scientific community about recent computing paradigms.

B. FIRST APPEARANCE

First of all, we looked for the first appearance of each keyword. For some keywords, it was difficult to accurately assess the year of the first appearance, since the meaning of terms might have been slightly changing in the last decade. Nevertheless, an approximate timeline is depicted in Figure 1.

As shown in the picture, the idea of Edge computing first appeared in the literature in 2004-2005 with the concept of pushing the application logic and data to the edge of the network [8], [9].

Subsequently, Cloud computing and IoT appeared. The term "Cloud computing" was first used by Google and Amazon in 2006. Eric Schmidt, Google CEO, mentioned it in the Search Engine Strategies (SES) conference [10], while Amazon referred to the Cloud as a commercial product [11]. Later, in 2008, scientific papers about Cloud computing also appeared [12], [13]. About Internet of Things, although the concept first appeared in 1999 by the Auto-ID Center at Massachusetts Institute of Technology (MIT) [14], first literature works are dated 2006 [15], [16].

Fog computing has instead a clear origin. It was first mentioned and defined in 2012 by Flavio Bonomi at CISCO [17].

C. STATISTICS

In order to better understand research trends of computing paradigms, we analyzed the scientific activity related to each of them and we compared it with the interest for Internet of Things. The results are drawn in Figure 2.

Even though the concept of Edge computing appeared in the literature before Cloud computing (as discussed in Subesection II-B), the latter has clearly been the leading paradigm of the last decade, with more than 500 publications since 2010 and peaks of about 1200 publications in 2014 and 2016. On the other hand, the interest in Edge and, subsequently, Fog computing have been constantly increasing over the last few
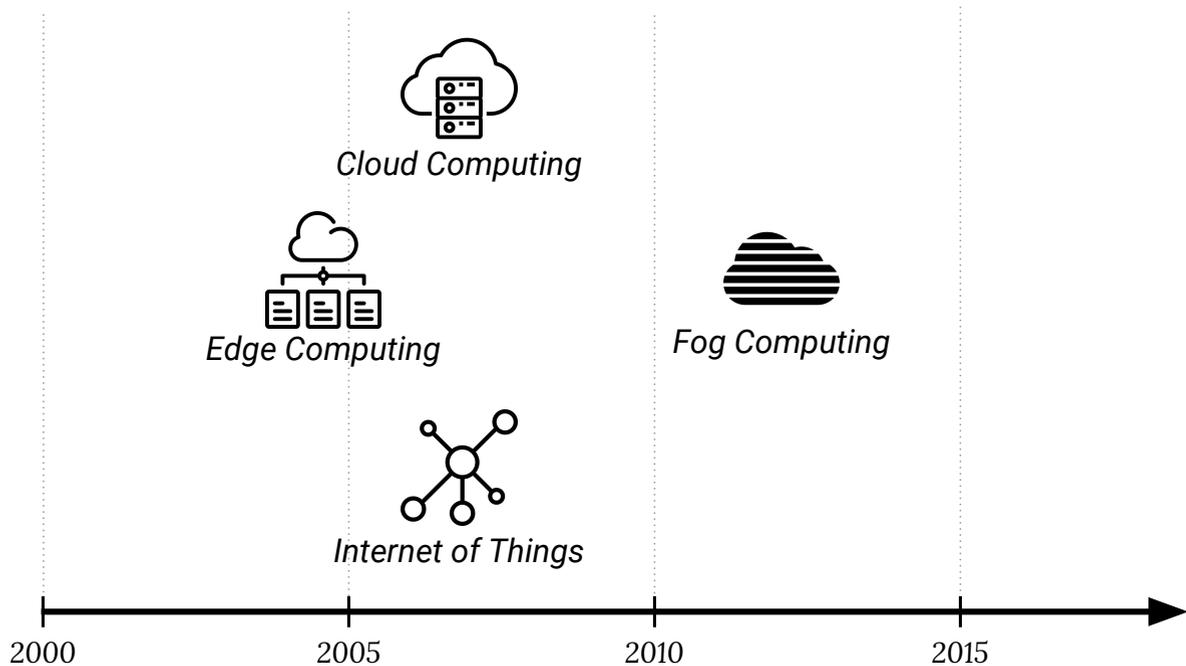
IEEE *Access*

FIGURE 1: First appearance of IoT, Cloud, Edge, and Fog computing in the literature.

years, with a sudden growth in 2017, when the number of publications has been more than duplicated for both of them.

Looking at the IoT curve, some interesting correlations can be observed. It appears that the interest in Edge and Fog computing is directly linked to Internet of Things. Indeed, with the increase of scientific papers about IoT, there is a growth of the interest in Edge and Fog computing. Conversely, the relation between IoT and Cloud computing seems to be opposite. In fact, the steady growth of attention for IoT of the last few years is slightly reducing the interest in Cloud computing.

D. COMMENT AND DISCUSSION

We are aware that the analysis conducted so far can be considered neither comprehensive nor exhaustive, because it is based on the presence or absence of keywords in the title of scientific documents and it only relies on two main digital libraries. Nevertheless, we think that the results are interesting and realistically represent research trends related to the major modern computing paradigms. Moreover, this work can represent a starting point for those interested in Edge and Fog computing, as in the rest of the paper we will drive the reader through the jungle of keywords and definitions available in literature and we will provide a structured picture of these paradigms on the basis of a careful analysis and comparison with related computing paradigms and concepts.

Cloud computing is undoubtedly the main computing paradigm of the last decade and it will still be a key research subject for several years. Nevertheless, the sudden spreading of IoT has undermined its strength. Indeed, there are several challenges related to IoT that Cloud computing can hardly

address. Therefore, the interest for Edge computing has increased, because of its aim of tackling the IoT challenges with the move of the computation at the edge of the network. In this transition, Fog computing made its way, embodying the rising paradigm that fully bridges the gap between Cloud computing and IoT.

This is the base on which the rest of the paper is built.

III. CLOUD COMPUTING

Nowadays, Cloud computing is a well-known paradigm. However, for the sake of readability and self-containment of the paper, we consider relevant to recap its basic notions. This also allows us to define a common terminology that is going to be used throughout the rest of the paper. For these reasons, fundamentals about Cloud computing are provided in this section.

A. DEFINITION AND ARCHITECTURE

NIST [18] defines Cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

The reference architecture for Cloud computing [19] is depicted in Figure 3. It provides a high-level overview of the Cloud and identifies the main actors and their role in Cloud computing. Each actor is an entity, i.e. a person or an organization, that either takes part in a transaction/process or performs some tasks in Cloud computing. There are five main
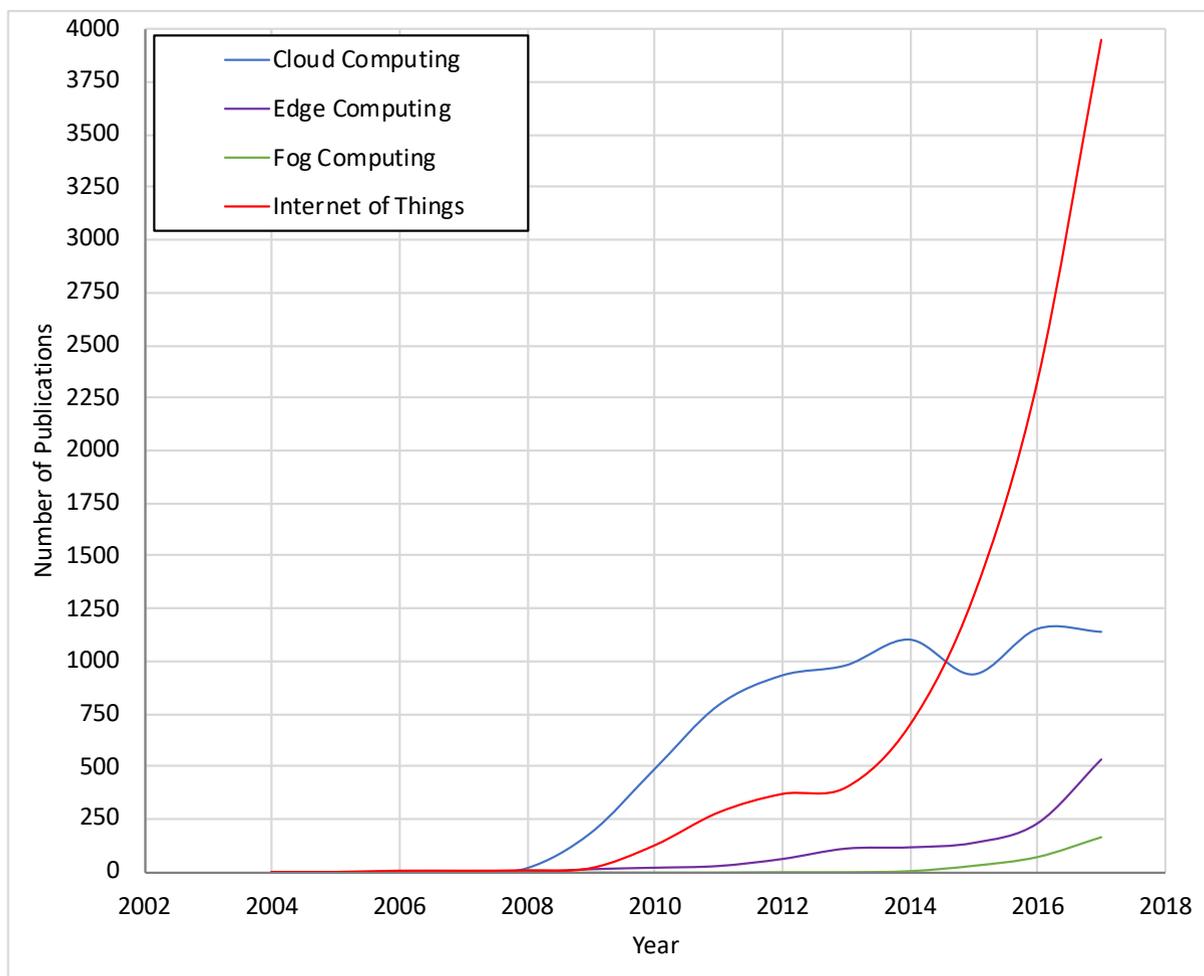
FIGURE 2: Temporal evolution of the number of scientific publications related to IoT, Cloud, Edge, and Fog computing. Databases used as sources: IEEE Xplore DL [6] and ACM DL [7]

actors: *Cloud Provider*, *Cloud Consumer*, *Cloud Broker*, *Cloud Carrier*, *Cloud Auditor*.

The *Cloud Provider* is an entity that provides a service to interested parties. The *Cloud Consumer* is an entity that uses a service from, and has a business relationship with, one or more Cloud providers. The *Cloud Broker* is an entity that mediates affairs between Cloud providers and Cloud consumers, and that manages the use, performance, and delivery of Cloud services. The *Cloud Carrier* is an intermediary that supplies connectivity and delivery of Cloud services from Cloud providers to Cloud consumers. Finally, the *Cloud Auditor* is a party that conducts independent assessments of the Cloud infrastructure, including services, information systems operations, performances, and security of the Cloud implementation.

In terms of interactions, there are several possible scenarios [19]. Generally, a Cloud consumer may request a Cloud service from a Cloud provider, either directly or via a Cloud broker. A Cloud auditor conducts independent audits and may contact other actors to collect the necessary information.

B. ESSENTIAL CHARACTERISTICS

The essential characteristics of Cloud computing are summarized below [18]:

- *On-demand self-service*: computing capabilities can be provided automatically when needed, without requiring any human interaction between consumer and service provider;
- *Broad network access*: computing capabilities are available over the network and accessible through several mechanisms disposable for a wide range of client platforms (e.g., workstations, laptops, and mobile devices);
- *Resource pooling*: computing resources are pooled to accommodate multiple consumers, dynamically allocating and deallocating them according to consumer demand. In addition, the provider resources are location independent, i.e. the consumer does not have any knowledge or control of their exact location;
- *Rapid elasticity*: computing capabilities can flexibly be provided and released to scale in and out according to demand. Thus, the consumer has the perception of unlimited, and always adequate, computing capabilities;
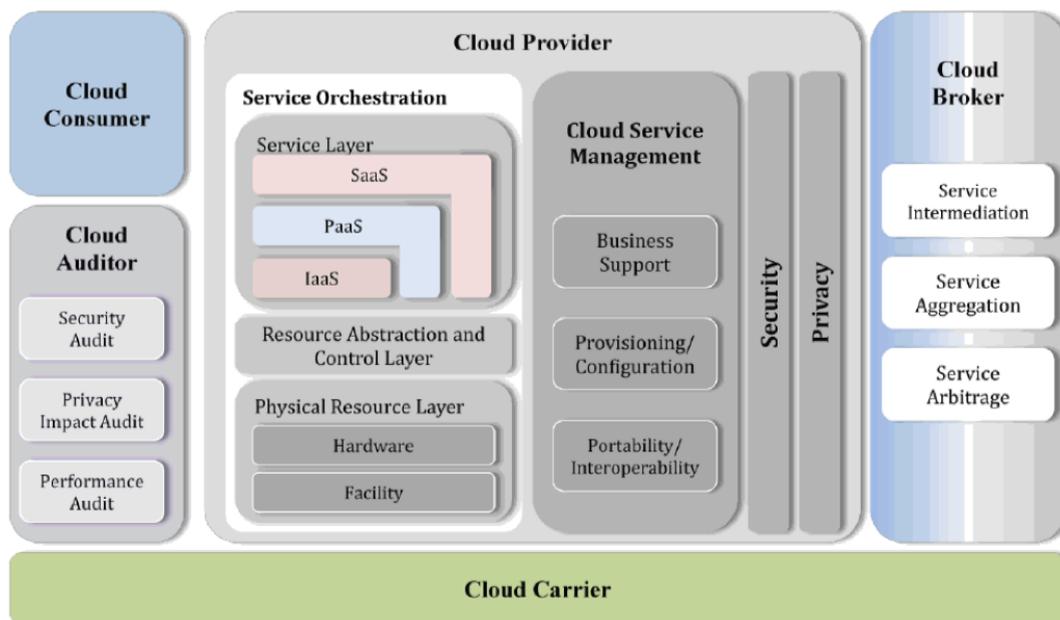
FIGURE 3: NIST Cloud computing reference architecture (source [19])

- *Measured service*: resource usage can be monitored and reported according to the type of service offered. This is particularly relevant in charge-per-use, or pay-per-user, services because it grants great transparency between the provider and the consumer of the service.

A *Cloud infrastructure* is a collection of hardware and software that empowers the aforementioned essential characteristics of Cloud computing.

IV. INTERNET OF THINGS

Over the past decade, Cloud computing has been the predominant paradigm. According to this trend, computing, control, and data storage have been centralized and moved into the Cloud [20]. On the other hand, Internet of Things (IoT) is now becoming widespread. In 2017, there were about 20 billion IoT connected devices and this number will grow to about 30 billion in 2020, and will more than duplicate by 2025[1]. The emerging IoT brings in many new challenges that Cloud computing has a hard time to meet, due to its own drawbacks.

In this section, we provide fundamentals about Internet of Things.

A. DEFINITION

The term "Internet of Things" was originally coined in 1999 by Kevin Ashton, executive director of the Auto-ID Center at Massachusetts Institute of Technology (MIT), and then it has assumed several slightly different meanings. Today, there is no unique and commonly accepted definition of IoT and several formalizations can be found on the web and in

the literature [21]–[24]. In this work, the definition given by the International and Telecommunication Union (ITU) is assumed: *Internet of Things* is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)" [25]. In this context, a *thing* is intended as "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks", while a *device* is "a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing" [25].

In simple, Internet of Things is a collection of computing devices (namely, *things*) interconnected via the Internet and aimed at offering services addressed to all types of applications, while security requirements are fulfilled [25].

B. ARCHITECTURE

A number of different IoT architectural models can be found in the literature [25]–[27], but, to the best of our knowledge, the most commonly used is based on three architectural levels [27]–[31]: *Perception* (or *Sensing*) *layer*, *Network* (or *Transmission*) *layer*, *Application layer*. The three-layer IoT architectural reference model is depicted in Figure 4. Each architectural layer is characterized by the devices that belong to it and by the functions performed.

The *Perception layer* has the aim of acquiring data from the environment (such as light, temperature, pressure, humidity, etc.) through the help of sensors and actuators. Basically, the main goal of this layer is the detection and collection of information before transmitting it to the network layer. The

---

[1]https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ *[Accessed on January 15th, 2018]*

Network layer is the middle one and its aim is to provide functions of data routing and transmission to the proper destination. Therefore, the main goal of this layer is efficiently transmitting data within heterogeneous networks and without losing information. Internet gateways, switches, routers, and other network devices operate at this layer. The *Application layer* is the highest one and it uses the information received from the bottom layers in order to implement different services and applications. This layer usually contains the user interface, the formulas related to data models, the business logic and all that is needed for the specific IoT service or application.

C. ESSENTIAL CHARACTERISTICS

The main features of Internet of Things are summarized below [24], [25], [32]:

- *Interconnectivity*: everything in IoT can be interconnected with the global communication and information infrastructure;
- *Things-related services*: IoT is able to provide thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical and virtual things;
- *Heterogeneity*: the devices in IoT can be based on different networks and/or hardware platforms. Moreover, they can interact with different service platforms and/or devices through different networks;
- *Constrained resources*: IoT usually involves devices characterized by energetic and computational constraints;
- *Dynamic changes & uncontrolled environment*: in IoT, the devices state (e.g., sleeping/awake, connected/disconnected) and context (e.g., location, speed) change dynamically. Therefore, IoT devices are part of an uncontrolled environment which is characterized by unstable surroundings and in which interactions among devices are unreliable due to both unstable network connectivity and device state dynamic changes. In addition, the number of devices can dynamically change;
- *Huge scale*: the number of devices that have to be managed and that have to communicate with each other is huge and it will be even more in the future. Moreover, the ratio of communications triggered by devices will steadily grow to the detriment of human-triggered communications. Even more critical will be the management and interpretation of data generated by such devices with the aim of sharing information with each other.

V. THE POST-CLOUD ERA

The emerging of IoT lets the post-Cloud era begin. Most of IoT data are currently processed in the Cloud, but the close interaction between Cloud and IoT introduces several new challenges that cannot be fully addressed by Cloud computing alone. In addition, there has been an increasing number and variety of smart clients and powerful edge devices, such as smartphones, tablets, edge routers, industrial and consumer robots, smart vehicles, etc.. In this context, Edge computing has become feasible and extremely interesting, and so has done Fog computing, as the highest evolution of the Edge computing principles.

In this section, we give a brief overview of the challenges that IoT drags in [17], [20], [33] and that are driving the increasing interest for Edge and Fog computing, as solutions to such difficulties [4].

Low Latency

Both industrial control systems [34] and IoT applications [17] often require low latency (within a few milliseconds) and jitter. This requirement is definitely not within reach of the Cloud computing paradigm.

High Network Bandwidth

The increasing number of IoT connected devices is increasingly generating a large amount of data [35]. Sending all this data toward the Cloud requires incredibly high network bandwidth and it is often useless or not permitted (e.g. due to data privacy concerns). Thus, the data generated at the edge of the network often needs to be stored and processed locally without involving the Cloud.

Limited Resources

Several IoT devices (such as sensors, drones, cars, etc.) have very limited resources. It means that they are not able to interact directly with the Cloud, since these interactions often require either complex protocols or intensive computation. As a result, devices with resources constraints have to rely upon an intermediate layer of devices to connect to the Cloud.

IT & OT Convergence

Recently, with the advent of Industry 4.0, industrial systems are experiencing the convergence of Operational Technology (OT)[2] and Information Technology (IT)[3] [36]. This trend brings new business priorities and operational requirements. Indeed, incessant and safe operation is often a priority in modern cyber-physical systems, since an offline system can cause a remarkable business loss or an unacceptable customer inconvenience. As a consequence, updating hardware and software in such systems is an issue. The result is the need for a new architecture that reduces the necessity of system updates over time.

Intermittent Connectivity

Some IoT devices (e.g., vehicles and drones) have intermittent network connectivity. As a result, it is difficult to provide uninterrupted Cloud services to such devices. Therefore, it is necessary to rely on an intermediate layer of devices to alleviate or solve the issue.

---

[2]Hardware and software systems used to monitor and control physical processes.
[3]Hardware and software systems used to process, transmit, and store business data.
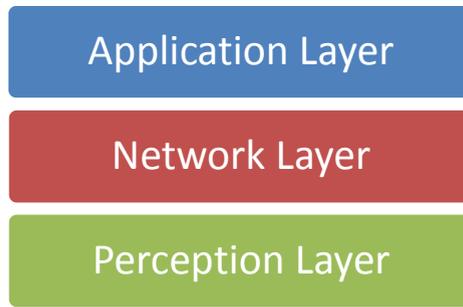
FIGURE 4: Three-layer IoT architectural model

Geographical Distribution

The great number of IoT devices requiring computation and storage services is distributed in vast geographical areas [37]. Therefore, it is hard to find a location for the Cloud infrastructure that allows meeting all the requirements of IoT applications. An intermediate layer of devices is useful to bridge this gap.

Context Awareness

Many IoT applications, such as vehicular networks and augmented reality, require to access and process local context information (e.g., user location, network conditions, etc.) [38]. This requirement does not fit the Cloud computing centralized approach due to the physical distance between IoT devices and central computing.

Security and Privacy

Emerging IoT security and privacy challenges are unique. Today, cybersecurity solutions aim at defending enterprises and consumers providing perimeter-based protection through firewalls, Intrusion Prevention Systems (IPSs), and Intrusion Detection Systems (IDSs). Unfortunately, this paradigm is no longer adequate to address the new security challenges that IoT brings in [31], [33].

Addressing these challenges requires radical changes to existing paradigms. That is where Edge and Fog computing come in, providing a new technological pattern aimed at creating the missing link in the Cloud-to-Things continuum.

VI. EDGE COMPUTING

Edge computing is an emerging paradigm born of necessity to move the computation at the edge of the network. Although the first appearance of Edge computing in the literature is previous to the Cloud, the increasing interest for Edge computing starts with the emerging of IoT and related new challenges.

In this section, we first describe the main idea behind Edge computing, then, we define the main implementations of the Edge computing paradigm, clarifying their difference: Mobile Cloud Computing (MCC), Cloudlet Computing (CC) and Mobile Edge Computing (MEC).

A. DEFINITION

According to [39], "Edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream data on behalf of Cloud services and upstream data on behalf of IoT services". Basically, the idea is to extend Cloud computing to the network edge with the aim of having the computation at the proximity of data sources, i.e., IoT devices.

This layer can be implemented in different ways. However, all the different implementations are designed with the Edge paradigm in mind, therefore many similarities are present.

B. EDGE COMPUTING IMPLEMENTATIONS

The Edge computing principles can be put in practice in several ways, in terms of the type of devices, communication protocols, and services [3], [4]. The major implementations of Edge computing are described below.

1) Mobile Cloud Computing & Cloudlet Computing

Mobile Cloud Computing (MCC) is based on the idea of mobile offloading: mobile devices should delegate storage and computation to remote entities in order to reduce the workload and optimize objectives like energy consumption, lifetime, and cost. MCC was originally conceived with the idea of moving data storage and data processing from inside mobile devices to the Cloud, bringing mobile applications to a wider range of users and not only to the ones with a powerful smartphone [40]. Today, the concept of MCC has been extended with the Edge computing paradigm in mind. The new vision is to delegate data processing and data storage to devices located at the edge of the network, rather than implementing them into the Cloud [38].

The most common implementation of this new vision of MCC is Cloudlet Computing (CC). Basically, CC consists of using cloudlets to perform data processing and storage close to end devices. A *cloudlet* is a trusted, small Cloud infrastructure, located at the edge of the network and available for nearby mobile devices [38], [41], that collaborates with the Cloud to compute the results and then sends them back to mobile devices [42].

2) Mobile Edge Computing

The *Mobile Edge Computing* (MEC) is an implementation of the Edge computing paradigm that brings Cloud computing capabilities (e.g., computation and storage) to the edge of the mobile network, inside the Radio Access Network (RAN) [38], [43]. MEC nodes are generally located with the Radio Network Controller or with a large base radio station [3].

The deployment of Cloud services inside the RAN provides several benefits, such as location/context awareness, low latency, and high bandwidth [38], [43].

3) Differences and Similarities

The aforementioned implementations of Edge computing share some features. First of all, they have the same aim: to extend Cloud capabilities to the edge of the network. Also, they rely upon a decentralized infrastructure, even though, it is accessible through different types of networks (e.g., wireless, mobile, Bluetooth) and composed of diverse devices (e.g., cloudlets, MEC nodes). In addition, all Edge implementations provide a set of benefits, mainly originated from the proximity to the edge of the networks: low latency, context and location awareness, high scalability and availability, and support to mobility.

Undoubtedly, even if these implementations share the same goal and a number of features, they present some differences. They can be deployed in different ways, both in terms of the type of devices and proximity to end users. For instance, the deployment of MEC nodes is linked to the mobile network infrastructure, while MCC has a wider scope. There are differences also in terms of entities eligible to own these infrastructures. For example, since MEC nodes are bound to the edge of the mobile network infrastructure, only telecommunication companies can provide MEC services, while any entity can deploy an MCC infrastructure.

Clearly, here we discussed only a subset of differences and similarities between Edge computing implementations. Detailed comparisons can be found in the literature [3], [38], [42], [44].

VII. FOG COMPUTING

Fog computing is often considered as an implementation of Edge computing [3], [38], [39], [42], [45]. Indeed, Fog computing provides distributed computing, storage, control, and networking capabilities closer to the user [46].

However, in our vision, Fog computing is not yet another implementation of Edge computing, it is rather the highest evolution of the Edge computing principles. Indeed, Fog computing is not limited to only the edge of the network, but it incorporates the Edge computing concept, providing a structured intermediate layer that fully bridges the gap between IoT and Cloud computing. In fact, Fog nodes can be located anywhere between end devices and the Cloud, thus, they are not always directly connected to end devices. Moreover, Fog computing does not only focus on the "things" side, but it also provides its services to the Cloud. In this vision, Fog computing is not only an extension of the Cloud

to the edge of the network, nor a replacement for the Cloud itself, rather a new entity working between Cloud and IoT to fully support and improve their interaction, integrating IoT, Edge and Cloud computing.

In this section, we define Fog computing and comment on its architectural model. Finally, we point out the main benefits of such a paradigm.

A. DEFINITION

The first definition of Fog computing dates back to 2012 when CISCO defined it as "a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud computing Data Centers, typically, but not exclusively located at the edge of network" [17]. Subsequently, several works have been defining Fog computing in the literature [20], [47]–[50].

Amongst others, Vaquero et al. [51] proposed a "comprehensive" definition of Fog computing: "Fog computing is a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third-parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so".

One year later, Yi et al. [52] came up with a similar definition of Fog computing: "Fog computing is a geographically distributed computing architecture with a resource pool consists of one or more ubiquitously connected heterogeneous devices (including edge devices) at the edge of network and not exclusively seamlessly backed by Cloud services, to collaboratively provide elastic computation storage and communication (and many other new services and tasks) in isolated environments to a large scale of clients in proximity".

In this work, we comply with the definition of Fog computing provided by the OpenFog Consortium [53], thus we consider Fog computing as "*a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things, thereby accelerating the velocity of decision-making*".

Analyzing this definition, some key concepts can be extrapolated. First, Fog computing is a *distributed* approach. It descends from its Edge computing nature and derives from the need for overcoming the limitations of the centralized approach of Cloud computing. Secondly, Fog nodes can be placed *anywhere* between end devices and Cloud infrastructure. This flexibility with the location of Fog nodes is one of the most distinctive features of Fog computing from the different implementations of Edge computing. Finally, the definition of Fog computing includes the *Cloud-to-Things continuum*. It remarks on the idea of Fog computing as a smart extension of Cloud computing aimed at bridging the

gap with IoT devices. Therefore, Fog computing should not be seen as a replacement of the traditional Cloud architecture, but rather as a new architecture that puts together Cloud computing, Edge computing, and IoT.

B. ARCHITECTURE

Over the last few years, defining the architectural model of Fog computing has been a hot research topic. Most of research works related to the topic refer to a three-layer architecture composed of Cloud, Fog, and IoT [31], [44], [47], [52], [54]. Furthermore, the OpenFog Consortium has defined a broader N-layer reference architecture [55], which can be considered a refinement of the three-layer one. In this subsection, an overview of the Fog architecture is given.

1) Three-layer Architecture

The essential three-layer architecture of Fog computing is depicted in Figure 5. It derives from the main idea of Fog computing as a non-trivial extension of Cloud computing in the Cloud-to-Things continuum. Indeed, it presents an intermediate layer (namely, the Fog layer) bridging the gap between Cloud infrastructure and IoT devices. The three layers composing the architecture are described below [44].

IoT Layer

This layer is composed of IoT devices, such as sensors, smart vehicles, drones, smartphones, tablet, etc. Usually, they are extensively geographically distributed and mainly aimed at sensing data and sending them to the upper layer for storage or processing. Nevertheless, devices with considerable computational capabilities (e.g., smartphones) might also perform some local processing before involving upper layers.

Fog Layer

This layer is the core of the Fog computing architecture. It is composed of a large number of Fog nodes. According to the OpenFog Consortium, a Fog node is "the physical and logical network element that implements Fog computing services" [53]. Fog nodes are able to compute, transmit, and temporary store data and they can be located anywhere between Cloud and end devices. As a result, on the one hand, Fog nodes are directly connected to end devices to offer services. On the other hand, they are connected to the Cloud infrastructure to both provide and obtain services. For instance, Fog nodes might benefit from Cloud storage and computational capabilities, while providing users' context information.

Cloud Layer

This layer is mainly composed of the centralized Cloud infrastructure (discussed in Section III). It is composed of several servers with high computational and storage capabilities, and provides different services. Differently from the traditional Cloud computing architecture, in the Fog architecture some computation or services might be proficiently moved from Cloud to Fog layer in order to reduce the load on Cloud resources and increase the efficiency.

2) OpenFog N-Tier Architecture

The N-tier architecture proposed by the OpenFog Consortium [55] is depicted in Figure 6. It is mainly aimed at giving an inner structure to the Fog layer of the three-layer architecture (Subsection VII-B1), driving the stakeholders when it comes to deploying Fog computing in a specific scenario. Indeed, although the deployment of Fog software and Fog systems is scenario-specific, the key features of the Fog architecture remain evident in any Fog deployment.

The idea is to have, again, three main entities (matching the three-layer architecture proposed in Subsection VII-B1): endpoints/things, Fog nodes, Cloud. However, the Fog layer is further composed of several tiers of Fog nodes (N-tiers) and, the farther nodes move away from end devices, the more they gain computational capabilities, thus intelligence. Each upper level in the Fog layer increasingly refines and extracts relevant data, rising the intelligence at each level. The number of tiers in a specific deployment depends on the scenario requirements, such as: number of end devices, load and type of work addressed by each tier, capabilities of nodes at each tier, latency requirements, and so on. In addition, Fog nodes on each layer might be linked together to form a mesh able to provide additional features, such as resilience, fault tolerance, load balancing, and so on. It means that Fog nodes are able to both communicate horizontally and vertically within the Fog architecture.

In this N-tier vision, Fog nodes can be grouped according to their proximity to endpoints and Cloud:

- *lowest tier*: Fog nodes in the lowest layer usually command and control sensors and actuators and are mainly focused on acquiring, normalizing, and collecting data;
- *intermediate tiers*: Fog nodes in the intermediate layers are mainly focused to filter, compress, and transform data received from the lower layer. In general, these nodes have more analytic capabilities;
- *highest tier*: Fog nodes nearest to the Cloud are typically in charge of aggregating data and building knowledge out of them.

C. THE BENEFITS OF FOG COMPUTING

Fog computing is a distributed paradigm acting as an intermediate layer between Cloud computing and IoT [56]. As such, it serves as the glue between Cloud computing, Edge computing, and IoT. This is the hallmark of Fog computing, but it also drags a number of benefits that it is relevant to point out.

Although the advantages of Fog computing are usually summarized as *CEAL* [20], [50], we believe that *Security* is one of them, thus we refer to the advantages of Fog computing as *SCALE* [46]: *Security*, *Cognition*, *Agility*, *Latency*, *Efficiency*.
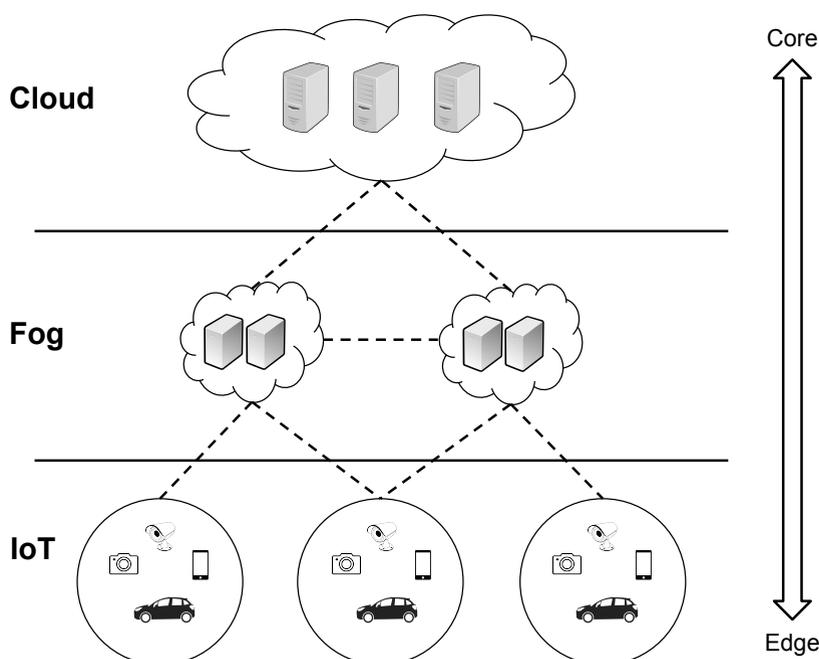
FIGURE 5: 3-tier architecture of Fog computing.

Security

The Fog paradigm offers a new perspective on security. In this context, security is considered a base building block of the architecture rather than an additional, and often overlooked, feature to add on top of it. As a matter of fact, the OpenFog Consortium [57] is actively working on the definition of a reference architecture of Fog computing that has security as the first pillar [55]. Particularly, the OpenFog Security Group (SWG) has drawn up the main security goals of Fog computing [58] that we have reinterpreted and summarized as follows:

- *Security as a Pillar (SECaaP)*: Fog computing as an intrinsically secure paradigm itself, that takes over the role of responsive, available, survivable, and trusted part in the Cloud-to-Things continuum;
- *Security as a Service (SECaaS)*: Fog computing as a security service provisioned to other entities, ranging from powerful Cloud servers to weak IoT devices. Thanks to the proximity of Fog nodes to these entities, the Fog infrastructure can both offer basic security services (e.g., protecting resource-constrained endpoints that often cannot adequately secure themselves) and improve existing security solutions (e.g., strengthening mechanisms for identity verification) [46]. This should be accomplished without interfering with the business process of the involved applications/services and respecting their domain structure.

Cognition

The Fog infrastructure is aware of customers requirements and objectives, thus it distributes more finely computing,

communication, control, and storage capabilities along the Cloud-to-Things continuum, building applications that better meet clients' needs.

Agility

The development of a new service is usually slow and expensive, due to the cost and time needed by large vendors to initiate or adopt the innovation. The Fog world, instead, offers rapid innovation and affordable scaling, being an open marketplace where individuals and small teams can use open development tools (e.g., APIs and SDKs) and the proliferation of IoT devices to offer new services.

Latency

The Fog architecture supports data processing and storage close to the user, resulting in low latency. Thus, Fog computing perfectly meets the request for real-time processing, especially for time-sensitive applications.

Efficiency

The Fog architecture supports the pooling of computing, communication, control, and storage functions anywhere between Cloud and IoT. In this vision, the Fog infrastructure "pushes" capabilities from the Cloud and "pulls" capabilities from powerful IoT devices (e.g., smartphones, tablets, laptops, etc.), integrating them in the Fog infrastructure, increasing the overall system performance and efficiency.

In the literature, a number of other advantages and characteristics of Fog computing are discussed, often with a different
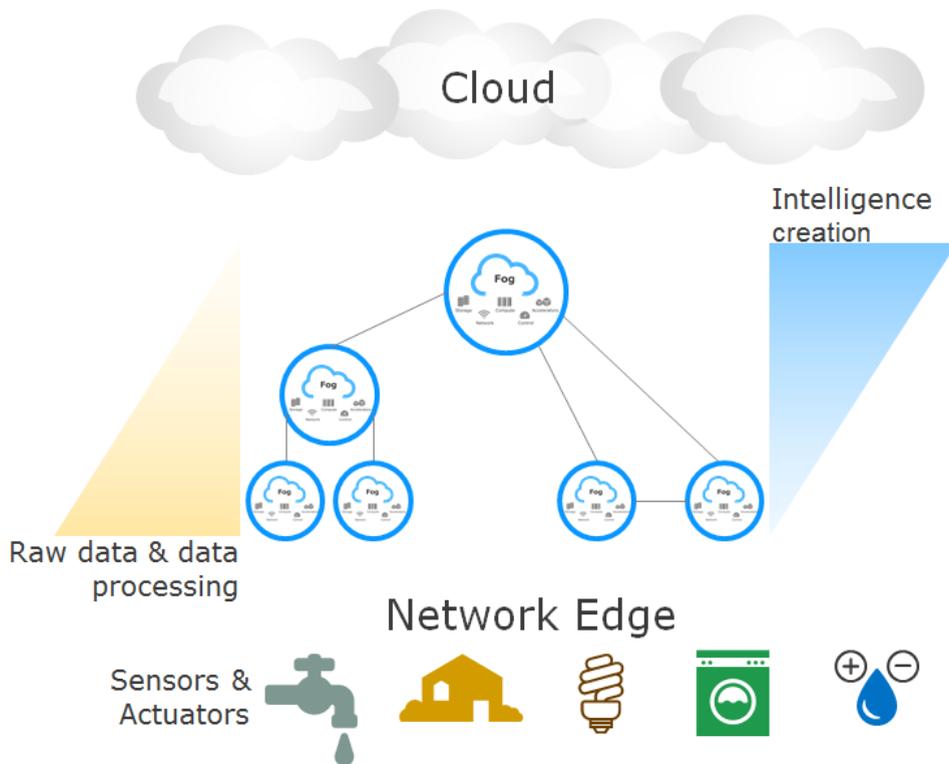
FIGURE 6: OpenFog N-tier architecture of Fog Computing (source: [55])

outline [17], [44], [49], [52], [54], [56]. Nevertheless, we believe that the advantages presented in this section are generic enough to be considered the key concepts from which the other features derive.

VIII. OPEN CHALLENGES

Described the IoT, Cloud, Edge, and Fog paradigms, a natural question arises: what are the main technical challenges that community has still to address in order to realize the potential of each paradigm? This section aims at giving a first tentative answer to this question. We do not aim to extensively review all the technical challenges affecting these paradigms, but we want to give a brief overview of some of the key open challenges that, in our opinion, should be part of future research directions in the field.

A. CLOUD COMPUTING

Despite being around for the longest amount of time, Cloud computing still faces numerous challenges.

In particular, many parties involved in Cloud computing see Cloud security as a challenge [59]. Researchers have also identified the reliability of services provided by the Cloud as a major issue. When critical functionality is provided by a small number of data centres, it might prove disastrous if one of the data centres becomes unavailable. Research efforts to mitigate this focus on minimizing the overhead incurred from disaster recovery, and improving VM migration techniques [60].

Sustainability is another challenge that warrants more research [61]. Cloud data centres require vast amounts of energy to work, and research is being done to minimize energy usage through by optimizing resource provisioning and management policies, but also by other means such as the investigation of new system architectures [60].

Cloud networking infrastructure has a number of open issues of its own, as identified by Moura and Hutchison in [62]. Some notable issues are related to network utilization, data congestion, Cloud federation, and network-capable Hypervisors.

B. IOT

With the advent of smart devices, there has been a trend towards minimization of energy/resource consumption. Increasing battery life and otherwise optimizing the energy usage of connected devices is seen as one of the major challenges [63] in this field. Promising advances are being made in various directions, such as wireless energy harvesting [64].

The security of IoT devices is identified by many as a critical field that is full of open challenges. These challenges cover both physical security and software security. Some identified challenges relate to lightweight authentication protocols, low-power networks, and awareness/education [65]. There are also various open challenges regarding forensics in IoT networks [66].

Privacy is closely related to this and plays a large role for IoT devices that users might directly interact with. This type of devices faces unique challenges regarding the privacy of its

users, e.g. when collecting health-related data. Research into privacy models that can manage the complexity of determining which devices in an IoT network have (and should have) access to privacy-sensitive data is an open challenge [66].

Silva et al. [67] state that there is a need for evaluation of holistic IoT approaches, where interaction between multiple systems as well as Cloud infrastructure is taken into account, instead of focusing on the capabilities of one component. Other open challenges identified in their work relate to high-availability IoT networks, reliability, scalability, and interoperability. Interoperability is also discussed in [68], wherein the authors argue that one aspect that makes this particularly challenging is that the most lightweight devices can be extremely constrained in their capabilities, but must still be able to communicate and interoperate with other devices.

C. EDGE COMPUTING

Edge computing, with its idea of moving the computation at the edge of the networks, drags a number of challenges that are still to be addressed.

Shi et al. [39] identify programmability of Edge devices as a challenge. Currently, there is a large gap in flexibility between programmability of Cloud services and Edge devices, which needs to be addressed. Secondly, there exists a need for naming schemes that can handle the vast amount of devices that the Edge is predicted to provide. These schemes should fit in highly dynamic environments. Additionally discussed challenges relate to security and privacy, data abstraction, service management, and optimization problems.

Another perspective is explored by Li et al. [69], wherein they consider network openness (to various parties), exploring multi-service operations and new business models, robustness and resilience, and security and privacy as the major challenges for Edge computing.

D. FOG COMPUTING

Fog computing is still in its infancy, thus, there are many open research challenges.

Given its correlation with Edge computing, many of the challenges in Fog are similar to those faced by Edge computing. Therefore, it is not surprising that programmability and the ability to deal with heterogeneous systems are seen as open challenges in the Fog computing domain [70]. Additionally, the authors of this work consider security, interoperability and energy/resource efficiency to be major challenges for industrial applications of Fog computing.

In their comprehensive survey on the state of Fog computing, Mouradian et al. [71] state that the most pressing challenges in Fog computing relate to heterogeneity, QoS management, scalability, mobility, federation and interoperability. As can be seen, this is in line with [70] and generally covers similar themes to those challenges faced by the Cloud as well as the Edge. However, each of these domains has its own set of requirements to fulfil, implying different solutions are needed as well. For example, federation is of much higher importance to Fog computing than it is to Cloud

computing, as there will be many more (clusters of) nodes communicating with each other in the Fog paradigm. And while heterogeneity is an issue for both the Fog and the Edge, it is expected that Fog devices will be more uniform in their capabilities than Edge devices.

IX. CONCLUSION

Nowadays, Internet of Things, Cloud computing, Edge computing, and Fog computing represent the most advanced computing paradigms. However, with a first look at the literature, it might be difficult to fully understand their main differences and similarities, as well as, the way they relate to each other. In this light, our work provides clarification about those concepts resulting in what can be considered a first paper to be read for those who start their research in Edge and Fog computing.

First, we gave an idea of how the different paradigms evolved and what the main research trends are today. Then, starting from this global picture, we focused on each of the paradigms, explaining main characteristics, architecture, and main features, along with considerations on how they interact and influence each other. We concluded by remarking how relevant Fog computing is and arguing that Fog is the glue that keeps IoT, Cloud and Edge computing together. Also, a brief overview of open challenges and future research directions for IoT, Cloud, Fog, and Edge computing was provided as food for thought.

This manuscript was born from the necessity of providing a clear picture of the current state of computing paradigms and their relation. This is the kind of work that we would have liked to find in the literature when we first started digging into Edge and Fog computing, thus, we consider it a helpful resource for those who will start next.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] W. Shi and S. Dustdar, "The promise of edge computing," Computer, vol. 49, no. 5, pp. 78–81, 2016.

[3] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in 2017 Global Internet of Things Summit (GIoTS), June 2017, pp. 1–6.

[4] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: Architecture, challenges, and optimization," IEEE Access, vol. 5, pp. 25 445–25 454, 2017.

[5] OpenFog Consortium, "Glossary of terms related to fog computing," 2018, [Accessed on July 10th, 2018]. [Online]. Available: https://goo.gl/cS7un3

[6] IEEE Xplore Digital Library. [Accessed on July 10th, 2018]. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[7] ACM Digital Library. [Accessed on July 10th, 2018]. [Online]. Available: https://dl.acm.org/

[8] H. H. Pang and K. L. Tan, "Authenticating query results in edge computing," in Proceedings. 20th International Conference on Data Engineering, March 2004, pp. 560–571.

[9] R. Grieco, D. Malandrino, and V. Scarano, "Secs: Scalable edge-computing services," in Proceedings of the 2005 ACM Symposium on Applied Computing, ser. SAC '05. New York, NY, USA: ACM, 2005, pp. 1709–1713.

[10] Google Press Center. (2006) [Accessed on July 10th, 2018]. [Online]. Available: https://www.google.com/press/podium/ses2006.html

[11] Amazon Web Service website. (2006) [Accessed on July 10th, 2018]. [Online]. Available: https://goo.gl/gU82sF

[12] B. Hayes, "Cloud computing," Commun. ACM, vol. 51, no. 7, pp. 9–11, Jul. 2008.

[13] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in 2008 10th IEEE International Conference on High Performance Computing and Communications, Sept 2008, pp. 5–13.

[14] K. Ashton, "That 'Internet of Things' thing," RFID Journal, June 1999.

[15] R. A. Dolin, "Deploying the "internet of things"," in International Symposium on Applications and the Internet (SAINT'06), Jan 2006, pp. 4 pp.–219.

[16] J. P. Conti, "The internet of things," Communications Engineer, vol. 4, no. 6, pp. 20–25, Dec 2006.

[17] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC '12. New York, NY, USA: ACM, 2012, pp. 13–16.

[18] P. Mell, T. Grance et al., "The NIST Definition of Cloud Computing," Tech. Rep., 2011.

[19] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture," Tech. Rep. 2011, 2011.

[20] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, Dec 2016.

[21] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[22] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," Journal of Computer and Communications, vol. 3, no. 05, pp. 164–173, 2015.

[23] C. Folk, C. D. Hurley, K. W. Kaplow, and P. X. F. James, "The security implications of the Internet of Things," February 2015.

[24] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Enabling consumer trust upon acceptance of iot technologies through security and privacy model," in Advanced Multimedia and Ubiquitous Engineering: FutureTech & MUE. Springer, 2016, pp. 111–117.

[25] ITU-T, "Overview of the Internet of Things," International Telecommunication Union, Recommendation Y.2060, June 2012.

[26] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, February 2015.

[27] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), Dec 2015, pp. 336–341.

[28] K. Sonar and H. Upadhyay, An Approach to Secure Internet of Things Against DDoS. Springer Singapore, 2016, pp. 367–376.

[29] R. Ravindran, J. Yomas, and J. E. Sebastian, "IoT: A review on security issues and measures," International Journal of Engineering Science and Technology, vol. 5, no. 6, pp. 348–351, December 2015.

[30] Q. Gou, L. Yan, Y. Liu, and Y. Li, "Construction and strategies in IoT security system," in 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Aug 2013, pp. 1129–1132.

[31] 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.

[32] P. Saichaitanya, N. Karthik, and D. Surender, "Recent trends in IoT," in 4th International Conference on Recent Trends in Engineering Science and Management, August 2016, pp. 318–326.

[33] T. Zhang, Y. Zheng, R. Zheng, and H. Antunes, Securing the Internet of Things. John Wiley & Sons, Inc., 2017, pp. 261–283.

[34] M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikolié, "Design of a low-latency, high-reliability wireless communication system for control applications," in 2014 IEEE International Conference on Communications (ICC), June 2014, pp. 3829–3835.

[35] R. Kelly. (2015, April) Internet of Things Data To Top 1.6 Zettabytes by 2020. [Accessed on July 25th, 2018]. [Online]. Available: https://goo.gl/2YxB5M

[36] D. Harp and B. Gregory-Brown, "IT/OT Convergence-Bridging the Divide," Tech. Rep., 2014.

[37] M. Yannuzzi, M. R., R. Serral-Gracià, D. Montero, and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing," in 2014 IEEE 19th International Workshop

on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Dec 2014, pp. 325–329.

[38] 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.

[39] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Oct 2016.

[40] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless communications and mobile computing, vol. 13, no. 18, pp. 1587–1611, 2013.

[41] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-Based Cloudlets in Mobile Computing," IEEE Pervasive Computing, vol. 8, no. 4, pp. 14–23, Oct 2009.

[42] M. Gusev and S. Dustdar, "Going Back to the Roots - The Evolution of Edge Computing, An IoT Perspective," IEEE Internet Computing, vol. 22, no. 2, pp. 5–15, Mar 2018.

[43] P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," IEEE Communications Surveys Tutorials, vol. 19, no. 3, pp. 1628–1656, thirdquarter 2017.

[44] 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, 2017.

[45] C. Li, Y. Xue, J. Wang, W. Zhang, and T. Li, "Edge-oriented computing paradigms: A survey on architecture design and system management," ACM Comput. Surv., vol. 51, no. 2, pp. 39:1–39:34, Apr. 2018.

[46] M. Chiang, S. Ha, I. Chih-Lin, F. Risso, and T. Zhang, "Clarifying fog computing and networking: 10 questions and answers," IEEE Communications Magazine, vol. 55, no. 4, pp. 18–20, April 2017.

[47] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, 2014, pp. 1–8.

[48] 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. ACM, 2015, pp. 37–42.

[49] S. Chen, T. Zhang, and W. Shi, "Fog computing," IEEE Internet Computing, vol. 21, no. 2, pp. 4–6, 2017.

[50] M. Chiang, B. Balasubramanian, and F. Bonomi, Fog for 5G and IoT. John Wiley & Sons, 2017.

[51] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," SIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 27–32, October 2014.

[52] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), Nov 2015, pp. 73–78.

[53] OpenFog Consortium Architecture Working Group and others, "OpenFog architecture overview," White Paper, February 2016.

[54] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing Fog Computing for Internet of Things applications: Challenges and solutions," IEEE Communications Surveys & Tutorials, 2017.

[55] OpenFog Consortium Architecture Working Group and others, "OpenFog Reference architecture for Fog Computing," OPFRA001, vol. 20817, February 2017.

[56] R. Mahmud, R. Kotagiri, and R. Buyya, Fog Computing: A Taxonomy, Survey and Future Directions. Singapore: Springer Singapore, 2018, pp. 103–130.

[57] OpenFog Consortium. [Accessed on July 25th, 2018]. [Online]. Available: https://www.openfogconsortium.org/

[58] B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "Openfog security requirements and approaches."

[59] S. Durcevic. (2019) [Accessed on Sept 4th, 2019]. [Online]. Available: https://www.datapine.com/blog/cloud-computing-risks-and-challenges/

[60] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849 – 861, 2018.

[61] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," in 2015 International Conference on Computational Intelligence and Networks, Jan 2015, pp. 116–123.

[62] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," Journal of Network and Computer

Applications, vol. 60, pp. 113 – 129, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S108480451500288X

[63] Z. Abbas and W. Yoon, "A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects," Sensors, vol. 15, no. 10, pp. 24 818–24 847, 2015.

[64] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," IEEE Communications Magazine, vol. 53, no. 6, pp. 102–108, 2015.

[65] V. Adat and B. B. Gupta, "Security in internet of things: issues, challenges, taxonomy, and architecture," Telecommunication Systems, vol. 67, no. 3, pp. 423–441, 2018.

[66] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544 – 546, 2018.

[67] B. N. Silva, M. Khan, and K. Han, "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges," IETE Technical Review, vol. 35, no. 2, pp. 205–220, 2018.

[68] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," Mobile Networks and Applications, vol. 24, no. 3, pp. 796–809, 2019.

[69] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile Edge Computing: Progress and Challenges," in 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), March 2016, pp. 83–84.

[70] I. Bouzarkouna, M. Sahnoun, N. Sghaier, D. Baudry, and C. Gout, "Challenges Facing the Industrial Implementation of Fog Computing," in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Aug 2018, pp. 341–348.

[71] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp. 416–464, Firstquarter 2018.

MICHELE DE DONNO is a PhD Student at DTU Compute, Technical University of Denmark (Denmark), under the supervision of Prof. Nicola Dragoni. He got an M.Sc. Degree (cum laude) in Computer Engineering from Politecnico di Torino, Turin (Italy), in 2017 and a B.Sc. Degree in Computer Engineering from Politecnico di Bari, Bari (Italy), in 2014. His main research interests include cyber-security, networking, Internet-of-Things, and Fog computing.

KOEN TANGE is a PhD student at DTU Compute, Technical University of Denmark (Denmark), under the supervision of Prof. Nicola Dragoni. He received a B.Sc in Software Science at Eindhoven University of Technology (TU/e), Eindhoven, the Netherlands, in 2016. Afterwards, in 2018, he received a joint M.Sc. degree in Engineering, Security, and Mobile Computing from the Technical University of Denmark, Lyngby, Denmark, and Aalto University, Espoo, Finland, as part of the Nordic Masters Programme in Security and Mobile Computing. His research interests include information security, Fog computing, trusted hardware, and distributed systems.

NICOLA DRAGONI is Associate Professor in Distributed Systems and Security at DTU Compute, Technical University of Denmark, Denmark, and Professor in Computer Engineering at Centre for Applied Autonomous Sensor Systems, Örebro University, Sweden. He is also affiliated with the Copenhagen Center for Health Technology and the Nordic IoT Hub. He got a M.Sc. Degree (cum laude) and a Ph.D. in Computer Science at University of Bologna, Italy. His main research interests lie in the areas of pervasive computing and security, with focus on domains like Internet-of-Things, Fog computing and mobile systems. He has co-authored 100+ peer-reviewed papers in international journals and conference proceedings, and he has edited 3 journal special issues and 1 book.