Citation:
Mahmood, Z and Ramachandran, M (2018) "Fog computing: Concepts, principles and related paradigms." In: Fog Computing: Concepts, Frameworks and Technologies. Springer, pp. 3-21. ISBN 9783319948898 DOI: https://doi.org/10.1007/978-3-319-94890-4_1

Link to Leeds Beckett Repository record:
https://eprints.leedsbeckett.ac.uk/id/eprint/7423/

Document Version:
Book Section (Accepted Version)

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.

The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please contact us and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on openaccess@leedsbeckett.ac.uk and we will investigate on a case-by-case basis.

Chapter 36:

Fog Computing: Concepts, Principles and Related Technologies

Zaigham Mahmood* and Muthu Ramachandran**

*Debesis Education, Derby, UK
Shijiazhuang Tiedao University, Hebei, China
**Leeds Becket University, Leeds, UK

Corresponding Author Email: dr.z.mahmood@hotmail.co.uk

Abstract: Fog Computing, sometimes also referred to as Edge Computing, extends the Cloud Computing paradigm to lower latency, improve location awareness, provide better support for mobility and increase business agility. There is necessarily a requirement for these attributes in this age of Internet of Things (IoT) where, according to one estimate, there will be close to 50 billion interconnected smart devices by 2020 and the amount of Big Data generated by these devices is expected to grow to around 200 exabytes per year by 2020. The core characteristic of the Fog Computing architecture is that it provides compute and data analytics services more immediately and close to the physical devices that generate such data, ie at the *Edge* of the network, and thus bypassing the wider Internet. In this chapter, we discuss the Fog paradigm, its concepts, principles, present the difference between the Cloud and Fog architectures, and briefly discuss the OpenFog Reference Architecture. Hopefully, this chapter will set a scene for the various Fog-related topics presented in the rest of this book.

Keywords: Fog Computing, Cloud Computing, Edge Computing, Mobile Computing, Mobile Edge Computing, Cloudlet, OpenFog Reference Model, Networking, Smart Devices, IoT, Internet of Things

1.0 Introduction

Ubiquitous deployment of smart devices (such as mobile phones, tablets, sensors, motors, relays and actuators) connected though the IoT is estimated to reach 50 billion units by 2020 [1]. The data generated by these devices as well data from newly-connected factories, homes communities, cars, hospitals and more is expected to grow from 1.1 zettabytes (or 89 exabytes) per year in 2016 to 2.3 zettabytes (or 194 exabytes) per year by 2020 [19]. Managing such amounts of data, as well as data generated by social media technologies (such as Facebook, Twitter, etc) is one of the biggest challenges, which the traditional IoT and Cloud based architectures are unable to cope with. The reason being the large scale and variety of data, often known as Big Data, heterogeneity of the IoT devices, differing connectivity protocols, lack of suitable standards, and high latency of the Cloud-based environments and systems. One solution is to *decentralise applications,*

management and data analytics into the network itself using a distributed and federated compute model [7, 9].

Fog Computing [1], a term created by Cisco, is sometimes also referred to as Edge Computing [9], Mist Computing, Fogging, or Cloudlets. Although, there are some subtle differences between these different terms, at a higher level, the terms can be regarded as synonyms. The term "Fog computing" or "Edge computing" means that rather than hosting and working from a centralized Cloud, Fog systems operate on network ends. It is a term for placing some processes and resources at the edge of the Cloud, instead of establishing channels for Cloud storage and utilization [8, 6].

Fog Computing appears to be the next big thing for the Inter of Everything (IoE). According to one research [23], the Fog Computing market is currently valued at $22.3 million in 2017 and is expected to expand at an explosive rate and grow to $203.5 million over the next five years.

In this chapter, we attempt to present, first, the various definitions of this emerging paradigm known as Fog Computing and characterise some core aspects of Fogging; then we link it up to the Cloud paradigm discussing the limitations and inherent difficulties of Cloud environment and how Fogging may possibly address the related issues. We also articulate the subtle differences between Fog Computing and Edge Computing; and also suggest a layered approach to visualise where exactly Cloud, Fog and Mist Computing may be placed in a wider context of a Cloud-based system serving smart end-user devices in a distributed IoT environment.

1.1 Fog Computing

Fog computing is a way of providing compute and storage services more immediately and close to the physical devices of an organisation [6], ie at the *Edge* of the Cloud network, and thus bypassing the wider internet. Fog computing can really be thought of as a way of providing services more immediately, but also as a way of bypassing the wider internet, whose speeds are largely dependent on carriers [6].

NIST (Special Publication 800-191 (Draft) [5]) define it as horizontal, physical or virtual resource paradigm that resides between smart end-devices (that generally reside within the organisations) and traditional Cloud computing or connected data centers. According to the OpenFog Consortium [20], Fog Computing is *a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a Cloud-to-thing continuum*. It is a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers [9, 10].

The Fog paradigm provides reduced latency and context awareness because of the localisation of Fog nodes; and supports *vertically-isolated latency-sensitive applications by providing ubiquitous, scalable, layered and federated network connectivity* [9]. Fog nodes deploy and provision same types of services as provisioned by Cloud computing viz: SaaS, PaaS and IaaS. Additionally, the Fogging architecture uses one or more collaborative end-user clients or near-organisation Edge devices to carry out a substantial amount of communication, control, configuration, measurement and management services. It is a paradigm that extends Cloud Computing services to the edge of the network. The distinguishing characteristic being that: whereas Cloud environment may be geographically a long way away from the organisation, often not even knowing where the Cloud-based services actually reside and relying heavily on the wider Internet bandwidths; Fog services are much closer to end-users, with dense geographical distribution, and much better support for mobility.

As presented in Fig 1, Fog Computing Characteristics include the following [9]:

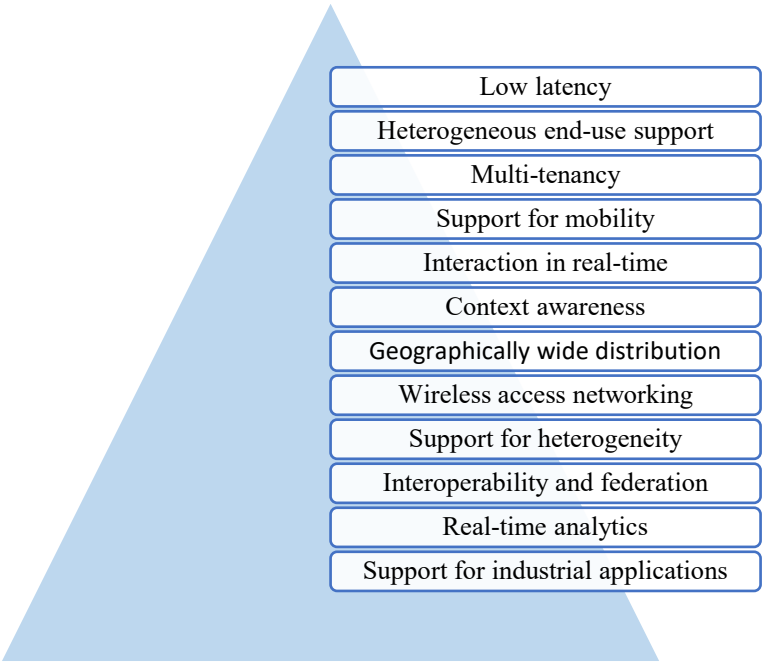

Fig 1: Fog Computing Characteristics

- Low latency – because of closeness of Fog nodes to the on-premise end-point devices, resulting in response and analysis in a much quicker time frame
- Rich and heterogeneous end-use support – because of proximity of Edge devices to the compute nodes
- Multi-tenancy in controlled environment – because of highly virtualised platform
- Better support for mobility – because of more direct communication between the Fog applications and the mobile devices
- Interaction in real-time – as opposed to batch processing as, for example, in case of Cloud-based applications
- Context awareness – as the devices and nodes in the environment have knowledge and understanding of the environment
- Geographical distribution – as fog environment is geographically distributed; so it plays active role in delivery of high quality of streaming services
- Wireless access networking – that is more appropriate for wireless sensing devices that require time-distributed analysis and communication
- Support for heterogeneity – as the Fog nodes come in different form factors, and deployed in a variety of distributed environments
- Seamless interoperability and better federation – for better communication between devices from various vendors and across various domains
- Analytics in real-time – which is easily possible because of ingestion and processing of data close to the source
- Support for a wide variety of industrial applications – through processing and analysis in real time

These characteristics are useful when devising Fog computing driven applications such as smart cities, smart home, smart health, and eminent applications such as emergency response systems for flood monitoring and recovery. Varshney and Simmhan [24] discusses three essential characteristics such as resource, physical presence and access, and mobility that distinguishes fog computing from the characteristics of edge and cloud computing. In addition, the wider Fog paradigm is composed mainly of two other technologies [1]:

- Cloudlets: These are applications located on the edge of the network [12], mainly to respond to low-latency in machine communications. A Cloudlet is a Fog node, resource-rich computer - or cluster of computers (a datacentre in a box), that is well-connected to the Internet and available for use by localised mobile devices. Fog nodes can be either physical or virtual elements and are tightly coupled with the smart end-devices or access networks. These have four major attributes: self-managing, having computer power, low end-to-end latency, and based on Cloud technology. In the network architecture, cloudlets reside in the middle of the 3-part *mobile device – cloudlet – Cloud* structure.
- Mobile Edge Computing (MEC): This is a technology related to mobile networking, within the Radio Access Network (RAN) and in close proximity to mobile subscribers [13]. It is a network architecture that enables cloud computing capabilities and an IT service environment at the edge of the cellular network. The underlying idea is that related processing is closer to the cellular customers, that in turn helps to reduce network congestion and increase application performance.

As for the advantages of Fogging, a closer look at the Fog model suggests that it is about taking decisions as close to the data and sources of generation of data as possible. Hadoop and other big data solutions have started the trend to bring processing closer to the location of data. Fogging is about doing the same on a larger scale. There are obvious advantages in taking decisions as close to where the data generation taking place and not needing for certain data to be processed in the Cloud [6]. This, in turn, resolves the issues of security and privacy as well. Only valuable data should be traveling Cloud computing networks. Some of the advantages include:

- Dense geographical distribution and support for mobility
- Low latency, location awareness and improved QoS
- Greater business agility and reduced operating costs.

These advantages of Fog computing concepts and principles need to be considered when designing applications with some of the key service design principles of loose coupling, scalability, and business process modelling and simulation will hep to predict the Fog computing characteristics discussed in this section. However, there are some issues to be considered that are similar to cloud computing research issues such as security and privacy, resource management, and communication protocols.

1.1.1 Fog Computing Issues

Although, the promise of Fog paradigm is attractive, it is important to note and understand the different issues that come with the use and deployment of Fog Computing. Besides the issues inherited from Cloud Computing, some of Fog-related issues refer to the following:

Security and Privacy

Most security related issues of distributed computing environments apply to Fog paradigm, nature of some of these issues are subtly different because of the Fog nodes residing at the edge of the network, close to the devices in the network. Main issues relate to client authentication at different levels of gateway, as well as at the level of networked devices. As an example, consider a smart meter that is connected and has an IP address. A malicious user can easily tamper with this device or report false reading or spoof an IP address. As another example, consider a gateway that serves a number of Fog devices. These may be easily compromised or replaced by fake ones or by connecting to malicious access points that provide deceptive SSID as a legitimate one. Also, s msn-in-the-middle attack in the Fog environment is simple to launch, it can be difficult to address. Although, techniques such as signature or anomaly-based intrusion detection, multicast authentication and Diffie-

Hellman key exchange can be used to counter act, such issues at the local level are matters of serious concern. The main issues can be grouped into the following categories:

- **Advance Persistent Threats (APT):** these refer to unauthorized users gaining access to systems or networks and remain there for a long time without being detected
- **Access Control Issues (ACI):** These refer to unauthorized users managing to install malicious software to gain unauthorised access to cause malicious damage
- **Account Hijacking (AH):** Here, the intention of the attack is to gain access to user accounts using phishing techniques for malevolent aim to compromise the system
- **Denial of Service (DoS):** Here, the objective of the hacker is to disable and render inaccessible the entire system or parts of the system resulting in the interruption in an authorised user's access
- **Data Breaches (DB):** This refers to unauthorised or illegal viewing, access, deletion. Modification, or retrieval of data by an individual attacker or malicious application
- **Data Loss (DL):** This refers to an event or situation that results in data being corrupted, deleted or made unavailable by unauthorised user or malicious application
- **Malicious Insider (MI):** This is an authorised user who uses his access permissions for harmful, unethical or illegal activities to cause damage or harm to the system resources
- **Insufficient Due Diligence (IDD):** This refers to lacking in the required standard of care and not fulfilling the legal obligation, as a result of which damage or failures may be caused
- **Shared Technology Issues (STI):** These refer to multi-tenancy when many users share the same resources, that can result in compromising the system by threats such as DoS, ML, DB.

Fog Network Topology and Location Awareness of Nodes

Fog networks are heterogeneous where management and maintenance of the connectivity of a wide variety of diverse devices is not easy. In this context. design and the arrangement of nodes therein, consisting of heterogeneous devices with varied communication protocols, is one of the key issues. Architecture is grounded in Virtualisation technology and that itself has certain inherent limitations in terms of security and shared boundaries. Relevant issues, here, relate to network scalability (horizontal, vertical, up and down), topological arrangement, virtualisation, redundancy, measurement of performance, monitoring and management, and operational costs.

Although, network topology issues can be managed using techniques such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV), the performance and scalability of virtualised network appliances is yet another serious key concern [2].

It is important that interface mechanisms between nodes are dynamic and the nodes themselves have an additional layer that have ambient intelligence (AmI) embedded so that the nodes become location and context aware. However, application-aware provisioning can be easily compromised because of the bandwidth, storage and latency.

Resource Management

In any network, there are issues concerning resource discovery, end-points determination, resource allocation and sharing resources. Fog architecture is no different. The most critical problem is designing resource management techniques that determine which modules of analytics applications are pushed to each edge device to minimize the latency and maximize throughput. We, therefore, need an evaluation platform that enables the quantification of performance of resource management policies on an IoT or Fog computing infrastructure in a repeatable manner.

Interoperability

Another key challenge in facilitating Fog Computing is building the necessary level of interoperability to support access of Fog-based resources. This requires a collaborative approach between the different elements of Fog infrastructure. One solution towards achieving the interoperability is the need for an open architecture that can significantly reduce the cost of developing Fog applications, increase the adoption of Fog Computing model, and ultimately increase the quality and innovation of Fog Computing services [22].

Other Issues

There are also some serious issues due to the multi-tenant nature of the Fog environment. Such issues revolve around security and privacy (as mentioned above) and service level agreements. Lack of appropriate tools for the measurement of connectively, capacity, reliability, effectiveness, and delay are also of serious concerns [2]. Here, the issues are the same as for the Cloud paradigm because of similarity due to the nature of distributed computing environments.

To resolve, or at least minimise, the inherent issues of distributed computing environments, we need new approaches that satisfy, at least, the following requirements [13]:

- Minimise latency
- Conserve network bandwidth
- Address security and privacy concerns
- Collect data securely from different environments
- Manage data processing effectively.

2.0 Cloud vs Fog Computing

After briefly introducing the Fog Computing concept in the preceding section, in the first part of the current section is about the Cloud paradigm. Here, first, we present, what this paradigm entails - this is for the sake of completeness. Later, in the section, we articulate the differences between the Cloud and the Fog models.

2.1 Cloud Computing

Cloud Computing is a generic term for anything that involves delivering hosted services over the Internet [11]. It is a paradigm based on a pay-as-you-go approach. Gartner [11] defines Cloud Computing as a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies. It is an all-inclusive solution in which computing resources (hardware, software, networking, storage, and so on) are provided rapidly to users as demand dictates [12]. Cloud Computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather

than a local server or a personal computer. It is generally a heavyweight and dense form of computing power that providers the following benefits:

- Cost saving with respect to capital investment - as organisations can leave or deploy Cloud-based resources for Cloud providers
- Reduction in costs with respect to developing and delivering IT services – as all manner of services (software, hardware, networking, storage, etc) are already available in the Cloud environment
- Reduction in management responsibilities and thus allowing key personnel to focus more on production and innovation – as the maintenance and deployment of services is the responsibility of Cloud owners/providers
- Increased business agility to allow enterprises to meet the needs of rapidly changing markets – as the latest technologies can be easily provisioned on a pay-as-you-go basis for from Cloud providers.

Some of the core characteristics include [10]:

- On-demand self-service - to enable users to consume computing capabilities (e.g. applications, server time, network storage) as and when required
- Resource pooling - to allow combining computing resources (e.g. hardware, software, processing, network bandwidth) to serve multiple consumers
- Rapid elasticity and scalability - to allow functionalities and resources to be rapidly and automatically provisioned and scaled as demand dictates
- Measured provision to optimize resource allocation - to determine usage for billing purposes
- Extension to existing on-premise hardware and application resources – to reduce the cost of additional resource provisioning.

Cloud-based services (software, hardware, networking, servers, virtualisations, security, etc) come in different varieties, however, these are generally classified as three types: Software Services, Platform Services and Infrastructure Services. These are generally abbreviated as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), respectively. More specifically, these can also be of the following variety (and many more):

- Storage-as-a-Service
- Database-as-a-Service
- Security-as-a-Service
- Communication-as-a-Service
- Management/Governance-as-a-Service
- Integration-as-a-Service
- Testing-as-a-Service
- Business Process-as-a service

Cloud environments come in different varieties and these may be deployed in a number of ways, more generally as:

- Public Clouds or External Clouds – These are owned, managed and hosted by third parties. Cloud providers assume the responsibilities of installation, management, provisioning and maintenance. This variety of Clouds provides a much greater level of efficiency of pooling of resources.
- Private Clouds or Enterprise Clouds – These are proprietary networks, often data centres, owned and managed by, and residing within the enterprise. Thus, the enterprise can take better control of all aspects of the provision and functioning.
- Hybrid Clouds – These are a combination of private and public Clouds, where the management responsibilities are split between the enterprise and the public Cloud providers. Main advantage is that the organizations can keep the sensitive data within the private Cloud and the rest in the public Cloud.

Although, the Cloud paradigm presents numerous benefits and that is the exactly reason that it is an attractive model for enterprises, there are also numerous inherent issues. Some of these relate to the following:

- data governance and service management
- product and process monitoring
- infrastructure reliability and system availability
- information and visualization security
- business continuity
- high latency and bandwidth bottlenecks
- data transmission across existing broadband speeds.

2.2 Cloud vs Fog Computing Comparison

In this sub-section, we compare the two models and look into the similarity and differences and also discuss how some of the issue inherent in the Cloud paradigm may be resolved, or at least, minimised by the Fog paradigm.

Fog computing is a distributed computing paradigm that extends Cloud computing to the edge of the network – as a compliment to the Cloud solution, to adjust to the emerging IoT. It facilitates the operation of compute, storage, and networking services between end devices and Cloud computing data centers. Fog computing typically involves components of an application running both in the Cloud as well as in the Edge devices in the Fog i.e. in smart gateways, routers or dedicated Fog devices. Refer to Fig 2 where the bottom layer has the enterprise smart sensor devices that are accessing resources and compute power in the middle layer as well as resources and compute power in the Cloud; the Fog environment in the middle layer is also linked with the Cloud environment in the top layer. Table 1 also illustrates the benefits of storage and processing 'closer to home' rather than in a geographically distant Cloud environment.

To summarise, the cloud requires a huge amount of bandwidth, the Internet is inherently unreliable and wireless networks have limitations. By using Fog Computing, the amount of bandwidth required is much reduced. It allows, essentially, transmitted data to bypass the internet, keeping it as local as possible, on the smart devices in the Fog environment. The most valuable data may still be transmitted through cloud networks, but much of the traffic, especially the sensitive data, could be kept off of those networks, freeing up bandwidth for everyone using the cloud.

Figure 2: 3-layer Cloud-Fog Enterprise Model

Table 1: Fog Computing vs Cloud Computing

	Fog Computing	**Cloud Computing**
Response Time	Milliseconds – sub seconds	Minutes, days, weeks
Data storage period	transient	Months and years
applications	e.g. M2M	e.g. Data Analytics
Location coverage	Very Local	global

Similar to Cloud computing, Fog computing provides storage, compute, and applications to be consumed by end-users. However, Fog computing has a bigger proximity to end-users and bigger geographical distribution [4]. Compared to Cloud paradigm, 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 better quality of service (QoS) and Edge analytics/stream mining, resulting in superior user-experience [3]. Thus, Fog Computing extends the Cloud model to the edge of the network to address applications and services that do not fit the paradigm of the Cloud due to technical and infrastructure limitation such as the following [11]:

- Applications requiring much lower and predictable latency
- Geographically widely distributed applications and processing
- Faster mobility and mobile applications
- Large-scale distributed control systems requiring faster processing.

There are certain inherent issues in Cloud computing. Fog computing is highly suited to resolving at least some of these e.g. reducing the need for bandwidth by not sending every bit of information over Cloud channels; and instead aggregating it at certain access points [6]. This type of distributed strategy, in turn, also lowers costs, improves efficiencies and improves QoS. More interestingly, it is another approach to dealing with the emerging and much popular concept of Internet of Things (IoT).

2.3 Fog vs Edge Computing

Fog Computing and Edge Computing are often used to mean the same architecture and therefore, even in this contribution, we have regarded the terms as interchangeably; however, a subtle distinction can be made. In this section, we aim to highlight the differences between the two architectures.

Although, Fog and Edge Computing both refer to having intelligence, processing and storage at the edge of the network i.e. closer to the sources of data, the main difference is to do with exactly where the intelligence and processing are placed. Whereas, Fog computing pushes intelligence down to the local area network level of network architecture, processing data in a Fog node or IoT gateway; Edge computing places the intelligence, processing and communication capabilities of an

Edge gateway directly into the smart devices like programmable automation controllers [14]. Besides, Edge Computing is an older expression predating the Fog Computing term. While Edge computing is typically referred to the location where services are instantiated, Fog computing implies distribution of the communication, computation, and storage resources and services on or close to devices and systems in the control of end-users [9].

In Fog computing, data communication between the data generating devices and the Cloud environment requires a number of steps [15] including:

- communication is first directed to the input/output points of a programmable automation controller (PAC) that runs a control system program to perform automation
- it is then sent to a protocol gateway that converts data to an understandable format such as HTTP
- data is then transmitted to a Fog node on the local network that performs the required analysis and organises data transmission to the Cloud for storage etc. Thus, in the Fog environment, there are many links and so many potential points of failures.

In Edge Computing, the communication is much simpler and there potentially less points of failures. Here, data generating devices are physical connected to PACs for onboard automation as well as for parallel processing and analysis of data. Again, it is PACs that determine which data is to be stored locally or sent to the Cloud. Thus, apart from reducing possibility of failures, there is saving of time and streamlining of communication, as well reduction in complexity of architecture [15, 16].

In Fog computing, there is a single centralised device responsible for processing data from different endpoints in the network. In the Edge architecture, IoT data is collected and analysed directly by the connected devices, so every network node participates in processing. Shariffdeen [16] suggests that whereas Fogging is much preferred by the service providers and data processing companies, Edge architecture is much preferred by middle-ware companies that own back-bone and radio networks. Table 2 compares Fog vs the Edge computing in terms of advantages.

According to [19, 20], Fog works with the Cloud but Edge is defined by the exclusion of Cloud. Fog has a hierarchical and flat architecture with several layers forming a network whereas Edge is often limited to separate nodes (in addition to compute power) that do not form a network. Fog also addresses networking, storage, control and acceleration. Fog computing has extensive peer-to-peer interconnect capability between nodes, where Edge runs its nodes in silos, requiring data transport back through the Cloud for peer-to-peer traffic [20].

Table 2: Advantages of Fog vs Edge Computing

	Fog Computing	**Edge Computing**
Advantages	• Location awareness, low latency, QoS – but requires large resources • Data closer to the user – but not for systems that require limited data • Integration of distributed data with Cloud services	• All nodes participate so reduced delays • Real time local analysis • Lower operating costs and network traffic

		• Improved performance

The Fog model architecture consists of three main segments [17]:

- IoT devices: these are connected devices that generate and transit large amounts of a variety of structured and semi-structured data
- Fog network: that receives real-time data from IoT devices using a diverse variety of communication protocols; and performs real-time analysis
- Cloud environment: that receives data for storage from Fog nodes and also performs analysis for business intelligence.

Edge computing architecture consists of the following components [17]:

- Edge devices: these are connected smart devices (sensors, actuators, etc) that generate, analyse and take other relevant actions
- IoT Gateway: that has responsibility for connecting Edge devices with the Cloud environment; deals with varied protocols and stores peripheral data
- Cloud environment: that receives data from gateway, analyses and send instructions back to the gateway.

Design for resource constrained fog computing applications requires well established principles of service computing and to follow a software engineering approach to building fog computing applications that safe and secure. Therefore, OpenFog consortium has established a reference architecture which provides an open, distributed, and secure platform for developing fog computing applications.

3.0 Fog Computing Reference Architecture

In order to develop a Fog Computing architecture, a collaboration by the name of OpenFog Consortium, comprising the joints of industry (such as Cisco, Dell, Intel and Microsoft), research institutions such as Princeton University and users, was founded in November 2015. This consortium is an independent non-profit organisation run under the direction of its board of directors; its committees and working groups are run by its membership. Their deliberations have resulted in, what is now called as the OpenFog Reference Architecture (OpenFog RA) that aims to help business leaders, software engineers and system designers in developing and maintaining hardware, software, and system elements necessary for Fog computing.

The OpenFog RA is built upon a set of eight core principles called Pillars viz: security, scalability (scalable performance, capacity, reliability, security, hardware, software), openness (composability, interoperability, communication, location transparency), autonomy (of discovery, orchestration, management, security, operation, cost savings), RAS (reliability, availability, serviceability), agility, hierarchy, and programmability (adoptive infrastructure, efficient deployment, effective operations, enhanced security). In determining the relevant pillars, ISO/IEC/IEEE standards have been followed.

Fig 3 shows the OpenFog layered architectural logical view of the IoT system from a computational perspective. The hierarchical layers are deployed in the Fog-Cloud model as illustrated in Fig 4.

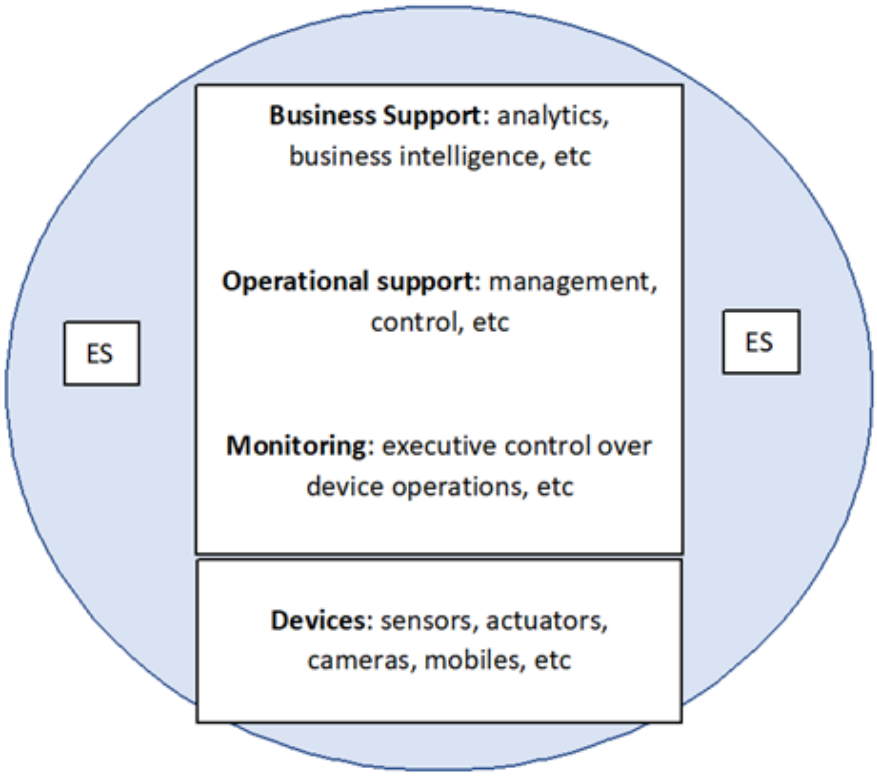

Figure 3: OpenFog layered architectural view – ES refers to Enterprise Systems for implementation of various systems within the hierarchy

Enterprise systems	Enterprise systems	Enterprise systems	Enterprise systems	Enterprise systems
Business support	Fog .	Cloud .	Cloud .	Cloud .
Operational support	Fog .	Fog .	Cloud .	Cloud .
Monitoring	Fog	Fog	Fog	Cloud
Devices	{1}	{2}	{3}	{4}

Figure 4: OpenFog Hierarchy Fog deployment (in Fog-Cloud) models (adapted from [21])

In Fig 4, we note that:

- Enterprise Systems (ESs) in the model designated as {1} reside only in the Fog environment and are independent of the Cloud services
- Model {2} uses the Cloud for ESs needed for business support at strategic level e.g. strategic decisions making
- Model {3} suggests that local Fog infrastructure is used for time-sensitive processing, while the Cloud provision is accessed for operational and business-support related information processing
- The last model, referred to as {4}, is employed in scenarios such as connected cars etc.

The discussion in this section, so far, has referred to an abstract logical higher-level architecture as proposed by the OpenFog RA. For various stakeholder perspectives in terms of the other pillars and for more detailed information, reader is referred to the OpenFog Consortium Reference Architecture baseline but full paper [21] - as the fuller description, here, is out of the scope of this chapter.

Here, at this point, it is worth noting that the OpenFog RA offers a number of distinct advantages which the OpenFog Consortium refer to as SCALE [21], that are as follows:

- Security: additional security to ensure safe and trusted transactions
- Cognition: awareness of client-centric objectives to enable autonomy
- Agility: rapid innovation and affordable scaling under common infrastructure
- Latency: real-time processing and cyber-physical system control
- Efficiency: dynamic pooling of resources from participating end-user devices.

3.1 Fog Computing Application Scenarios

Having discussed the differences between Cloud and Fogging, there are any commercial applications that require both Fog localization and Cloud globalization, particularly for analytics and Big Data processing and manipulation.

Technology giants, such as IBM, are the driving force behind Fog computing and to link it to the concept to IoT. Most of the buzz around Fog has a direct correlation with IoT. The fact that everything from cars to thermostats are gaining web intelligence means that direct user-end computing and communication may become much more important than ever. The following are some of the practical example applications where Fog computing is already being applied [6]:

- **Smart grids:** Fogging, for the same reason as above, provides fast machine-to-machine (M2M) handshakes and human to machine interactions (HMI), resulting in a more efficient cooperation with the wider Cloud provision. Fog devicescollect the local information and collectively take real-time decisions based on 360 degree view of what is happening in the environment.
- **Smart homes and cities:** Fog computing enables getting sensor data at all levels of the activities of homes as well as entire cities, integrating the mutually independent network entities within the homes and cities and faster processing to create more adaptive user environment.
- **Connected vehicles:** Fogging provides an ideal architecture for vehicle-to-vehicle (V2V) communication, because of proximity of devices embedded in cars, roads and access points. Fogging, with context awareness, makes real-time interactions between cars, access points and traffic lights much safer and efficient.

- **Self-drive cars:** These vehicles rely entirely on automated input to perform navigation. Thus, a slow response when vehicles are moving at 60 mph can be dangerous or even fatal, so real-time processing speed is required. Fog computing networks are especially suitable for applications that require a response time of less than a second, according to Cisco [23].
- **Traffic light system:** Fogging is suitable for building smart traffic light systems that change signals based on surveillance of incoming traffic to prevent accidents or reduce congestion. Data can also be sent to Cloud for longer term analysis. The communication between vehicles and access points are being improved with the arrival of 3G and 4G and more powerful WiFi.
- **Healthcare management:** Cloud computing market for healthcare has already reached in excess of $5.4 billion [6]. Fog computing is helping to speed up the process by localising the device connectivity and proximity of devices to the patients and user community.
- **Medical wearables**: These are increasingly being used by healthcare providers to monitor patient conditions, provide remote telemedicine and even to guide on-site staff and robots in procedures as delicate as surgery. Thus, reliable real-time data processing is crucial for these types of applications [23].
- **IoT and Cyber-Physical Systems (CPSs) –** Fogging has a vital role to play in CPSs (integration of system's physical and computational elements) and IoT (interlink physical objects). The combination of these is already changing the world comprising computer-based control systems, physical reality and engineered systems.

Other application scenarios include: rail safety, power restoration from smart grid network, smart parking meters, self-drive cars, air traffic control, cyber security, IoT Cyber-Physical systems, Machine-to-Machine Communication and Human-Computer-Interaction.

4.0 Future of Fog Computing

Attractive nature of Fog and Edge computing will result in the development of new business models, thus helping the industries to grow more efficiently and much faster. As a result, new vendors and new industries will come on board with new offerings and new architectural approaches to networking.

One exciting area of development is Fog-as-a-Service (FaaS) where a Fog service provider deploys interconnected Fog nodes to blanket a regional service area [18]. This, in turn, will provide opportunities for creating new applications and services that cannot be easily developed using the current host-based and Cloud-based platforms; for example, Fog based security services that would address many challenges that we are currently facing in the IoT environment.

The emergence of 5G and smart city applications will reveloutionise quality of living such as health monitoring and predictions, recycling and waste management systems, connecting people, wearables, tourism, smart building, smart transportation, and smart home.

1.8 Conclusion

Fog Computing is becoming an attractive paradigm for reasons of proximity of processing, storage and data analytics to the devices that generate and exchange data. In this chapter, we have discussed the Fog Computing paradigm in some detail, compared it with the Cloud Computing model, and presented the OpenFog Reference Architecture, albeit only briefly. We have illustrated the usefulness of Fog paradigm as an extension of the Cloud architecture and also presented some use cases. The aim in this contribution has been to provide some general background information with some critical analysis so that the chapter serves as a foundation for

the more detailed accounts of the more specialised Fog-related topics articulated in the other chapters in this book.

References

1. Evans D, (2011), The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Cisco White Paper, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

2. Yi S, Li C and Li Q, (2012), A Survey of Fog Computing: Concepts, Applications and Issues. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.702.7773&rep=rep1&type=pdf

3. Cisco (2013), Fog Computing, Ecosystem, Architecture and Applications, Cisco Report RFP-2013-078.

4. Bonomi F, Milito R, Zhu J, and Addepalli S, 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. ACM, 2012, pp. 13–16.

5. NIST, (2018), The NIST Definition of Fog Computing, https://csrc.nist.gov/csrc/media/publications/sp/800-191/draft/documents/sp800-191-draft.pdf

6. Banafa A, (2014), what is Fog computing? https://www.ibm.com/blogs/Cloud-computing/2014/08/Fog-computing/

7. NIST, (2018), Fog Computing Conceptual Model, NIST special publ (SP) 500-325, https://doi.org/10.6028/NIST.SP.500-325

8. Bar-Magen Numhauser, J (2012). Fog Computing introduction to a New Cloud Evolution. Escrituras silenciadas: paisaje como historiografía. Spain: University of Alcala. pp. 111–126. ISBN 978-84-15595-84-7.

9. NIST, (2017), the NIST Definition of Fog Computing, NIST Special Publ 800-191 (Draft)

10. Mahmood, Z, (2011), Cloud Computing: Characteristics and Deployment Approaches, 11th IEEE International Conference on Computer and Information Technology

11. Cearley D W, (2010) Cloud Computing: Key Initiative Overview, Gartner Report, 2010

12. Amrhein D and Quint S, (2009), Cloud Computing for the Enterprise: Part 1: Capturing the Cloud, DeveloperWorks IBM Report, www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html

13. Cisco, (2015), Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, White Paper – Cisco; available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

14. Greenfield D, (2016), Fog Computing vs. Edge Computing: What's the Difference? https://www.automationworld.com/Fog-computing-vs-edge-computing-whats-difference

15. OPTO-22, (2018), Fog Computing vs Edge Computing, http://info.opto22.com/Fog-vs-edge-computing

16. Shariffdeen R, (2017), Fog Computing vs Edge Computing, https://medium.com/@rshariffdeen/edge-computing-vs-Fog-computing-5b23d6bb049d

17. Shah, H, (2017), Edge computing and Fog computing for enterprise IoT, https://www.simform.com/iot-edge-Fog-computing/

18. McKendrick, J, (2016), Fog Computing: a New IoT Architecture?, https://www.rtinsights.com/what-is-Fog-computing-open-consortium/

19. Adams F, (2017), OpenFog Reference Architecture for Fog Computing, https://knect365.com/Cloud-enterprise-tech/article/0fa40de2-6596-4060-901d-8bdddf167cfe/openFog-reference-architecture-for-Fog-computing

20. Hardesty L, (2017), Fog Computing Group Publishes Reference Architecture, https://www.sdxcentral.com/articles/news/Fog-computing-group-publishes-reference-architecture/2017/02/

21. OpenFog, (2017), OpenFog Reference Architecture for Fog Computing, https://www.openFogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf

22. Gorlatova M, (2017), Reference Architecture, http://pages.di.unipi.it/throughtheFog/wp-content/uploads/sites/13/2017/02/gorlatova.pdf

23. Rasmussen R, (2017), How Fog Computing Will Shape The Future Of IoT Applications And Cybersecurity, https://www.informationsecuritybuzz.com/articles/fog-computing-will-shape-future-iot-applications-cybersecurity/

24. Varshney, P., and Simmhan, Y (2017) Demystifying Fog Computing: Characterizing Architectures, Applications and Abstractions, E/ACM 1st International Conference on Fog and Edge Computing, 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)

Index