

Chapter 1

Fog Computing: Concepts, Principles and Related Paradigms



Zaigham Mahmood and Muthu Ramachandran

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 the 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, i.e. at the *Edge* of the network, and thus bypassing the wider Internet. In this chapter, we discuss the concepts and principles of Fog paradigm as well as the related paradigms and technologies, 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.

1.1 Introduction

Ubiquitous deployment of smart devices (such as mobile phones, tablets, sensors, motors, relays and actuators) connected through the Internet of Things (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, social and media and more is expected to grow from 1.1 zettabytes (or 89 exabytes)

Z. Mahmood (✉)
Debesis Education, Derby, UK
e-mail: dr.z.mahmood@hotmail.co.uk

Z. Mahmood
Shijiazhuang Tiedao University, Hebei, China

M. Ramachandran
Leeds Beckett University, Leeds, UK

per year in 2016 to around 2.3 zettabytes (or 194 exabytes) per year by 2020 [2]. Managing such amounts of data, as well as data generated by social media technologies (such as Facebook, Twitter), is one of the biggest challenges, which the traditional IoT- and Cloud-based architectures are unable to cope with. The reasons being: the large scale, variety and velocity of data often known as Big Data; heterogeneity of the IoT devices; differing connectivity protocols and lack of communication 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* [3, 4].

Fog Computing [1], a term first put forward by Cisco, is sometimes also referred to as Edge Computing [4], 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 centralised Cloud environment, Fog systems operate on network ends. It refers to placing some intelligence, processes and resources at the edge of the Cloud, instead of establishing channels for Cloud storage and utilisation [5, 6]. Fog Computing appears to be the next big thing for the Internet of Everything (IoE). According to one research [7], 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 5 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 environments and how Fogging may possibly address at least some of 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–Fog-based system serving smart end-user devices in a distributed IoT environment.

1.2 Fog Computing

Fog Computing is a way of providing compute and storage services more immediately and close to the physical devices of an organisation [5], i.e. at the *Edge* of the Cloud network. 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 bandwidth and carriers [5].

NIST Special Publication 800-191 [8] defines 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 centres. According to the OpenFog Consortium [9], 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 virtualised platform that provides compute, storage and networking services between end devices and traditional Cloud Computing data centres [4, 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* [4]. Fog nodes deploy and provision same types of services as provisioned by Cloud Computing, viz: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (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 the end-users, with dense geographical distribution, and much better support for mobility.

As presented in Fig. 1.1, Fog Computing characteristics include the following [4]:

- 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-user support—because of proximity of Edge devices to the compute nodes,

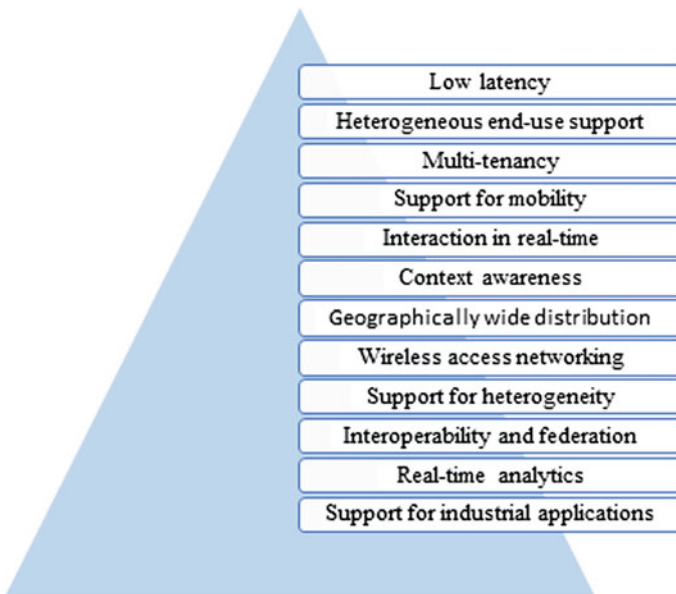


Fig. 1.1 Fog Computing characteristics

- Multi-tenancy in controlled environment—because of highly virtualised distributed 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 sources,
- Support for a wide variety of industrial applications—through processing and analysis in real time.

These characteristics are useful when devising Fog Computing applications or environments such as smart cities, smart home, smart grids, smart health and eminent applications such as emergency response systems for flood monitoring and recovery. Varshney and Simmhan [11] also discuss three essential characteristics—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 related 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 data centre 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 having based on Cloud-related technologies. In the network architecture, Cloudlets reside in the middle of the three-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. In this context, Hadoop and other Big Data solutions have already 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 [5]. This, in turn, resolves the issues of security and privacy as well—as the valuable and sensitive data should not really be travelling to and through the Cloud Computing networks. Some of the advantages of Fogging 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. This will also help 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 those relating to security and privacy, resource management, shared boundaries in case of distributed environments and communication protocols.

1.2.1 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 the Fog Computing approach. Besides the issues inherited from Cloud Computing, some of the Fog-specific issues refer to the following:

1.2.1.1 Security and Privacy

Most security-related issues of distributed computing environments apply to Fog paradigm, and 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 metre 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, as the man-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 counteract, 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 unauthorised users gaining access to systems or networks and remain there for a long time without being detected
- **Access Control Issues (ACI):** These refer to unauthorised 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 as 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 an unauthorised user or a 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, DL and DB.

1.2.1.2 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 are not easy. In this context, design and the arrangement of nodes therein, consisting of a wide variety of devices with varied communication protocols, are 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 are yet another serious key concern [14].

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.

1.2.1.3 Resource Management

In any network, there are issues concerning resource discovery, end-point determination, resource allocation and resource sharing. 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 minimise the latency and maximise 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.

1.2.1.4 Interoperability

Another key challenge in facilitating Fog Computing is building the necessary level of interoperability to support the 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 [15].

1.2.1.5 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 connectivity, capacity, reliability, effectiveness and delay are also of serious concerns [14]. 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.

1.3 Cloud Paradigm Versus Fog Computing

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

1.3.1 Cloud Computing

Cloud Computing is a generic term for anything that involves delivering hosted services over the Internet [16]. It is a paradigm based on a pay-as-you-go approach. Gartner [16] 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, 17]. 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 promises the following benefits:

- Cost saving with respect to capital investment—as organisations can lease or deploy Cloud-based resources, whether virtualised hardware, software, storage or network capabilities from the 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 from the Cloud providers.

Some of the core characteristics of the Cloud paradigm include [10, 17]:

- 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 up or down as demand dictates,
- Measured provision to optimise resource allocation—to determine usage for billing purposes,
- Extension to existing on-premise hardware and application resources, e.g. through Cloud bursting—to reduce the cost of additional resource provisioning.

Cloud-based services (software, hardware, networking, servers, virtualisation, 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 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 or Enterprise Clouds—These are proprietary networks, often data centres, owned and managed by the organisations, and residing within the enterprise. Thus, the enterprises can take better control of all aspects of the provision and functioning.
- Hybrid Clouds—These are combination of private and public Clouds, where the management responsibilities are split between the enterprise and the public

Cloud providers. The main advantage is that the organisations 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 exactly the 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 visualisation security,
- Business continuity,
- High latency and bandwidth bottlenecks,
- Data transmission across existing broadband speeds.

1.3.2 Cloud Versus Fog Computing Comparison

In this subsection, we compare the two models and look into the similarity and differences and also discuss how some of the issues 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 vision. It facilitates the operation of compute, storage and networking services between end devices and Cloud Computing data centres. 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. 1.2 where the bottom layer has the enterprise smart sensor devices that are accessing resources and compute power from the



Fig. 1.2 Three-layer Cloud-Fog enterprise model

Table 1.1 Fog Computing versus 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	Local	Global

middle layer as well as resources and compute power directly from the Cloud; the Fog environment in the middle layer is also linked with the Cloud environment in the top layer. Table 1.1 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 else using the Cloud.

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 [18], as mentioned before. Compared to the Cloud paradigm, Fog Computing emphasises proximity to end-users and client objectives, local resource pooling, latency and the backbone bandwidth reduction to achieve better quality of service (QoS) and Edge analytics/stream mining, resulting in superior user experience [19]. 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 [16]:

- Applications requiring 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, as discussed before. 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 [5]. This type of distributed strategy, in turn, also lowers costs, improves efficiencies, and so the QoS. More interestingly, it is another approach to dealing with the emerging and much popular concept of Internet of Things (IoT).

1.4 Fog Computing Versus 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 interchangeable; 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 the network architecture, processing data in a Fog node or the IoT gateway, Edge Computing places the intelligence, processing and communication capabilities of an Edge gateway directly into the smart devices like programmable automation controllers (PAC) [20]. 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 [4].

In Fog Computing, data communication between the data generating devices and the Cloud environment requires a number of steps [21] 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 are potentially less points of failures. Here, data generating devices are physically 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 the complexity of architecture [21, 22].

In Fog Computing, there is a single centralised device responsible for processing data from different end-points in the network. In the Edge architecture, IoT data is collected and analysed directly by the connected devices, so every network node participates in the processing. Shariffdeen [22] suggests that whereas Fogging is much preferred by the service providers and data processing companies, Edge architecture is more preferred by middle-ware companies that own the backbone and radio networks. Table 1.2 compares Fog vs the Edge Computing in terms of advantages.

Table 1.2 Advantages of Fog versus Edge Computing

	Fog Computing	Edge Computing
Advantages	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • All nodes participate so reduced delays • Real-time local analysis • Lower operating costs and network traffic • Improved performance

According to [2, 9], 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 [9].

The Fog model architecture consists of three main segments [23]:

- 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 [23]:

- 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 sends 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 are safe and secure. Therefore, OpenFog consortium has established a reference architecture which provides an open, distributed and secure platform for developing Fog Computing applications. This architecture is briefly outlined in the following section.

1.5 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: safety, trust,
- 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: innovation, affordability,
- Hierarchy,
- Programmability: adoptive infrastructure, efficient deployment, effective operations, enhanced security.

In determining the relevant pillars, ISO/IEC/IEEE standards have been followed.

Figure 1.3 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. 1.4.

In Fig. 1.4, 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

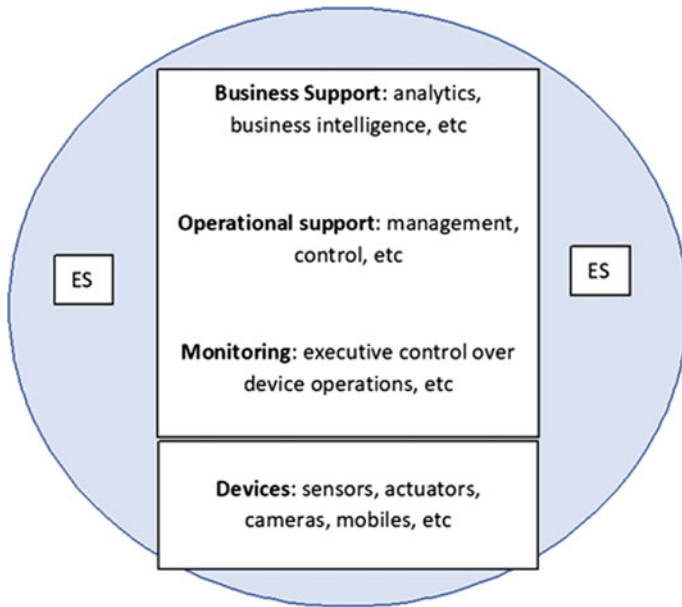


Fig. 1.3 OpenFog layered architectural view—ES refers to enterprise systems for implementation of various systems within the hierarchy

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}

Fig. 1.4 OpenFog hierarchy Fog deployment (in Fog–Cloud) models. Adapted from [24]

referred to the OpenFog Consortium Reference Architecture paper [24]—as the fuller description, here, is out of the scope of this chapter.

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 [24] 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.

1.6 Fog Computing Application Scenarios

Having discussed the differences between Cloud and Fogging, there are many commercial and industrial applications that require both Fog localisation and Cloud globalisation, 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 of IoT. Most of the buzz around Fog Computing has a direct correlation with IoT. The fact that everything from cars to thermostats to pumps to smart energy metres 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 [5]:

- **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 devices collect the local information and collectively take real-time decisions based on 360° 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 from the entire cities, integrating the mutually independent network entities within the homes and cities and faster processing to create more adaptive user environments for better human conditions and the quality of living.
- **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 more 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 and immediate decisions

are required. Fog networks are especially suitable for applications that require a response time of less than a second, according to Cisco [7].

- **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 the 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 [5]. 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, to 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 [7].
- **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 networks, smart parking metres, self-drive cars and trains, air traffic control, cyber security, IoT cyber-physical systems, machine-to-machine communication and human-computer interaction.

1.7 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 [25]. 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 would address many challenges that we are currently facing in the IoT environment.

The emergence of 5G technologies, development of smart city applications and building the distributed computing environments with embedded ambient intelligence will all help to revolutionise the quality of life and assisted living through better and more efficient health monitoring and predictions, recycling and waste management systems, connecting people, smart wearables, tourism, smart buildings, smart transportation and adaptable smart homes.

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. Adams F (2017) OpenFog reference architecture for fog computing. <https://knect365.com/Cloud-enterprise-tech/article/0fa40de2-6596-4060-901d-8bddf167cfe/openFog-reference-architecture-for-Fog-computing>
3. NIST (2018) Fog computing conceptual model, NIST special publ (SP) 500-325. <https://doi.org/10.6028/NIST.SP.500-325>
4. NIST (2017) The NIST definition of fog computing, NIST Special Publ 800-191 (Draft)
5. Banafa A (2014) What is fog computing? <https://www.ibm.com/blogs/Cloud-computing/2014/08/Fog-computing/>
6. Bar-Magen Numhauser J (2012) Fog Computing introduction to a New Cloud Evolution. *Escrituras silenciadas: paisaje como historiografía*. University of Alcalá, Spain, pp 111–126. ISBN 978-84-15595-84-7
7. 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/>
8. NIST (2018) The NIST definition of fog computing. <https://csrc.nist.gov/csrc/media/publications/sp/800-191/draft/documents/sp800-191-draft.pdf>
9. Hardesty L (2017) Fog computing group publishes reference architecture. <https://www.sdxcentral.com/articles/news/Fog-computing-group-publishes-reference-architecture/2017/02/>
10. Mahmood Z (2011) Cloud computing: characteristics and deployment approaches. In: 11th IEEE international conference on computer and information technology
11. Varshney P, Simmhan Y (2017) Demystifying fog computing: characterizing architectures, applications and abstractions. In: E/ACM 1st international conference on fog and edge computing (ICFEC), IEEE 2017
12. Amrhein D, Quint S (2009) Cloud computing for the enterprise: Part 1: capturing the cloud, developer works. 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. Yi S, Li C, 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>
15. Gorlatova M (2017) Reference architecture. <http://pages.di.unipi.it/throughtheFog/wp-content/uploads/sites/13/2017/02/gorlatova.pdf>
16. Cearley DW (2010) Cloud computing: key initiative overview. Gartner Report, 2010
17. Mahmood Z (2011) In: Mahmood Z, Hill R (eds) Cloud computing for enterprise architectures. Springer, Berlin
18. Bonomi F, Milito R, Zhu J, Addepalli S (2012) 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
19. Cisco (2013) Fog computing, ecosystem, architecture and applications. Cisco Report RFP-2013-078
20. Greenfield D (2016) Fog computing vs. edge computing: what's the difference? <https://www.automationworld.com/Fog-computing-vs-edge-computing-whats-difference>
21. OPTO-22 (2018) Fog computing vs edge computing. <http://info.opto22.com/Fog-vs-edge-computing>
22. Shariffdeen R (2017) Fog computing vs edge computing. <https://medium.com/@rshariffdeen/edge-computing-vs-Fog-computing-5b23d6bb049d>
23. Shah H (2017) Edge computing and fog computing for enterprise IoT. <https://www.simform.com/iot-edge-Fog-computing/>
24. OpenFog (2017) OpenFog reference architecture for fog computing. https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf
25. McKendrick J (2016) Fog computing: a new IoT architecture? <https://www.rtingsights.com/what-is-Fog-computing-open-consortium/>