Fog Computing : A New Era for the Cloud Computing Paradigm

Sangeeth Dev Sarangi

Abstract

In the world of the Internet of Things (IoT), Cloud is a centralised system that helps to deliver and transport data for real-time operations and processing. This involves a lot of time as data must be sent from the end-user to the cloud before the cloud can process the data. To overcome issues related to latency between the cloud data centre and end-user, an extension of cloud computing, known as fog computing, is introduced. Fog nodes operate at the edge of the network, optimizing data security, accuracy, consistency, and reducing the latency rate. This significantly reduces the time required for the process and makes it more efficient because the cloud is not overloaded. In this paper, we discuss Fog computing in-depth, emphasising its crucial role as a bridge between IoT, Cloud, and Edge computing. Finally, we address open challenges in Fog computing.

1 Introduction

In the world of technology, almost all devices are connected to the internet. The number of IoT devices is rapidly expanding, and all of these devices rely on cloud computing systems for data computation and storage. The cloud computing paradigm has been at the heart of the Internet of Things (IoT) ever-growing network in recent years, where businesses may shift their control and computing skills, as well as store, acquired data, in a medium with almost unlimited resources [1].

Today, this paradigm is facing increasing difficulties in satisfying the stringent requirements of new IoT applications. New use cases have evolved as a result of the fast adoption of IoT devices to improve our daily life. Smart cities, smart homes, smart grids, and smart manufacturing are just a few of the new use cases that have the potential to transform industries (such as health care, oil and gas, and automotive) by improving the working environment and optimizing workflow. Because most use cases involve diverse applications that require high response time (real-time or near-real-time) and better privacy, the cloud frequently fails to satisfy these demands (i.e. network congestion and ensuring privacy).

The Fog Computing concept was proposed to address these limitations, providing a structured intermediate layer that completely bridges the IoT and Cloud computing layers. Fog nodes, in reality, can be found anywhere between end devices and the Cloud, thus they aren't always physically connected to them. Furthermore, Fog computing not only focuses on the "things" side, but it also offers Cloud services. In this view, fog can be treated as a new entity that works between the Cloud and the Internet of Things to fully support and improve their interaction by combining IoT, Edge, and Cloud computing [13].

The rest of this paper is organised into a description of the Fog computing in Section 2, Characteristics of Fog Computing in Section 3, Applications of Fog Computing in section 4, Challenges faced in Fog Computing in section 5, with Conclusion in Section 6.

2 Fog computing

Fog computing is defined as a distributed computing model that extends the cloud's services to the network's edge [2]. According to Cisco, fog computing is defined as an extension of the cloud computing paradigm from the core of the network to the edge of the network [3]. It is not a complete replacement for the cloud; rather, it enhances cloud capability. Fog works closer to the edge devices, providing them with computing resources. Fog computing solves the scalability and reliability problems that exist in traditional IoT-cloud architecture. Because fog nodes operate at the edge and are more geographically distributed, they improve data security [4] [5], consistency, and latency, all of which are crucial factors in any IoT application. Additionally, the overall bandwidth to the cloud is reduced, resulting in enhanced service quality (QoS). Thus this technology makes it easier to maintain a continuous, massive information activity capable of assisting billions of hubs in exceptionally powerful, diverse scenarios.

2.1 Architecture of Fog Computing

In a traditional network, a centralised hub cannot handle large amounts of data generated by various devices or transactions. The fog computing paradigm can handle this effectively. Low latency and less traffic congestion are provided by fog computing [6]. The fog computing architecture is made up of highly dispersed heterogeneous devices to enable the deployment of IoT applications that require storage, computation, and networking resources distributed across different geographies [7]. Each fog server has the computing power to handle a massive amount of workload at the edge. As a result, only a small portion of the workload is moved to the cloud for storage and analytic processing. As a result, fog computing becomes a major driving force in IoT systems. The number of connected devices is growing, resulting in a vast volume of data and the ability to connect that data to a central cloud [8]. Fog computing enables local data analysis and the selection of which data should be transferred to a centralised cloud.

The majority of discussions on the topic refer to a three-layer architecture made up of Cloud, Fog, and IoT [9] [10] [11]. The OpenFog Consortium has proposed a larger N-layer reference design [12], which is a generalization of the three-layer architecture. This section provides an overview of the Fog architecture.

2.1.1 Three-Layer Architecture of Fog

Figure 1 depicts the basic three-layer architecture of fog computing. It stems from the central concept of Fog computing, which is a non-trivial extension of Cloud computing in the Cloud-to-Things continuum. Indeed, it introduces a middle layer (the Fog layer) that bridges the gap between Cloud infrastructure and IoT devices. The three layers that comprise the architecture are described below [9].

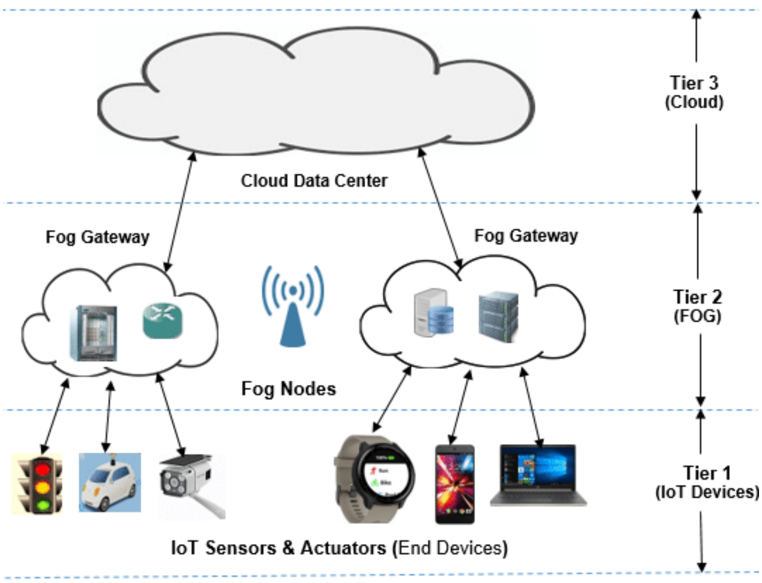

Figure 1: 3 Tier Fog-Cloud computing architecture [14].

1. IOT layer: This layer is made up of IoT devices such as sensors, smart vehicles, drones, smartphones, tablets, and other devices that are closest to the end customer and physical state. They are usually widely scattered geographically and are primarily responsible for detecting data and delivering it to the upper layer for storage or processing.

2. Fog layer: This layer serves as the foundation of the Fog computing architecture. It's made up of a large number of Fog nodes. A Fog node is defined as "the physical and logical network piece that implements Fog computing services," as per the OpenFog Consortium [10]. Fog nodes can compute, transmit, and temporarily store data and can be placed anywhere between the Cloud and the end devices. As a result, Fog nodes are directly attached to end devices to provide services effectively. For example, when giving context information to users, Fog nodes may benefit from Cloud storage and computing capabilities.

3. Cloud layer: Cloud layer is made up of several servers with advanced processing and storage capabilities that deliver a variety of services. Unlike typical Cloud computing architectures, some computations or services may be efficiently shifted from the Cloud to the Fog layer in the Fog architecture to minimise the demand for Cloud resources and boost efficiency.

2.1.2 OpenFog N-Tier Architecture

Figure 2 depicts the N-tier architecture proposed by the OpenFog Consortium [10]. Its primary goal is to provide an inner structure to the Fog layer of the three-layer architecture (Subsection 2.1.1), thereby driving stakeholders when it comes to deploying Fog computing in a specific scenario. Even though the deployment of Fog software and Fog systems is scenario-specific, the key features of the Fog architecture are visible in any Fog deployment.

The idea is to have three main entities (again, reflecting the three-layer architecture proposed in Subsection 2.1.1): endpoints/things, fog nodes, and cloud. The Fog layer, on the other hand, is made up of several tiers of Fog nodes (N-tiers), and the further nodes move away from end devices, the more computational capabilities, and thus intelligence, they gain. Each higher level of the Fog layer refines and extracts relevant data, increasing intelligence at each level. The number of tiers in deployment is determined by scenario requirements such as the number of end devices, the load and type of work addressed by each tier, the expertise of nodes at each tier, latency requirements, and so on. Furthermore, Fog nodes on each layer may be linked to form a mesh capable of providing additional features such as resilience, fault tolerance, load balancing, and so on. This means that Fog nodes can communicate both horizontally and vertically within the Fog architecture [13].

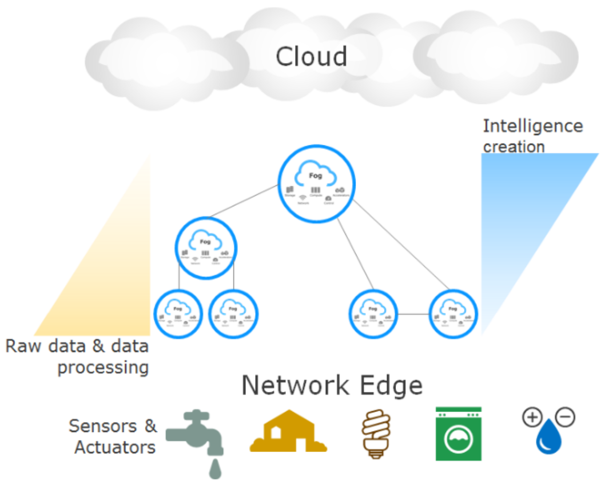

Figure 2: OpenFog N-tier architecture of Fog Computing [6].

Fog nodes in this N-tier vision can be grouped based on their proximity to endpoints and the Cloud :

- Lowest tier: Fog nodes in the lowest layer typically command and control sensors and actuators and are primarily concerned with data acquisition, normalisation, and collection.
- Intermediate tier: The intermediate layer fog nodes are primarily concerned with filtering, compressing, and transforming data received from the lower layer. These nodes, in general, have greater analytic capabilities.
- Highest tier: The fog nodes closest to the Cloud are typically in charge of aggregating data and generating knowledge from it.

3 Characteristics of Fog Computing

Fog computing is a distributed paradigm that lies between Cloud computing and the Internet of Things [6]. As a result, it acts as a link between Cloud computing, Edge computing, and the Internet of Things. This is the trademark of fog computing, but it also brings with it many advantages worth mentioning. When the properties of fog and cloud computing are compared (as shown in Table 1), fog computing offers numerous effective solutions to overcome many of the limitations that exist in the traditional cloud computing model. The main characteristics of the fog computing paradigm are listed below [16].

1. Better Security: The Fog paradigm brings a clear view towards security. In this environment, security is viewed as a fundamental component of architecture. A Fog system can scan for malware, monitor the security condition of surrounding devices, and act as a proxy to automatically update software credentials and detect threats. Furthermore, a fog device can process private data locally rather than sending it to the cloud for processing, assuring greater privacy and giving the user complete control over the data acquired [8].

2. Lower Latency: The Fog architecture facilitates data processing and storage near the user, resulting in low latency. As a result, fog computing perfectly meets the demand for real-time processing, particularly for time-sensitive applications.

3. Efficiency: Since the fog allows data processing tasks to be performed closer to the network's edge, reducing the amount of raw data sent to the cloud, it is the ideal device for using data analytics to obtain quick responses and send only filtered data to the cloud for storage. This improves overall system performance and efficiency.

4. Real-time interactions: Fog applications involve real-time interactions rather than batch processing.

5. Agility: Due to the cost and time required by large vendors to initiate or adopt the innovation, the development of a new service is typically slow and expensive. The Fog world, on the other hand, provides rapid innovation and economical scaling by being an open marketplace where individuals and small teams can offer new services using open development tools and the proliferation of IoT devices [13].

6. Location awareness: In contrast to the centralised cloud, Fog provides services that are broadly distributed. To support mobility, the geographically distributed fog nodes can determine their locations and track end users' devices [17].

7. Cognition: Because the Fog infrastructure is aware of customers' needs and goals, it distributes compute, communication, control, and storage capabilities more finely along the Cloud-to-Things continuum, resulting in applications that better fulfil customers' expectations [13].

8. Scalability: If data created by end devices are regularly sent to the cloud, it may become congested. Fog computing relieves the pressure of centralised processing, addressing the scalability issue posed by the proliferation of end devices in the Internet of Things.

Table 1: Comparisons of Cloud and Fog computing parameters [15]

Parameters	*Cloud computing*	*Fog computing*
Server nodes Location	Within the Internet	At the edge of the network
Client and Server Distance	Multiple hops	Single/Multiple hops
Latency	High	Low
Delay Jitter	High	Very Low
Security	Less secure, Undefined	More secure, can be defined
Awareness about Location	No	Yes
Vulnerability	High Probability	Very low probability
Geographical Distribution	Centralized	Dense and Distributed
Number of Server nodes	Few	Very Large
Real Time Interactions	Supported	Supported
Kind of last mile connectivity	Leased line	Wireless
Mobility	Limited support	Supported

4 Applications of Fog computing

The new fog computing technology provides better quality of service (QoS), reduced latency, and ensures that latency-sensitive applications can meet their requirements. Many industries, including healthcare, oil and gas, automotive, and gaming, stand to benefit from the adoption of this new paradigm. Every IoT application necessitates immediate analysis and action. Most of the time, the action required is so severe that it is either corrective or life-saving. Given the volume of data, the opportunity to use it appropriately should have passed by the time it reaches the cloud.For example, in the healthcare sector, traditional cloud paradigms can pose a potential threat in medical emergency scenarios, but fog can effectively handle this situation. In this section, we will go over a potential use case, ie; a Smart Healthcare system.

4.1 Smart Healthcare System

Figure 3 depicts the architecture of a fog-based Smart Healthcare System. This architecture is composed of three layers: the Thing layer, the Fog layer, and the Cloud layer [18]. End-user devices such as sensors, wearable IoT devices, and actuators that collect body diagnostic data, heart rate, and other information are included in the Thing layer. The Internet gateway, local router, and fog servers are all part of the fog layer. Between the Thing and Cloud levels, this layer communicates and transfers data. It makes judgments for emergency medical scenarios using data from the underlayer. This data can be analysed locally to provide insight into the fog layer, which is an integral part of fog computing. The fog layer deals with a large amount of data provided by sensors and responds quickly. This is a critical step to take in case of a medical emergency. Before further data processing, basic data analysis is carried out. The data analysis technique verifies the data's sensitivity and aids the fog layer in detecting critical circumstances. Thus in emergency scenarios, the system reacts faster [8]. The Cloud layer has servers with massive storage, processing, and analysis capabilities that aid health practitioners in making long-term treatment decisions for patients. Also, it aids in future analysis, studies and prediction use cases.

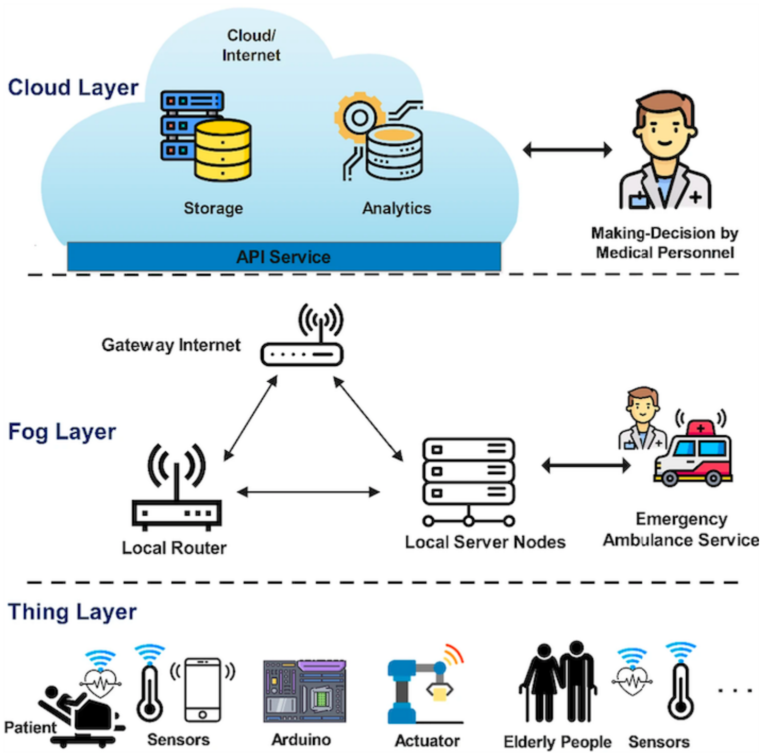

Figure 3: Architecture of Fog-based Smart Healthcare System [18].

5 Challenges faced in Fog Computing

Fog computing is a prospective expansion of the Cloud computing paradigm for dealing with IoT-related difficulties at the network's edge. Fog computing, on the other hand, uses heterogeneous and distributed computational nodes. Furthermore, fog-based services must cope with a variety of features of the constrained environment. As a result, the Fog server must adapt its services, resulting in increased management and maintenance costs. When looking at the characteristics of fog computing from a broad perspective, the following challenges can be identified:

1. Privacy: Fog computing dominates the market with wireless technology, but it raises a major concern in network privacy. Network operators manually create configurations, where fog nodes are deployed at the Internet's edge, and huge maintenance costs are involved in this process [2]. While accessing networks, the leakage of private data is drawing attention.

2. Security: Fog computing is very prone to security breaches because it is built on conventional networking components. In a widely distributed paradigm like Fog computing, ensuring authenticated access to services and maintaining privacy is difficult. The implementation of security methods for data-centric integrity can have a significant impact on the QoS of fog computing.

3. Delay in Computing: Delays caused by data aggregation and resource overuse diminish the effectiveness of fog server services, creating data processing delays. Before data processing, data aggregation should be performed. Resource-constrained fog nodes should be scheduled using a priority and mobility model.

4. Fog Server Placement: It's difficult to arrange a collection of fog servers so that they provide the finest quality service to the local requirements. The maintenance cost can be reduced by analysing the work done in each node in the server before deployment.

5. Network Management: Unless Software-defined networking and Network function virtualization approaches are used, connecting to heterogeneous devices, maintaining fog nodes, the network, and connecting each node would be a hassle [3].

6. Energy Utilization: When fog environments employ a high number of fog nodes, computation is distributed and can be inefficient in terms of energy consumption. As a result, lowering energy consumption in fog computing is crucial

7. Service-oriented issues: Not all Fog nodes have been supplemented with resources. As a result, large-scale application development on resource-constrained nodes is more difficult than in traditional data centres. In this instance, a potential programming platform for developing distributed applications in Fog must be introduced.

6 Conclusion

We examined the fog computing paradigm in this report by describing its fundamental architecture, applications, and key characteristics, as well as the model's current challenges. Fog computing has caught the interest of numerous researchers over the last decade because of its adaptable sensor application architecture. This helps overcome the limitations of cloud computing, as they are located far away from the sensors and data transmission has overhead and delays. Fog computing can handle the huge volume of data generated by the Internet of Things at the network's edge. Fog computing has characteristics such as mobility, proximity to end-users, low latency, location awareness, heterogeneity, and because of its real-time applications, it is regarded as an appropriate platform for the Internet of Things.

Fog computing is entering an exciting period in which it has the potential to reduce operational costs. Fog computing resolve congestion, space, and internet traffic issues that existed in the traditional cloud computing model. In addition, fog computing offers an intelligent platform for managing the distributed and real-time nature of emerging IoT infrastructures. Hence Fog computing will enable network operators to develop these services at the edge, resulting in new business models and opportunities.

References

[1] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854-864, Dec. 2016.

[2] Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International conference on wireless algorithms, systems, and applications. Springer, Cham, 2015, pp. 685-695.

[3] Yi, Shanhe, Zijiang Hao, Zhengrui Qin, and Qun Li. "Fog computing: Platform and applications." In 2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb), pp. 73-78. IEEE, 2015.

[4] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in IEEE Access, vol. 5, pp. 22313-22328, 2017

[5] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, Mar.-Apr. 2017

[6] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," in Internet of Things, Singapore: Springer Singapore, 2017, pp. 103–130.

[7] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K.-K. R. Choo, and M. Dlodlo, "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," IEEE Access, vol. 5, pp. 8284–8300, 2017

[8] H. Wadhwa and R. Aron, "Fog Computing with the Integration of Internet of Things: Architecture, Applications and Future Directions," Dec. 2018.

[9] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," Journal of Network and Computer Applications, vol. 98, pp. 27–42, Nov. 2017

[10] OpenFog Consortium Architecture Working Group and others,"OpenFog reference architecture for fog computing," OpenFog Consortium, White Paper OPFRA001.20817, Feb. 2017

[11] S. Yi, Z. Hao, Z. Qin and Q. Li, "Fog Computing: Platform and Applications," 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), 2015, pp. 73-78

[12] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," 2014 Federated Conference on Computer Science and Information Systems, 2014, pp. 1-8

[13] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog," IEEE Access, vol. 7, pp. 150936–150948, 2019

[14] D. M. A. da Silva, G. Asaamoning, H. Orrillo, R. C. Sofia, and P. M. Mendes, "An analysis of fog computing data placement algorithms," Nov. 2019

[15] Anuj Kumar, K.P Saharan, "Fog in comparison to cloud: A survey", International Journal of Computer Applications, Jul - 2015

[16] P. P, D. K. G., Yaazhlene. P, M. Venkata Ganesh, and V. B, "Fog computing: Issues, challenges and future directions," International Journal of Electrical and Computer Engineering (IJECE), vol. 7, no. 6, p. 3669, Dec. 2017

[17] S. Delfin, N. P. Sivasanker., N. Raj and A. Anand, "Fog Computing: A New Era of Cloud Computing," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019, pp. 1106-1111

[18] V. K. Quy, N. V. Hau, D. V. Anh, and L. A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges," Complex and Intelligent Systems, Nov. 2021