



Paper Type: Original Article

Fog Computing for Distributed IoT Data Processing in Smart City Networks

Zongke Bao

Department of Accounting, Zhejiang University, China; zongkebao@mail.cnas.ac.cn.

Citation:

Received: 25 July 2024

Revised: 12 September 2024

Accepted: 18 January 2024

Bao, Z. (2025). Fog computing for distributed IoT data processing in smart city networks. *Computational engineering and technology innovations*, 2(1), 45-53.

Abstract

The swift expansion of Internet of Things (IoT) devices in urban areas has resulted in immense amounts of data that require prompt and efficient processing. Conventional cloud-based methods often encounter issues related to latency, bandwidth limitations, and privacy risks. Fog computing, which is a decentralized computing framework, emerges as an attractive solution by positioning computing resources nearer to the data origin. This paper investigates the use of fog computing for decentralized IoT data processing within smart city networks. We highlight the main advantages of fog computing, such as lower latency, improved bandwidth efficiency, better privacy, and greater reliability. Furthermore, we analyze the possible applications of fog computing across various sectors in smart cities, including traffic management, environmental surveillance, smart grids, and public safety. By utilizing fog computing, smart cities can fully exploit IoT data to enhance efficiency, sustainability, and the overall quality of life for their inhabitants.

Keywords: Internet of things, Fog computing, Smart cities, Low latency, Decentralized data processing.

1 | Introduction


The proliferation of Internet of Things (IoT) devices in urban environments has led to a massive influx of data. Traditional cloud-based data processing approaches often face latency, bandwidth constraints, and privacy concerns. Fog computing, a decentralized computing paradigm, emerges as a promising solution to address these issues by bringing computing resources closer to the data source.

Key concepts: fog computing: a distributed computing model that extends the cloud computing infrastructure to the network's edge, closer to IoT devices.

IoT: a network of interconnected physical devices, vehicles, buildings, and other objects embedded with electronics, software, sensors, and network connectivity.

Smart city: a city that utilizes digital technologies to improve efficiency, sustainability, and quality of life for its citizens.

Corresponding Author: zongkebao@mail.cnas.ac.cn

 <https://doi.org/10.48314/ceti.vi.47>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

1.1 | Challenges in Traditional Cloud-Based Data Processing

Latency: long distances between IoT devices and cloud servers can introduce significant data transmission and processing delays.

Bandwidth constraints: the massive volume of data generated by IoT devices can overwhelm network bandwidth, leading to congestion and performance degradation.

Privacy concerns: sending sensitive data to remote cloud servers raises privacy risks, especially in contexts like healthcare or surveillance.

1.2 | Benefits of Fog Computing for IoT Data Processing

Reduced latency: by processing data closer to the source, fog computing can significantly reduce latency, enabling real-time applications and improving responsiveness.

Enhanced bandwidth efficiency: fog computing can offload some of the processing burden from the cloud, reducing the amount of data that needs to be transmitted over the network.

Improved privacy: fog computing allows data processing and analysis to be performed locally, reducing the risk of data breaches and privacy violations.

Increased reliability: fog computing can enhance system reliability by providing redundancy and fault tolerance at the network's edge [1].

1.3 | Applications of Fog Computing In Smart Cities

Traffic management: fog computing can enable real-time traffic monitoring, congestion detection, and intelligent traffic signal control.

Environmental monitoring: fog computing can process data from sensors measuring air quality, noise levels, and other environmental parameters.

Smart grids: fog computing can facilitate efficient energy distribution and consumption management in smart grids.

Public safety: fog computing can support public safety applications such as surveillance, emergency response, and crime prevention.

In the following sections, we will delve deeper into the architecture, technologies, and challenges associated with fog computing for distributed IoT data processing in smart city networks.



Fig. 1. Fog computing architecture.

1.1 | Definition of Fog Computing

Fog computing is a distributed computing paradigm where processing is done at the network's edge with seamless cloud infrastructure integration. It enables a computing facility for IoT or other latency-sensitive application environments. It is estimated that about 50 billion "things" will be connected to the Internet by Haroon et al. [2]. Transferring all data from all connected devices for cloud processing will require massive amounts of bandwidth and storage. Not all devices are connected to the controller via IP; other IoT industrial protocols connect them. Because of this, a translation process is also needed to process or store information from IoT devices. Various researchers have defined Fog computing in different ways. Some examples are:

- I. Fog computing is a highly virtualized platform that provides compute, storage, and networking services between IoT devices and traditional cloud computing data centers, typically, but not exclusively located at the edge of the network.
- II. Fog computing is a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among themselves and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can support basic network functions or new services and applications running in a sandboxed environment. Users leasing part of their devices to host these services get incentives.

1.2 | Fog Computing Research Trends

Growing attention towards processing data closer to the users has been observed among industries and academia in the past few years. Handling IoT-generated data at the edge level will help improve overall processing time. This section investigates Fog and other related technological trends in the research community for the past few years. According to the Gartner hype cycle, the peak emerging technology in July 2017 is the smart home, which would perform better by incorporating the Fog computing environment. A Hype Cycle [3] represents common patterns of new trending technologies. Fog computing enables latency-aware smart home services more efficiently (See *Table 1*). Summary of Fog computing definitions. It is a convenient way, especially for emergency response smart home applications. According to the Gartner hype cycle demonstration, other influencing technologies include virtual assistants, autonomous vehicles, IoT platforms, smart robots, edge computing, and smart workspaces required to support latency-aware applications. All these technologies could benefit from the support of the Fog computing paradigm due to latency sensitiveness, connectivity to the cloud, and edge-level data processing capability. Except for autonomous vehicle technology, all technologies above will reach the market adoption threshold in the next 10 years. Besides the hype cycle analysis, we analyzed the search occurrence of Fog and other related technologies in Google Scholar.

2 | Literature Review

The intersection of the IoT and smart cities has led to a surge in data generation and processing requirements. Traditional cloud-based approaches often struggle to meet the demands of real-time data processing, latency-sensitive applications, and privacy concerns. Fog computing, a decentralized computing paradigm, offers a promising solution by bringing computing resources closer to the data source.

This literature review aims to provide a comprehensive overview of existing research on fog computing for distributed IoT data processing in smart city networks. We will explore this domain's key concepts, challenges, and potential fog computing applications.

2.1 | Key Concepts

IoT: a network of interconnected physical devices, vehicles, buildings, and other objects embedded with electronics, software, sensors, and network connectivity.

Smart city: a city that utilizes digital technologies to improve efficiency, sustainability, and quality of life for its citizens.

Fog computing: a distributed computing model that extends the cloud computing infrastructure to the network's edge, closer to IoT devices.

2.2 | Challenges in Traditional Cloud-Based Data Processing

Latency: long distances between IoT devices and cloud servers can introduce significant data transmission and processing delays.

Bandwidth constraints: the massive volume of data generated by IoT devices can overwhelm network bandwidth, leading to congestion and performance degradation.

Privacy concerns: sending sensitive data to remote cloud servers raises privacy risks, especially in contexts like healthcare or surveillance [4].

2.3 | Benefits of Fog Computing

Reduced latency: by processing data closer to the source, fog computing can significantly reduce latency, enabling real-time applications and improving responsiveness.

Enhanced bandwidth efficiency: fog computing can offload some of the processing burden from the cloud, reducing the amount of data that needs to be transmitted over the network.

Improved privacy: fog computing allows data processing and analysis to be performed locally, reducing the risk of data breaches and privacy violations.

Increased reliability: fog computing can enhance system reliability by providing redundancy and fault tolerance at the network's edge [5].

2.4 | Applications of Fog Computing in Smart Cities

Cloud computing is "a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The reference architecture for Cloud computing [6] is depicted in *Fig. 3*. It provides a high-level overview of the cloud and identifies the main actors and their role in Cloud computing. Each actor is an entity, i.e., a person or an organization, that either takes part in a transaction/process or performs some tasks in Cloud computing. There are five main actors: Cloud Provider, Cloud Consumer, Cloud Broker, Cloud Carrier, and Cloud Auditor. The Cloud Provider is an entity that provides a service to interested parties. The Cloud Consumer is an entity that uses a service from and has a business relationship with one or more Cloud providers. The Cloud Broker is an entity that mediates affairs between Cloud providers and Cloud consumers and that manages the use, performance, and delivery of Cloud services. The Cloud Carrier is an intermediary that supplies connectivity and delivers cloud services from cloud providers to consumers. Finally, the Cloud Auditor is a party that conducts independent assessments of the Cloud infrastructure, including services, information systems operations, performances, and security of the Cloud implementation. In terms of interactions, there are several possible scenarios [6]. Generally, a Cloud consumer may request a Cloud service from a provider directly or via a broker. A Cloud auditor conducts independent audits and may contact other actors to collect the necessary information.

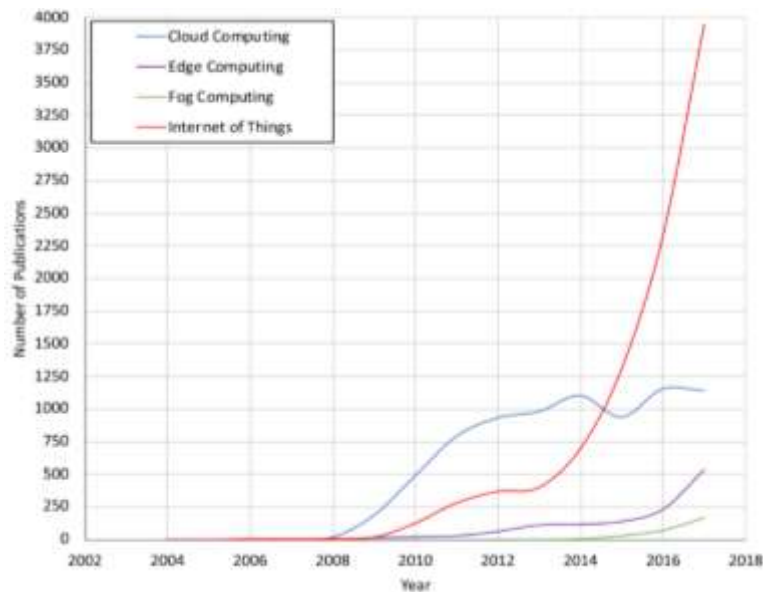


Fig. 2. temporal evolution of the number of scientific publications related to IoT, cloud, edge, and fog computing. Databases used as sources: IEEE xplore DL and ACM DL.

2.5 | Essential Characteristics

The essential characteristics of Cloud computing are summarized below [18]: 1) On-demand self-service: computing capabilities can be provided automatically when needed, without requiring any human interaction between consumer and service provider, 2) Broad network access: computing capabilities are available over the network and accessible through several mechanisms disposable for a wide range of client platforms (e.g., workstations, laptops, and mobile devices), 3) Resource pooling: computing resources are pooled to accommodate multiple consumers, dynamically allocating and deallocating them according to consumer demand. In addition, the provider resources are location independent, i.e., the consumer has no knowledge or control of their exact location, 4) Rapid elasticity: computing capabilities can flexibly be provided and released to scale in and out according to demand. Thus, the consumer perceives unlimited, and always adequate, computing capabilities, and 5) Measured service: resource usage can be monitored and reported according to the type of service offered. This is particularly relevant in charge-per-use or pay-per-user services because it grants great transparency between the provider and the service consumer. Cloud infrastructure is a collection of hardware and software that empowers the aforementioned essential characteristics of Cloud computing.

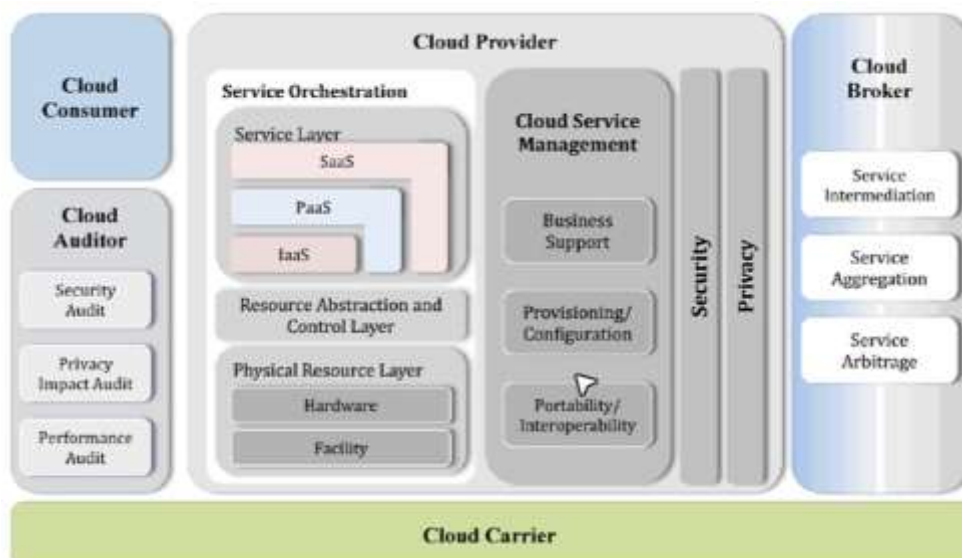


Fig. 3. NIST cloud computing reference architecture.

2.6 | Internet of Thing

Over the past decade, Cloud computing has been the predominant paradigm. According to this trend, computing, control, and data storage have been centralized and moved into the cloud [7]. On the other hand, the Internet of Things (IoT) is now becoming widespread. In 2017, there were about 20 billion IoT-connected devices, which will grow to about 30 billion in 2020 and more than duplicate by 2025.¹ The emerging IoT brings in many new challenges that Cloud computing has a hard time meeting due to its drawbacks. In this section, we provide fundamentals about the IoT.

3 | Definition

The term IoT was originally coined in 1999 by Kevin Ashton, the AutoID Center executive director at Massachusetts Institute of Technology (MIT). Then, it assumed several slightly different meanings. Today, there is no unique and commonly accepted definition of IoT, and several formalizations can be found on the web and in the literature. In this work, the definition given by the International and Telecommunication Union (ITU) assumes that the IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable Information and Communication Technologies (ICT)". In this context, a thing is intended as "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks", while a device is "a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing"¹. In simple terms, the IoT is a collection of computing devices (namely, things) interconnected via the Internet that are aimed at offering services addressed to all types of applications while fulfilling security requirements [8–10].

3.1 | Architecture

Several different IoT architectural models can be found in the literature, but, to the best of our knowledge, the most commonly used is based on three architectural levels: Perception (or sensing) layer, Network (or transmission) layer, Application layer. Each architectural layer is characterized by the devices that belong to it and by the functions performed. The Perception layer aims to acquire data from the environment (such as light, temperature, pressure, humidity, etc.) with the help of sensors and actuators. Basically, the main goal of this layer is detecting and collecting information before transmitting it to the network layer. The network layer is the middle, aiming to provide data routing and transmission functions to the proper destination. Therefore, the main goal of this layer is to efficiently transmit data within heterogeneous networks without losing information. Internet gateways, switches, routers, and other network devices operate at this layer. The application layer is the highest; the information received from the bottom layers is used to implement different services and applications. This layer usually contains the user interface, the formulas related to data models, the business logic, and everything needed for the specific IoT service or application.

3.2 | Various Proposed Architectures for Fog Computing

Layered representation is the best way to represent Fog architecture. Many works have been done to quantify the layer-based concept of Fog architecture. From our review, we found that researchers have proposed three, four, five, and six layers in the Fog architecture. Everyone has their justifications for their claims.

¹<https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide>

If we ignore the user plane, it is obvious that Fog architecture could be defined as three different levels from the high level. As we proceed to the more implementation-type level, the number of layers in the architecture would vary, giving rise to five and six levels in the Fog computing layer. Taneja and Davy presented six layers based on specific tasks. On the other hand, five layers were defined based on a network perspective. Other high-level architectures in Fog computing have also been presented by various researchers, including the hierarchical Fog architecture, Open Fog architecture, Fog network architecture, Fog architecture for the Internet of Energy, Fog computing architecture based on the nervous system, and IFCIoT architecture. After reviewing the literature stated above, the components of Fog computing architecture are defined and presented in the following subsection [11].

3.3 | Components of Fog Computing Architecture

Fog computing architecture consists of several layers. In this subsection, we discuss various components of the Fog computing architecture. The components are divided into several groups based on their functionality, defined as the layer. These functionalities will enable IoT devices to communicate with various Fog devices, servers, gateways, and the cloud. Below is a detailed explanation of each layer, where a smart transportation use case is considered. Physical layer the basic data source for Fog computing is the various forms of data emitted by the sensors. These data could be generated from smart devices, temperature sensors, humidity sensors, smart homes, CCTV surveillance systems, traffic monitoring systems, self-driving vehicles, etc. For instance, if we wanted to implement a smart traffic management and monitoring system, we need to get updated traffic conditions on all roads from various sensors, roadside devices, and cameras, which will help manage traffic signals. It is also necessary to predict future traffic demand by collecting data from various GPS sensors. Besides physical sensors, the role of virtual sensors is also important; if a road accident occurs, it would not be possible to decide using a single sensor whether the road should be blocked or traffic should keep going. The road might have one or more lanes. This occurrence may affect one lane, while another could enable the traffic flow to continue. However, the traffic handling capacity will be decreased due to this occurrence. In this case, a virtual sensor might help obtain an immediate decision on road conditions, traffic multiplexing, and traffic rerouting. Hence, the physical layer consists of physical and virtual sensors; any data generation device could fall into these groups.

3.4 | Difference Between Fog and Cloud Computing Paradigm

Fog computing architectures are based on Fog clusters where multiple Fog devices participate to cooperate with the processing. On the other hand, data centers are the main physical components of clouds. Because of this, cloud computing has high operational costs and energy consumption. By comparison, energy consumption and operation costs in the Fog computing paradigm are low. The Fog is located closer to the user, so the distance between users and Fog devices could be one or a few hops. However, some studies suggest that the distance between users and the Fog is one or two hops, while others argue that it should be one hop with wireless connectivity. Yet, all agree that the distance between the users and the cloud is a multi-hop distance. Due to the distance, communication latency for the cloud is always high compared to the Fog. The cloud is a more centralized approach, while the Fog is a more distributed approach based on geographical orchestration. Real-time Interaction is impossible for the cloud due to its high latency, but Fog computing can easily resolve this problem. On the other hand, the rate of failure in the Fog is high because of wireless connectivity, decentralized management, and power failure. Most devices in Fog environments will be connected wirelessly since smart gadgets and handheld devices will participate in Fog systems. These devices, and other network management devices, are mostly decentralized. These devices could fail when the software is not managed correctly. Users may not be aware of malicious software that could lead to device failure.

Moreover, Fog processing could also fail in other cases; for example, each Fog device is responsible for performing its own application processing. So, the IoT application processing in a Fog device always takes a second priority. If the application of the device fully utilizes the fog device, it will fail to process any fog. Hence, scheduling applications and resources in the Fog is more complex. In addition, failure handling in the Fog is competitive because of power failure, which is only an issue because the devices run on battery power. *Table 2* shows the technical differences between the cloud and the Fog. It cannot be said that Fog can replace the cloud. We cannot conclude that Fog is better than the cloud; both contribute differently by fulfilling different perspectives and requirements.

4 | Conclusion

The Fog computing paradigm is in its infancy, so an extensive investigation is required for this emerging technology. In this survey, we presented and discussed the overview, architecture, state-of-the-art, and other similar technologies in Fog computing. Based on the literature, we derived a taxonomy for Fog computing by analyzing the requirements of Fog infrastructure, platform, and applications. We also covered resource allocation and scheduling, fault tolerance, simulation tools, and microservices in Fog computing. Finally, we presented some challenging and open research issues. This comprehensive survey will bring to light IoT application execution for a Fog computing environment and point toward the direction for current and future research in this rapidly growing research area. In this way, this computing paradigm, which is still immature, will be propelled towards achieving market adoption shortly.

Acknowledgments

The author appreciates the feedback provided during the evaluation process, which contributed to improving the clarity and structure of the discussion. The editorial handling that supported the refinement of the manuscript is also acknowledged.

Funding

No external funding was received for this study, and the research was conducted independently.

Data Availability

This study is based on conceptual analysis and synthesis of existing research in fog computing and IoT systems. No primary dataset was generated; however, relevant references and sources are cited within the manuscript.

References

- [1] Yi, S., Li, C., & Li, Q. (2015). *A survey of fog computing: concepts, applications and issues*. Proceedings of the 2015 workshop on mobile big data (pp. 37–42), Hangzhou, China. <https://doi.org/10.1145/2757384.2757397>
- [2] Haroon, A., Shah, M. A., Asim, Y., Naeem, W., Kamran, M., & Javaid, Q. (2016). Constraints in the IoT: The world in 2020 and beyond. *International journal of advanced computer science and applications*, 7(11), 252–271. <https://dx.doi.org/10.14569/IJACSA.2016.071133>
- [3] Jari, K. O., & Lauraéus, T. (2019). Analysis of 2017 Gartner's three megatrends to thrive the disruptive business, technology trends 2008-2016, dynamic capabilities of VUCA and foresight leadership tools. *Advances in technology innovation*, 4(2), 105. <https://ojs.imeti.org/index.php/AITI/article/view/2521>
- [4] Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2017). A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE communications surveys & tutorials*, 20(1), 416–464. <https://doi.org/10.1109/COMST.2017.2771153>

-
- [5] Dubey, H., Yang, J., Constant, N., Amiri, A. M., Yang, Q., & Makodiya, K. (2015). Fog data: Enhancing telehealth big data through fog computing. *Proceedings of the ase bigdata & socialinformatics 2015* (pp. 1–6). <https://doi.org/10.1145/2818869.2818889>
- [6] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., ... Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication, 500*(2011), 1–28. https://www.cs.cmu.edu/~garth/15719/papers/nist_cloud_computing_reference.pdf
- [7] Goudarzi, M., Ilager, S., & Buyya, R. (2022). Cloud computing and internet of things: Recent trends and directions. *New frontiers in cloud computing and internet of things*, 3–29. https://doi.org/10.1007/978-3-031-05528-7_1
- [8] Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., & Hassan, M. (2019). The internet of things (IoT) and its application domains. *International journal of computer applications*, 182(49), 36-49. <https://doi.org/10.5120/ijca2019918763>
- [9] Mohapatra, H., Rath, A. K., & Panda, N. (2022). IoT infrastructure for the accident avoidance: An approach of smart transportation. *International journal of information technology*, 14(2), 761–768. <https://doi.org/10.1007/s41870-022-00872-6>
- [10] Hossain, N. (2009). HCR using neural network [Thesis]. <https://www.academia.edu/39142624>
- [11] Taneja, M., & Davy, A. (2016). Resource aware placement of data analytics platform in fog computing. *Procedia computer science*, 97, 153–156. <https://doi.org/10.1016/j.procs.2016.08.295>