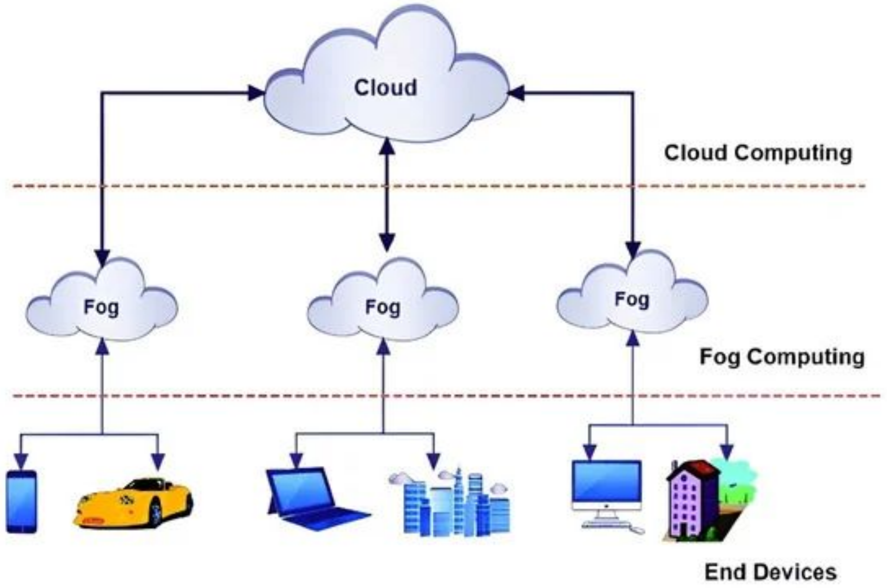
Chapter 4:Introduction to Fog Computing

Definition and basic concepts, Comparison with cloud computing and IoT, Data Management in Fog Computing. Comparison with cloud computing and edge computing. Fog Computing Architecture. Fog node and infrastructure components. Hierarchical and distributed models. Programming Models and Tools for Fog Computing
Self-Learning Topics: Applications and integration of Fog Computing.

Definition and basic concepts, Comparison with cloud computing and IoT,

Fog Computing

As the IoT is distinguished by limited storage and processing power, it also has relatively weak performance, privacy, reliability, and security. Combining IoT and cloud networks in the Cloud of Things (CoT) is one of the best ways to overcome almost all the barriers to the IoT . Moreover, the CoT can streamline the processes of IoT data collection, processing, integration, and deployment . The creation of new IoT applications is complicated due to the huge number of IoT devices with heterogeneous paradigms . Sensors and other devices provide huge amounts of data in IoT applications, generating Big Data that are later processed and analyzed to decide on suitable responsive actions. Data collected by sensors must be analyzed in the cloud, which requires a high bandwidth for the network used. Thus, these issues can be solved by using fog computing .Several fields, especially the IoT, can benefit from fog computing, a new technology that offers many advantages. It was invented by Cisco and provides a way to process data near the information source, making it more rapidly accessible and efficient . IoT users can take advantage of fog computing to access services such as storage and data processing. Just as the cloud delivers services to users, fog computing provides a way for IoT devices to connect to and use these services. Instead of transferring data to the cloud, fog computing offers local storage and processing capabilities to fog devices. Storage, computing, and networking resources are available through both cloud computing and fog computing . As illustrated in figure, fog computing extends the cloud to bring the environment close to the things that interact with IoT data (such as user devices).



Fog computing can be seen as an extension of cloud computing to the edge of the network, where data are processed near the source instead of being sent to the cloud. With the increasing abundance of sensors, more and more data are being generated. In the past, these data were processed and stored in the cloud. However, this approach has several drawbacks, including latency and network congestion .Fog as a service (FaaS) is a new class of service made possible by the Internet of Things and fog computing. Here, service providers create arrays of fog nodes across geographic areas, which act as ownerless resources that can be rented by businesses from many different industries. Every fog node has local computation, storage, and networking capabilities, making it an ideal solution for distributed data processing and analysis . FaaS affords a new method for businesses to offer services to clients. Rather than the large companies that typically operate clouds at different scales, FaaS provides public and private computing, control, and storage services to both large and small businesses. As a result, they can meet the needs of a wide range of clients .To explain how the fog works, the type of directed data from the fog should be identified first. Developers either create fog node ports or IoT applications at the edge of the network. The fog nodes that are near the network edge absorb the data collected from IoT devices, then the fog IoT application directs these data to the optimum place for analysis. The three types of data are

1)The most time-sensitive data: the fog node analyzes these types of data near the things (e.g., sensor systems) that produce the data.
2)Data that ca]n be delayed for minutes or seconds for response or actions: these data are directed to an aggregation node for analysis, evaluation, and action.
3)Data that are less time-sensitive to delay are forwarded to the cloud for archiving and historical analysis, long-term storage, and Big Data analytics.

Data Management in Fog Computing

The processing time in the cloud and delay of transferring cause the latency that affects performance, and that latency is unacceptable in IoT applications like e-Health, because late feedback about a suspicious or emergency situation may endanger someone’s life.
The sensors and end devices periodically generate row data that include use-less, noisy, or repetitive records, but transferring huge amount of data leads to increased errors, packet loss, and high probability of data congestion. In addi-tion, processing and storing the repetitive or noisy data waste the resource with no gain. So interactional applications with large scale of data generation must decrease end-to-end delay and achieve real-time data processing and analytics. Therefore, there is a need to do some local processing. Because of resource constraints and lack of aggregated data in each of IoT devices, however, they are not capable of processing and storing generated data.Bringing the storage, processing, and network close to the end-devices in fog computing paradigm is considered a proper solution. There are many definitions for fog computing. Qin defined it as “a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional cloud computer data-centers, typically, but not exclusively located at the edge of network” . In this way, only on-site processing and storage would be possible. However, fog computing has other benefits, such as better privacy by providing encryption and decryption, data integration, dependability, and load balancing

172 | *8 Data Management in Fog Computing*

Figure 8.1 Structure of data management in fog computing.

Fog plays a role as a mediator between devices and cloud; it is responsible for temporary data storage, some preliminary processing, and analytics. By this way after data generation by IoT devices, fog does some preliminary process and may store data for a while; these data are consumed by the cloud applications, {proper feedback is generated by fog or cloud, and they are returned to a device. A three-layer fog diagram with a data view is depicted in Figure 8.2.

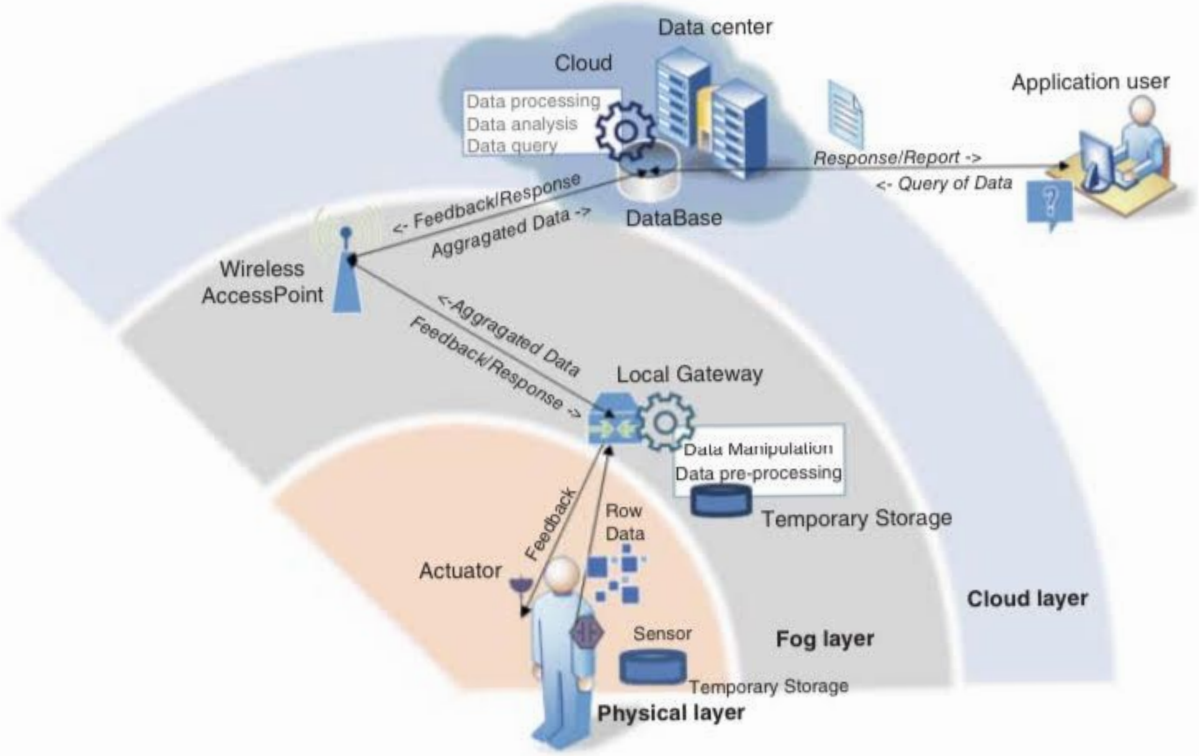


Figure 8.2 Basic data management diagram in fog computing.

Fog data management is about handling the data and its related concepts such as data aggregation approaches, data filtering techniques, data placement,providing data privacy, etc. Based on the three-layer fog architecture, which is shown in Figure 8.2, sensory and collected data as a part of the system are sent to the upper layer and should be managed properly. As before mentioned,end-to-end latency and network traffic are two of main motivations to use fog computing. Local data management yields benefits such as better efficiency,more privacy, and so on. The main advantages of data management in fog computing are described as following:

• **Increasing efficiency:**Local processing on data and elimination of corrupted, repetitive, or unneeded data in fog layer reduces the network load and increase the network efficiency. Because the transferred data to the cloud must be processed, stored, and analyzed in the cloud, by decreasing the amount of data, cloud processing and storage needs would also decrease.

• **Increasing the level of privacy:**Ensuring data privacy is one of the IoT and cloud computing challenges. In IoT systems, sensors may generate and transfer sensitive and confidential data, but transferring them without any manipulation and encryption bears the risk of disclosure. In addition,resource constraint devices cannot handle complicated mathematical operations. The privacy-preserving mechanisms such as encrypting algorithms in end-devices may be impossible. Therefore, privacy, data manipulations and encryption algorithms can be done in a fog layer. Nevertheless, protection of fog devices is another issue that will be investigated further.

• **Increasing data quality** Quality of data would be increased though the elimination of low-quality data such as repetitive, corrupted, or noisy data and the integration of received data in a fog layer.

• **Decreasing the end-to-end latency:** Because of the nature of networks,existence of delay is obvious and inevitable, so response time must account for issues such as network delay and processing time when gathering feedback from cloud in IoT scenarios. Putting data pre-processing close to the devices in fog layer will minimize the end-to-end delay.

.Increasing dependability: System dependability is about the ability of a system to provide the service as is expected. Refer to the definition of dependability which is provided in ISO/IEC/IEEE 24765 [13], three main aspects of dependability are reliability, availability, and maintainability. Fog devices and the local network can cover the possible failure of cloud networks and provide local data processing, therefore, the availability and reliability of a system would be increased.

• Decreasing cost: Local data processing and data compressing in a fog layer reduce the cost of network usage, cloud processing, and storage.However, the cost of fog devices should be considered, and there must be a trade-off.

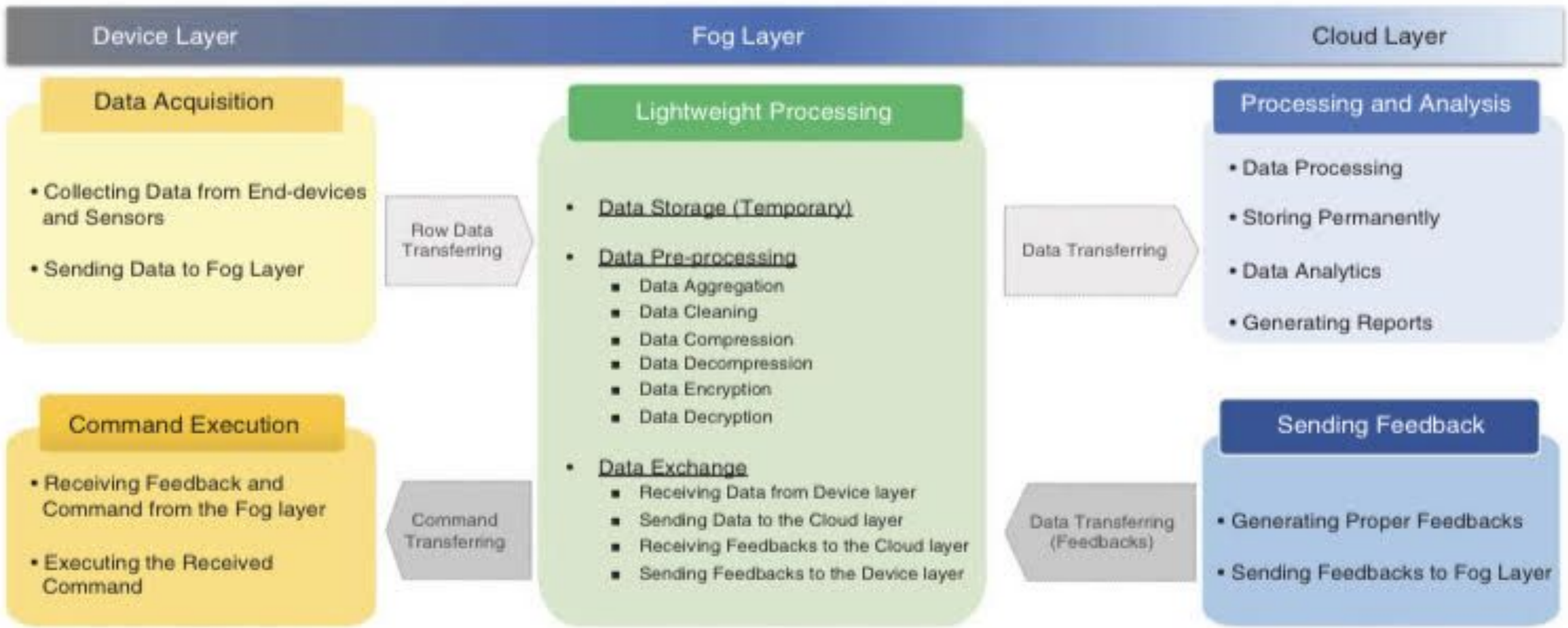


Figure 8.3 Data life cycle in fog computing.

8.3 Fog Data Management

Data life cycle and fog data characteristics as the essential concepts of fog data Management as well as the other important issues in fog computing such as data cleaning, data fusion, data analysis, privacy concerns, and fog data storage.

8.3.1 Fog Data Life Cycle

The fog data life cycle consists of several steps that start from data acquisition in the device layer where data is generated, continue with processing and storing in upper layers and sending feedback to the device layer, and finally end with execution of commands in the device layer. As is shown in Figure 8.3, we consider five main steps: data acquisition, lightweight processing, processing & analysis, study feedback, and command execution.

8.3.1.1 Data Acquisition

Data from different types of end devices should be acquired. It must be sent to upper layers. To this end, a sink node or local gateway node may exist to gather data, or sensors can send data directly to the fog.

8.3.1.2 Lightweight Processing

This step provides lightweight data manipulation and local data processing on the collected data. Lightweight processing may include data aggregation, data filtering, and elimination of unnecessary or repetitive data, data cleaning, compression/decompression, or some lightweight data analysis and pattern extraction. As data may be stored for a while in fog devices, the last period’s data would be accessible locally, so more feasibility for data pre-processing will be provided. The aggregated data will be transferred to the cloud via the network.In addition, the feedback as response data should be transferred to the device.Also, as the feedback is received from cloud layer and sent to the device layer,there may be a need for data decompression, data decryption, doing some format change on the received data, etc. These types of change must be supported by the fog layer.

8.3.1.3 Processing and Analysis

Received data may be stored permanently in the cloud layer, and it is processed based on predefined requirements. In addition, the application users may
access data to get reports or data analysis. Different types of analysis on stored data may be applied to obtain valuable information and knowledge, and these
types of processing and analysis are almost in the scale of big data. They need big data platforms and technologies such as HDFS for storage and map-reduce
for processing .

8.3.1.4 Sending Feedback

Based on data processing and analyzing, feedbacks such as proper commands or decisions are generated and sent to the fog layer.

8.3.1.5 Command Execution

8.3.2 Data Characteristics

Reviewing data characteristics is necessary to define and refine data quality and integration standards and to handle the related challenges properly in the data management process. Data quality refers to how much data characteristics are suitable and can comply with consumer requirements.IoT data characteristics were categorized into three categories:data generation, data quality, and data interoperability. The IoT data quality characteristics include uncertainty, redundancy, ambiguity, and inconsistency.Management of main IoT data characteristics and the related issues can be done in the fog data management process to fulfill the requirements. In the following, these characteristics are reviewed:

• Heterogeneity. Distributed heterogeneous end devices generate data in different formats. Generated data may be diversely varying in terms of structure or format.

• Inaccuracy. Inaccuracy or uncertainties of the sensed data refer to the sensing precision, accuracy, or misreading of data.

• Weak semantics. As mentioned before, the collected raw data that may be heterogeneous in terms of data formats, data structure, data source, etc. Must be processed and managed. Using the concepts of semantic web and injecting some information and extra data to the raw data make the data readable and understandable for machines. Nevertheless, most of the collected data from the environment has weak semantics

• Velocity. Data generation rates and sampling frequencies are varying in different types of end devices.

• Redundancy. Repetitive data that are sent by one or more end devices lead to redundancy in the collected data.

• Scalability. Large numbers of end devices and high data sampling rate that may exist in different scenarios may lead to generation of a huge amount of data.

• Inconsistency. Low precision or misreading in the sensed data may cause inconsistency in the gathered data

8.3.3 Data Pre-Processing and Analytics

Three of the main data pre-processing and analytics concepts that play important roles in fog data management are reviewed. They are data cleaning, data fusion, and edge mining.

8.3.3.1 Data Cleaning

Because of the mentioned characteristics, sensory data are not fully reliable,which is unpleasant for further processing and decision-making. Jeffery et al.stated, “Dirty data” refer to missed readings and unreliable readings.Cleaning mechanisms can be applied on the collected data in fog layers to reduce the effect of dirty and unreliable data, and to increase the quality of them. Data cleaning approaches can be divided in two categories: declarative data cleaning and model-based data cleaning [18]. In the following, each of them is reviewed briefly:

• Declarative data cleaning. High-level declarative queries such as CQL (continuous query language) are used to define the sensor values constraints. In this way, the user can express the queries and control the system easily via the provided interface. Extensible sensor stream processing (ESP),is an example of this type. It is a declarative-based and pipelined framework for sensor data cleaning for use in pervasive applications.

• Model-based data cleaning. Anomalies are detected by comparison of raw values with the inferred values that are resulted as the most probable values based on selected models. The model-based approaches also have subcategories such as regression models. These include polynomial regression and Chebyshev regression [18, 20], probabilistic models such as Kalman filter, and outliner detection models

8.3.3.2 Data Fusion

Data fusion refers to the elimination of redundant and ambiguous data and integration of data, and can be done in the fog layer as one of the data management tasks to increase the accuracy and efficiency. In data fusion was defined as “multilevel, multifaceted process handling the automatic detection, association, correlation, estimation, and combination of data and information from several sources.” Data fusion models can be categorized into three particular categories: data-based model, activity-based model, and role-based model.categorizes data fusion frameworks into four classes based on data-related aspects: **(i) imperfect data fusion framework; (ii) correlated data fusion framework; (iii) inconsistent data fusion framework; and (iv) disparate data fusion framework.** The first category is related to data imperfection, which is one the main data challenges and may be caused by impreciseness, incompleteness, vagueness, or uncertainty [25]. The second category is related to dependency of data. The last two categories are about the conflict and diversity on data. There are some famous data fusion techniques and models, such as Intelligent Cycle (IC) &Joint Directors of Laboratories (JDL)

8.3.3.3 Edge Mining

Fog computing can be effective for local analytics and stream processing to reduce the volume of data. Edge mining refers to utilize mining approaches on row data that are produced by devices in the edge of the network (fog layer). In this way, the size of the transferred data will be reduced and better energy savings can be achieved. Gaura et al. [26] stated that edge mining can be defined as “processing of sensory data near or at the point at which it is sensed, in order to convert it from a raw signal to contextually relevant information.” General Spanish Inquisition Protocol (G-SIP) is one of the edge mining algorithms; it has three instantiations, which are Linear Spanish Inquisition Protocol (L-SIP), ClassAct, and Bare Necessities (BN). L-SIP is a lightweight algorithm for local data compression and aims to reduce data size through the state estimation and improve storage and responsiveness. In this model, end devices and fog devices use a predefined and shared model for state calculation and prediction. In case of unexpected data, data would be sent to the fog devices.Based on [26], L-SIP, ClassAct, and BN reduce the packet transmission by 95%, 99.6%, and 99.98% respectively. Collaborative edge mining is another extension of edge mining that was proposed in to reduce the transferred data size.

8.3.4 Data Privacy

Privacy preserving and protection of data against unauthorized access are considered as one of the fog computing functionalities to keeps malicious and unauthorized end devices out of the system. However, due to the mobility of devices in some kinds of applications such as smart-transportation, the authentication phase must consider the mobility and dynamic nature of the network. Position is a sensitive data point that can represent the owner’s location, and it should be protected, as location privacy is considered as one the data protection issues in the fog data privacy. It was addressed in [28] in secure positioning protocol. The authors defined correctness, positioning security, and location privacy as three properties that the proposed protocol must satisfy to be secure.Providing the privacy of data aggregation was addressed in [5], which proposed a privacy-preserving data aggregation schema for fog enhanced IoT. In the proposed approach, Chinese remainder theorem, one-way hash,and homomorphic Paillier were used for fault-tolerant data aggregation from hybrid IoT devices, authentication, and detection of false data injection in the fog layer.

8.3.5 Data Storage and Data Placement

Data storage and data placement are the other issues that must be handled in fog data management. Based on the predefined policy, data may be discarded after pre-processing or may be stored for temporary in the fog devices for further processing or aggregation purpose. It should be noted that in addition to storage and memory constraints, for the sake of decreasing the end-to-end latency and providing real-time response time, storage should have low-latency, cache,and cache management techniques.Also, making decisions about the duration and volume of stored data is very dependent to application type and infrastructure capabilities. Another issue concerns efficient placing of gathered data in fog storages based on node characteristics, geographical zone, and type of application, because data placement strategy affects service latencies. Naas et al. proposed using iFogStore to reduce the latency, taking into account fog device characteristics as well as heterogeneity and location [29]. Sharing of data by different data consumers, dynamic location of data consumers, and the capacity constraints of fog devices are considered in iFogStore. In addition, to reduce the overall latency, it considers the storing and retrieval times.To provide the real-time decision-making, in based on the basic three-layer architecture, a storage management architecture in edge (fog) computing was proposed. In the edge (fog) layer, the architecture has six components to provide storage, and data management mechanism in a storage constrained system: monitoring, data preparation, adaptive algorithm,specification list, storage, and mediator component. The other two layers are cloud layer and gathering layer (device layer). The first is responsible for storing the historical data and the latter generates the row data.

Comparison with cloud computing and edge computing

	Cloud	Fog	Edge
Latency	Highest	Medium	Lowest
Scalability	High, easy to scale	Scalable within network	Hard to scale
Distance	Far from the edge	Network close to the edge	At the edge
Data analysis	Less time-sensitive data processing, permanent storage	Real-time, decides to process locally or send to cloud	Real-time, instant decision making
Computing power	High	Limited	Limited
Interoperability	High	High	Low

TABLE I: COMPARISON BETWEEN FOG, EDGE COMPUTING

	Fog Computing	*Edge Computing*
1.	Deployed at the local premises of mobile users.	Deployed as a traditional data centre with extended capabilities.
2.	Virtualized device with build-in data storage, computing and communication facility.	Uses an edge server similar to a traditional data centre server.
3.	Can be adapted from existing system components	It is completely built as new system or a mini cloud data centre.
4.	Energy consumption of fog less than cloud services but overhead is high compared to cloud.	Edge uses less resources than the cloud initial overhead to build is high compared to cloud
5.	No central entity controlling the fog cloud	Edge server using cloud technologies and virtualization used to control edge components.
6.	May not be controlled by network operators, uses an ad-hoc distribution.	Allows the mobile network operators improve existing services with edge.

A comparison between layers

Cloud Computing

- Centralized
- High processing & computing
- High latency
- AI processing power
- Highest storing capacity
- Cybersecured

Fog Computing

- Decentralized
- Low latency
- Dedicated bandwidth where most needed
- AI processing power
- Networking effect with other edge site nodes
- Cybersecured

Edge Computing

- Decentralized
- Lowest latency
- Saves Bandwidth
- Processing & networking limitations
- Potential data privacy issues
- Cybersecurity concerns

IoT Devices

seaflux

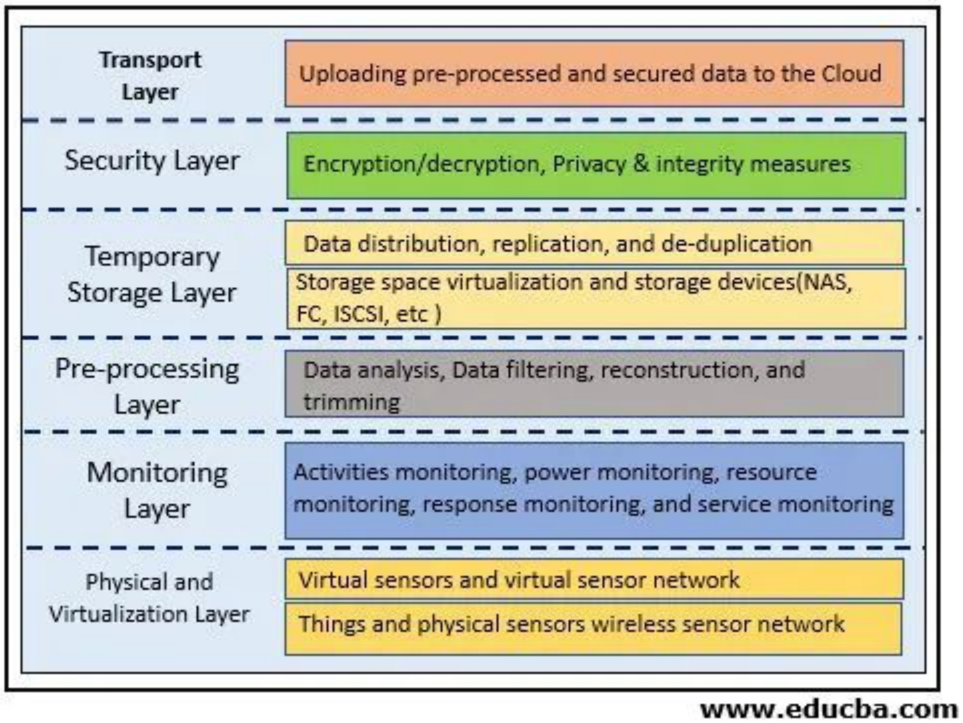
TABLE 2 COMPARISON BETWEEN FOG, EDGE AND CLONE CLOUD MODELS

Edge Computing	***Fog Computing***	***Clone cloud***
1. Close in distance to end user	Close in distance to end user by utilized existing resource provisioning	Uses Cloud Services
2. Latency benefit for users away from the data centres.	Latency benefit for users away from data centers	Application decides when to put data and execution to the clone (uses adaptive schemes to perform decision making).
3. It is a traditional data center with extended capabilities to deploy application at the edge networks.	Cloudlets are used to provide services to mobile users with limited security , distributed load balancing	Data and execution transfer mechanisms, to the cloud by provisioning the cloud servers.
4. Can work for all types of services including IoT platforms.	Can provide services to all types of applications	This scheme provides services at a distributed level
5. Provides its own security and load balancing	Limited security, distributed load balancing.	Distributed load balancing
6. Edge and cloud together forms a three layer service model	Fog and cloud together form three layer service model	It forms a two layer service model.
7. No cost analysis to transfer	No cost analysis to transfer	Overhead of cost analysis to obtain decision to offload
8. Call to edge resources need to be adjusted in the application	Call to fog resources need to be adjusted in the application	Complex application development
9. Resource allocation done by edge	Resource allocation done by fog	Low cost for surrogate resources utilization

Fog Computing Architecture. Fog node and infrastructure components. Hierarchical and distributed models. Programming Models and Tools for Fog Computing

1. Terminal Layer
The terminal layer is the basic layer in fog architecture, this layer includes devices like mobile phones, sensors, smart vehicles, readers, smartcards, etc.The devices which can sense and capture data are present in this layer. Devices are distributed across a number of locations separated far apart from each other.The layer mostly deals with data sensing and capturing. Devices from different platforms and different architectures are mainly found in this layer.The devices have the property of working in a heterogeneous environment, with other devices from separate technologies and separate modes of communication.
2. Fog Layer
Fog layer includes devices like routers, gateways, access points, base stations, specific fog servers, etc., called as Fog nodes.Fog nodes are located at the edge of a network. An edge can be a hop distance from the end device. The Fog nodes are situated in-between end devices and cloud data centers.Fog nodes can be static, e.g., located in a bus terminal or coffee shop, or they can be moving, e.g., fitted inside in a moving vehicle.Fog nodes ensure services to the end devices. Fog nodes can compute, transfer and store the data temporarily.Fog nodes and cloud data center connections are enabled by the IP core networks, providing interaction and cooperation with the cloud for enhancing processing and storage capabilities.
3. Cloud Layer
This layer consists of devices that can provide large storage and machines (servers) with high performance.This layer performs computation analysis and stores data permanently, for back-up and permanent access to the users.This layer has high storage and powerful computing capabilities.Enormous data centers with high computing abilities form a cloud layer. The data centers provide all the basic characteristics of cloud computing to the users. The data centers are both scalable and provide compute resources on-demand basis.The cloud layer lies at the extreme end of the overall fog architecture. It acts as a back-up as well as provides permanent storage for data in a fog architecture. Usually, data that isn’t required at the user proximity is stored in a cloud layer.

Layered Fog Computing Architecture



1. Physical and Virtualization Layer

This layer comprises nodes (Physical and virtual). The nodes perform the primary task of capturing data and are located at different locations. Nodes usually involve sensing technology to capture their surroundings.Sensors used at this node collect data from the surroundings and collect data which is then sent to upper layers via gateways for further processing.A node can be a stand-alone device like a mobile phone or it can be a part of a large device like a temperature sensor fitted inside a vehicle.

2. Monitoring Layer

In this layer, we perform node monitoring related to various tasks.Nodes can be monitored for the amount of time they work, the temperature and other physical properties they are possessing, the maximum battery life of the device, etc.The performance of applications as well as their present state is also monitored.The fog nodes are checked for their energy consumption, the amount of battery power they consume while performing their tasks.

3. Pre-processing Layer
This layer performs various data operations mainly related to analysis.Data is cleaned and checked for any unwanted data present. Data impurity is removed and only useful data is collected.Data analysis at this layer can involve mining meaningful and relevant information from a vast amount of data collected by the end devices.Data analysis is one of the essential features that should be taken into consideration before data is used for a specific purpose.
4. Temporary Storage
This layer is associated with non-permanent distribution and replication of data.Storage virtualization like VSAN is used in this layer.Data is removed from the temporary layer once data is moved to the cloud, from this layer.
5. Security Layer
This layer is involved with the privacy of data, the integrity of data, encryption, and decryption of data.Privacy in the case of fog computing data can include use-based privacy, data-based privacy, and location-based privacy.The security layer ensures secure and preservation of privacy for the data which is outsourced to the fog nodes.
6. Transport Layer
The primary function of this layer is to upload partly-processed and fine-grained secure data to the cloud layer for permanent storage. For efficiency purposes, the portion of data is collected and uploaded.The data is passed through smart-gateways before uploading onto the cloud. The communication protocols used are chosen to be lightweight, and efficient, because of the limited resources of fog computing.

https://www.mdpi.com/2224-2708/11/4/84#:~:text=Just%20as%20the%20cloud%20delivers,processing%20capabilities%20to%20fog%20devices.

https://classroom.google.com/c/NjE2Njg5MzE4MzIz/m/NjE4Nzk1Mjc5MDkx/details

https://www.semanticscholar.org/reader/996c6a4b9dc8c973b8da67059467a24abb562989

Milestone of 80%