International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

FOG COMPUTING IN CLOUD SYSTEM

SWETHA SURESHKUMAR[1] , DR.N.GOBI[2]

[1]Student of MCA, Department of CS&IT, Jain (Deemed-to-be-University),Bangalore 560042, India
[2]Assistant Professor, Department of CS&IT, Jain (Deemed-to-be-University),Bangalore 560042, India
Corresponding author: Swetha SureshKumar (jpc222736@jainuniversity.ac.in)
DOI: https://doi.org/10.55248/gengpi.5.0324.0760

ABSTRACT:

The increased use of Internet of Things (IoT) applications poses significant obstacles for integrated Cloud Computing (CC). These difficulties include worries about network performance, security, and disruptions. The Fog system has emerged to address these concerns by bringing cloud computing closer to IoT. Fog's primary function is to handle data generated by IoT devices at the edge, which entails processing and storing data on the fog node rather of transferring it to a remote cloud server. Compared to traditional cloud solutions, Fog Computing offers superior services with faster reaction times. This makes Fog Computing a promising choice for delivering efficient and safe services to a large number of IoT users.It's vital to realize that Fog Computing works alongside CC rather than replacing it. It permits edge data processing with the ability to maintain a connection to the cloud's datacenter. This methodology improves the efficiency of resource provisioning and service management near devices, at the network edge, or in accordance with Service Level Agreements (SLAs).In between IoT devices and the cloud datacenter, fog computing serves as a mediator. It facilitates information processing effectively, giving Internet of Things consumers faster and more secure services.

INDEX TERMS - Internet of Things (IoT) devices, fog computing, cloud computing, edge computing, cloud computing (CC), and service level agreements (SLAs)

INTRODUCTION:

A growing number of industries and people are depending more and more on desktop computers and smart gadgets to do their regular chores. Large volumes of data are consistently produced and stored by these smart systems thanks to a variety of sensors and apps that create data. The increasing amount of data from different sensors has been primarily caused by the expansion of the Internet of Things (IoT). Big data analytics has drawn a lot of attention since standard databases struggle to handle heterogeneous and unstructured data. Nowadays, businesses are examining data from many devices to extract valuable insights for important decision-making [2].

Because of characteristics like pay-per-use, scalability, and accessibility, industries are moving toward the cloud, which is driving up demand for reliable cloud-based infrastructure. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are among the services offered by cloud computing (CC), which is moving toward the idea of Everything as a Service (XaaS). Furthermore, some IoT applications need processing speeds quicker than standard cloud providers can offer. By utilizing the computational power of nearby smart devices, fog computing provides a solution. It facilitates data processing, networking, and storage at the edge. By utilizing IoT, Fog lessens the necessity of sending data to the cloud for functions like processing, analysis, and storage.

Performance and efficiency are enhanced as a result. Instead of going directly to the cloud, sensor data is routed to network devices, such as edge locations, for processing and temporary storing. By using this technique, the network is burdened less and delays are reduced. Fog Computing in conjunction with IoT creates a novel service paradigm known as Fog as a Service (FaaS). Service providers set up several fog nodes in various geographic regions to act as owners and serve residents from different industries. Every fog node is in charge of handling networking, processing, and storage.

Unlike Cloud Computing (CC), fog uses a distributed computing model, leveraging nearby devices with processing capacity that have fewer but more powerful cores. As a result, a variety of smart devices, including as smartphones, switches, stations, routers, and network device management, are outfitted with computational and storage capacity, functioning as fog computing devices. Research issues arise from fog computing's worldwide

connection and heterogeneous organizational systems. Key concerns in the Fog Computing paradigm are the environment's deployability and the needs that go along with it. This explains why the Fog Computing sector contains a diverse range of computing techniques.

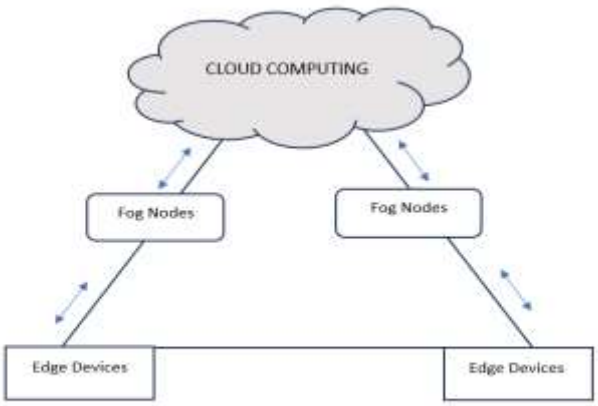

FIGURE 1. Fog computing

FOG COMPUTING :

Fog computing is a highly virtualized system that provides processing, storage, and networking capabilities. It is frequently located at the network edge, sandwiched between conventional cloud computing data centers. Multiple edge nodes, often referred to as fog nodes, with modest processing and storage capacities are part of the fog architecture. A fog network consists of edge nodes and several servers, commonly referred to as cloudlets, that collaborate in an edge computing environment. Clients who use low-latency apps can receive real-time responses by using these fog devices. Although fog computing was first described by Cisco, numerous researchers and companies have given it varied definitions. It is described as a "system-level flat framework" by the Open Fog Consortium, which divides networking, storage, resources, and services for computing across the spectrum from connected devices to the cloud.

Features of Fog Computing :

Similar to cloud computing (CC), fog computing is more closely aligned with Internet of Things (IoT) devices. By serving as a go-between for end devices and CC, it brings networking, compute, and storage functions closer to the edge devices. These gadgets, also known as fog nodes, have network connections and may be positioned anywhere. Any device with compute power, a network connection, and storage can be considered a fog node; switches, servers, routers, and security cameras are a few examples. Fog computing is thought to be the cornerstone of CC. The following is a summary of Fog Computing's primary characteristics:

a. Flexibility:

The network's numerous sensors monitor their environment, and fog offers processing and storage capabilities that integrate seamlessly with these numerous devices.

b. Instantaneous communication:

Unlike the slower batch analysis utilized in the cloud, fog computing allows for fast communication between fog nodes.

c. Dispersed applications:

In contrast to a central cloud, fog provides dispersed services and applications.

d. Fast reaction and position awareness:

Fog can analyze device information more rapidly by locating itself adjacent to edge devices, which cuts down on waiting times. It also enhances one's

sense of location awareness.

e. Compatibility:

Modules for fog can be seamlessly integrated with a variety of platforms and service providers.

f. Cloud connection and web-based analytics:

Fog, which sits between edge devices and the cloud, is essential for gathering and analyzing data close to edge devices.

g. Diversity:

Fog nodes, or edge devices, come in a variety of forms and require particular hosting. They are made by different vendors. Fog can adapt to these variations.

h. Provision of flexibility:

Because fog apps can establish a direct connection with mobile devices, they enable adaptable methods like the Locator ID Separation Protocol (LISP), which necessitates a distributed indexing system.

EDGE COMPUTING :

- Edge computing makes use of the computational power offered by edge devices, such as servers. It sets itself apart from more conventional cloud services by emphasizing Internet of Things (IoT) functionality at the device level. According to a particular study, edge computing is the processing of networks or resources that are located in between data sources and cloud data centers.

- Although sophisticated sensors and gadgets can act as data sources, edge computing takes a diverse approach. A cloudlet, or small data processing center, that serves mobile apps, is an example of an edge in cloud computing. In a similar vein, an edge between cloud computing and IoT sensors is provided by the IoT gateway. Furthermore, when a mobile phone serves as a conduit between the cloud and the application and a cloud computing application.

- Edge computing's fundamental concept is to carry out operations close to the data creation site. Devices in edge computing actively participate in data processing in addition to merely storing data.

- Due to their local computational capabilities, these edge devices require effective service delivery and lessen dependency on central cloud resources. Data execution, data offloading, and information storage are all handled by edge nodes. Additionally, edge devices are essential in fulfilling standards related to confidentiality, dependability, and security while representing cloud computing services to customers.

- By providing intelligence and information to adjacent analytical environments—such as Internet of Things sensors, audio, and video sources—where data is generated, fog and edge computing have a lot in common. Edge computing and fog computing are quite similar in that they both concentrate on controlling processing power inside a small network to do operations that are normally completed on the cloud. By using this technique, industries may make data-driven decisions more quickly and with less reliance on cloud platforms for data analysis and delay reduction.

The architecture of Fog computing :

An approach called fog computing moves some data center tasks closer to the edge of the network. It entails lowering processing, storage, and service network capacities cooperatively between endpoints and cloud computing (CC) data centers. Low and predictable latency for time-sensitive Internet of Things (IoT) functions is the primary objective of fog computing. Several scholars have contributed to the development of several fog reference designs. These architectures, which emphasize various configurations, are made for particular user applications and services.

The well-known reference framework for fog computing, put forth by, is divided into seven levels, each of which has a specific function:

Tier 1: Real and Virtual Indicators
Tier 2: Gateway, Server, and Fog Device
Tier 3: Observation
Tier 4: Before and After Handling
Tier 5: Resource Management and Storage
Tier 6: Security
Tier 7: Utilization

The order of these framework levels is based on how beneficial they are for different kinds of uses. We examine the significance of every level in detail, comprehending its various applications. These tiers share the same goal of streamlining tasks as they migrate from Internet of Things (IoT) devices to fog nodes and ultimately the cloud. In order to fulfill the needs of the users' applications, these levels are designed to handle a variety of duties such as managing, processing, analyzing, and organizing data for both cloud and fog servers. They also handle other jobs linked to the particular services of fog and cloud.

Tier 1: Real and virtual Indicators

The primary data source for fog computing, which forms the basis of this computing paradigm, is the many types of information generated by sensors. Numerous gadgets, including driverless cars, smart homes, temperature and humidity sensors, traffic monitors, CCTV systems, and more, provide this data. Consider a sophisticated traffic surveillance system, for instance. To successfully operate traffic signals, it requires continuous updates on traffic conditions from various sensors, roadside CCTV cameras, and gadgets along roads. It is crucial to gather information from multiple GPS sensors in order to forecast future traffic demands.

Virtual sensors play an important function in addition to physical sensors, particularly in cases like auto accidents. It might not be sufficient to base the decision of whether to close the road or allow traffic to continue on only one sensor. A different route could maintain smooth traffic flow while the impacted route, which may have numerous lanes, affects traffic flow.

But the incident makes it harder to control traffic. In these situations, a virtual sensor can offer prompt solutions for controlling numerous inputs, rerouting traffic, assessing the state of the road, and more. Because of this, the physical level comprises both real and virtual sensors, classifying every gadget that generates data into one of these groups.

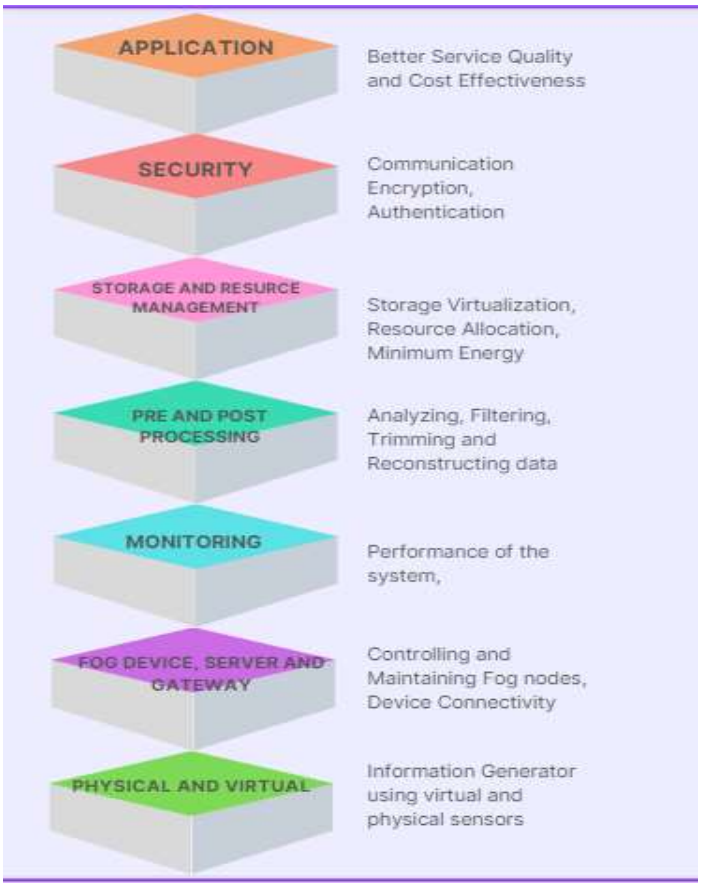

FIGURE 2. FRAMEWORK OF FOG COMPUTING

Tier 2: Gateway, Server And Fog Devices

A fog server, fog device, or gateway can be an Internet of Things device or a stand-alone entity. It's critical to realize that, because it manages numerous fog devices, the fog server requires a different configuration than fog gateways and devices. A fog server's ability to operate successfully depends on a variety of factors, including hardware configuration, network connectivity, and the quantity of devices it oversees. The fog server's

position inside the IoT ecosystem determines its function. Fog devices are connected to groups of real and virtual sensors, and the fog server is connected to groups of fog devices. Since the fog server is primarily responsible for managing the fog devices, it needs to be more capable of processing and storing data than the fog devices themselves. The same server is connected to certain groupings of fog devices.

Certain application computations may be dependent on other groups of fog devices in scenarios such as smart transportation. For example, you may require information from several fog device or sensor group sets if you're requesting a route that uses the least amount of fuel.

The computations need to be distributed among multiple servers and fog devices in order to make intelligent conclusions. The jobs comprise managing and monitoring data on both software and hardware installations, both at the fog server and device levels. It also entails managing the servers' and devices' network connections. This tier is in charge of controlling the processing demands that various apps impose. The amount of information that has to be processed depends on the information flow, the total number of IoT devices (including those connected to fog devices) and the total number of fog devices connected to fog servers. Additionally, this level handles the connection between many fog servers.

Tier 3: Observation

The monitoring level is essential for monitoring the system's resources and performance, as well as for giving feedback and utility. The operating system is monitored by selecting critical resources and keeping an eye on their performance. Certain processes, such as those in smart transportation systems, may consume resources on fog devices for calculations or storage, which may have an impact on their availability. On the fog server side, the same thing is possible. Devices and servers on the fog side request assistance from other peers in these situations. Therefore, the configuration of the system monitoring components determines how well these replies function. The resource demand section examines the resources that are currently available and projects future resource requirements based on user behavior and use trends. This approach is intended to manage potentially dangerous scenarios where errors could happen. The prediction monitor indicates the fog system's performance based on resource availability and network load. Maintaining the necessary Quality of Service (QoS) characteristics outlined in Service Level Agreements (SLAs) depends on this. Penalties for persistent SLA violations may raise system expenses. Performance prediction can lessen overall SLA violations by predicting system performance and usage, even if it cannot totally remove these penalties.

Tier 4: Before and After handling

This level consists of multiple components and focuses on analyzing both simple and complex data. Its primary responsibility is to collect data through analysis, filtering, trimming, and, if required, reconstruction. Following data processing, a component known as data flow determines whether to keep the data locally in the fog or for a longer period of time on the cloud. Dealing with information at the edge and attempting to retain only the data that is necessary is a major difficulty in fog computing. The basic concept is to send data that is utilized often to fog servers and data that is used seldom or for long-term storage to the cloud.

Various sensors provide data for smart transportation apps. To obtain the relevant data, we examine and process this information. However, not all of the data produced might be required. In certain cases, data is generated every second; however, to maintain a minimal volume of recorded data, only the average values for a minute or an hour are retained. In a different scenario, we might change a substantial amount of data by reducing the number of readings if information remains unchanged for a predetermined duration of time but performance is impacted. The goal is to satisfy the application's requirements, even when achieving complete accuracy might not be achievable.

Data reconstruction, which handles imperfect sensor data and allows for error, is another component of this level. This section ensures that in the event of a sensor failure, the data is reassembled using the data pattern, preventing further disruptions and the app from crashing.

Tier 5: Resource Management and Storage

Data preservation via storage virtualization is the responsibility of the storage component. Data backup is a component that ensures data is accessible and safeguarded against loss. Through the use of storage virtualization, a collection of hardware components functions as a single, manageable storage unit within the network. The primary advantage of storage virtualization is its cost-effectiveness in terms of hardware and storage, which improves business operations and simplifies storage. It's crucial to back up data because storage can fail; the data backup section takes care of this by establishing frequent data backup plans.

Planning, allocating resources, and energy conservation are all included in the resource management level. Reliability is one component that deals with maintaining the dependability of resource distribution and application design. Fog resources ensure that they can manage high resource demand, particularly during peak hours. The fog platform expands both vertically and horizontally, while the cloud platform expands horizontally. The allocation of resources presents a challenge in systems with numerous dispersed resources. The resource distribution division is responsible for allocating, reclaiming, and distributing resources in order to address issues.

Because many programs utilize fog areas concurrently, scheduling becomes crucial. The application scheduling section manages a wide range of application objectives. In order to reduce expenses, this level also includes an energy-saving section that manages all resources. The reliability component ensures that the system remains dependable by several techniques, such as redundant data centers, additional fog nodes, tracking the intervals between fog node failures, and estimating the latency for significant issues in Internet of Things applications. The intricate configuration of the fog system is intended to manage clouds, fog nodes, fog servers, and IoT devices.

Tier 6: Security

The security level addresses several safety concerns, such as communication encryption and data security. It guarantees the privacy of fog users' personal data. Consider the fog environment as a cloud-like utility system.

In contrast to the cloud, where users access services directly, clients connect to the fog system in order to access services, and all communication with the cloud is handled by a middle-tier component. Users must therefore obtain permission in order to utilize a service, and the validation process verifies that user requests made over the fog are legitimate.

It is critical to maintain security by encrypting communications in order to prevent malicious people from accessing the system. Different connections to and from IoT devices and the cloud are kept secure by the encryption component. Since many fog components are connected via wireless connections, security is a critical consideration. It's crucial to protect user data in the fog.

Certain services in smart homes or cities struggle because user data needs to be kept private. In the modern world, people frequently accept safety regulations without giving them much thought. For this reason, it's critical to consider providers where consumer privacy is a top priority.

Tier 7: Utilization

Originally developed for Internet of Things applications, the fog has found widespread use, particularly in systems that suffer from latency and depend on Wireless Sensor Networks (WSN). Virtually all applications that deal with latency have begun to leverage the advantages of the fog configuration. This covers a variety of services, such as utility services, that use fog computing to reduce costs and improve services.

Fog infrastructure can also improve applications using Augmented Reality (AR) technology, suggesting a bright future. The fog setup greatly aids in satisfying the augmented reality's fast processing requirements, improving various augmented reality services throughout time.

THE PROPOSED FRAMEWORK FOR CATEGORIZING FOG COMPUTING RESEARCH :

Recent years have seen a significant amount of study on edge, fog, and cloud computing. Given the wide range and depth of research and development efforts in this field of fog computing, it's critical to establish a framework in order to identify patterns, identify obstacles, and direct future work. Fog computing issues were categorized into seven primary problem categories in a significant study: resource management, networking, QOS, computation offloading, interfaces and programming models, accounting/billing/monitoring, and resource management.

Expanding upon previous classification schemes and the wealth of literature in this area, a novel organizational scheme has been proposed. Algorithms, technology, and architectural design are the three primary research topics. An overview of the system is provided by architectural design, which highlights its primary functional components and organizational structure. Subsequently, algorithms and technologies are explained in greater detail, elucidating the underlying procedures, tasks, and methods utilized in various architectural features. The six primary categories that comprise these three domains are computing paradigm, application, software, networking, computing resource management, and security. Each of these domains is employed in a variety of subject areas. As a result, a comprehensive list of research fields is produced, combining previous classifications and developing a framework that meshes with every prior set of categories.

FOG SYSTEM ALGORITHMS :

This section examines the classification of fog algorithms into three groups: tasks planning, resource allocation and loading, and fog node and device unloading.

Job Planning

Fog computing improves computation at the network edge, yet it raises a crucial issue about task effectiveness. Simply put, the task at hand involves determining which tasks belong at the cloud, fog, or IoT level.

Allocation of Loading and Unloading

Numerous techniques have been proposed for work scheduling in fog systems. When allocating computational jobs to fog nodes across many layers, they occasionally overlook the possibility of workload imbalances amongst fog
nodes. On the other hand, they solely concentrate on the fog layer, adding additional or directing the reorganization of tasks through a coding structure.

Resource Allocation

The primary focus of fog system computing is on the resource sharing and cooperative behavior of fog nodes. These properties are controlled in the fog layer to satisfy processing requirements. The author examines small movable fog-enabled structures to determine how to allocate computing resources to certain fog nodes. In order to balance the workload on the cellular device, these small cells form small groups, each of which is similar to a cluster of small cells that share resources. They address a comparable problem, but in the context of a mobile fog system. It features a cloud that can be accessed via the mobile structure and a fog layer created by mobile devices. Utilizing the CPU, bandwidth, and shared storage as efficiently as possible to support computational demands is the aim.

Our three-layer fog security model illustrates the flow of data and requests through the system and highlights potential points of attack at each tier. End-user devices connect to the fog system through the fog-access layer, which controls access and manages the devices. All of the computing nodes in the fog layer, including the access nodes, are covered by fog-computing. This layer ensures that data remains private by addressing vulnerabilities pertaining to the availability and integrity of the system. While establishing a connection between the two subsystems, the fog-cloud interconnection layer tries to stop any threats.

Security in the Access Layer

Ensuring the security of authentication, authorization, access control, and data protection for devices at the edge connecting to the network in a widely dispersed configuration is the main responsibility of the access layer. As conventional security techniques have been extensively discussed in previous research, this layer addresses issues unique to a fog system. This encompasses its dispersed and decentralized structure, including interoperability and mobility support, and incorporating location awareness.

Security in the Fog Layer

All nodes performing sub-cloud computing are part of the computing layer, and some of these nodes also perform tasks in the access layer. Fog nodes at the periphery of the network, for instance, can cooperate in a dispersed manner.

Security in Fog-Cloud Interconnection

Numerous servers in the cloud layer house service applications and frequently perform extensive computations using fog node data. Ensuring the security of the entire system depends on the interoperability and secure connectivity of the various computing tiers. Although maintaining the security of the cloud layer is a major component of a multi-level computing architecture, it is covered in another study.

Here, we present a comprehensive methodology to assess the current state of technology and predict its future directions. It provides a score ranging from 0 to 5 to indicate the level of technological advancement. The approach examines five primary factors:

A well-established ontology:

This entails structuring solutions, resolving issues, and precisely defining terms and subjects. It is crucial to have thorough surveys and system designs in this case.

2. General architecture:
This includes describing the physical components and levels of the system as well as how they interact and function.

3. Reference architecture:
This is primarily concerned with illustrating the logical components, their connections, and the data flow inside the system.

4. Universally approved components:
In order to create and utilize modules that function well together, it is critical to have components that are widely acknowledged.

5. Standard APIs and interfaces:
We need to employ standard methods for components to interact and communicate in order to ensure that various components can function together in a significant way.

6. Obstacles in the Research of Fog Computing:

With the rise in low-cost IoT devices, fog computing—which originated from cloud computing—has become increasingly important as a computationally economical option. These gadgets, which include sensors and cellphones, assist in decentralized computing at the edge, bringing down processing expenses and facilitating data transmission to the cloud. Concerns about security and privacy are also addressed by this move. But computing at the edge raises

new issues with networks, security, hardware, and Fog's interaction with the Internet of Things. The challenges encountered in developing Fog solutions are briefly discussed in this section.

CHALLENGES IN DEVICES AND NETWORK :

- Decentralized Framework: Fog computing is distributed, creating a recurring structure on edge devices using the same code. Reducing this repetition is crucial to maximizing the effectiveness of the Fog system.

- Networking Resources: The dispersed distribution of network resources at the edge of the fog architecture results in more intricate linkages. Resource allocation for the apps that use them may be facilitated by a well-structured network with middleware managing a shared set of resources at the edge.

- Device Heterogeneity: The diverse structure at the conclusion of the Fog architecture is created by the devices' differences from one another. Fog-compatible apps must take these variations in devices and networks into consideration.

Computational Challenges

Computation at Various Levels: Fog systems use cloud servers to process user requests fast for certain activities, while also transmit work to the cloud for lengthier procedures. It can be difficult to decide which jobs belong on the edge or in the cloud.

Distributed Computation Resources: We must obtain resources from other fog nodes when there are occasionally insufficient resources available for computation at the edge. It's crucial to create a common pool that includes memory, processing power, and network resources so that other apps can reserve what they require.

One drawback of the Fog system is portability: moving nodes around in the Fog edge necessitates that compute be present everywhere in the Fog arrangement.

b. Computations in a Distributed Environment: Fog Computing requires dispersed computing, so in order to ensure accuracy, programs must be created with as little computation discrepancies as feasible.
Mobilization Challenge: Determining the optimal number of layers for an Open Fog setup may be a time-consuming task, as additional layers may result in delays. A predetermined
number of layers is crucial, and the outcome of mobilization is contingent upon various factors, including the nature of the activity, the utilization of sensors, the effectiveness of the fog devices, and their speed and dependability.

Utilization of Resource Challenge
- Due to the wide variety of devices, resources are used differently in fog configurations. It's critical to forecast resource utilization over time, particularly when resource locations may shift while fog tasks are being completed.

OBSTACLES IN FOG COMPUTING :

Fog Device Breakdown Challenge:

The likelihood of a fog device malfunctioning increases when it is dispersed and not managed from a central location. Device malfunctions may result from user error, malfunctioning hardware, malfunctioning software, and problems with power, connectivity, and mobility. For these problems to have effective answers, research is required.

Request Provision Handling Difficulty:

Fog must deal with several IoT devices that occasionally answer and occasionally do not. Ensuring the continuous availability of services becomes difficult as a result. The best way to maintain service availability in Fog configurations requires further investigation.

Complexity Challenge:

Fog Computing makes use of several sensors and Internet of Things (IoT) devices manufactured by various businesses. It is challenging to decide which course of action is optimal given this variability. Because there are so many variations in hardware, software, and requirements, choosing the best approach can be challenging, particularly for security applications that require specific devices and protocols.

Fog Computing's Security and System Management Challenges :

Security Issues

- The Fog architecture makes use of a variety of devices that are susceptible to different types of attacks, such as the man-in-the-middle attack. Security issues with data and networks, as well as issues with cloud data centers, are major problems. It is crucial to ensure that fog devices operate securely at the edge when they are utilized in unsecure environments.

System Management Challenges :

a) Service-oriented Computing:

In fog computing, the services that consumers receive are divided into smaller components and dispersed around the edge and cloud. It is quite difficult to efficiently organize and provide these services using Fog architecture. This involves organizing, integrating, and placing minor services in the appropriate locations.

b) Resource Management:

Because fog computing is adaptable and dynamic, there are difficulties in relocating and starting up resources as well as in dealing with delays. When these difficulties are effectively managed, sufficient resources are available even in the face of problems.

The integration of fog nodes and the cloud In order to provide services from Fog nodes to the cloud and maintain Quality of Service (QoS) features, it is necessary to carefully arrange how various edge devices and cloud servers will cooperate. For fog computing, it is crucial to ensure that these devices are interoperable and to manage the cloud configuration for processing and storing data in a heterogeneous environment.

CONCLUSION :

A variety of technologies, including edge, cloud, mobile, and fog computing, are compared in this article. Additionally, it establishes a classification for study on fog computing in fields including networking, resource management, system, application, and software as well as security. The study examines fog computing architecture, methods, and technologies while presenting different viewpoints on the logical and physical elements of a fog computing environment. While some architectures concentrate on individual nodes, others consider the network as a whole. The study addresses research difficulties and future objectives in each topic area and evaluates proposed architectures according to predetermined criteria.

The Internet of Things (IoT) is becoming more prominent in the current situation, affecting our day-to-day activities. The Internet of Things (IoT) links everything around us, yet its gadgets are constrained by low processing and storage power. Issues with traditional cloud computing (CC) include higher latency and network outages. As CC gets closer to IoT devices, fog computing has becoming more prevalent. It decreases wait times for important applications by processing data at fog nodes. There are benefits for a variety of applications when IoT and fog computing are combined. This study provides an in-depth architecture for fog computing, several computing paradigms, and an analysis of the synergy between fog and IoT.

The talk discusses different fog system methods and lists the obstacles facing fog computing development. To put it briefly, the research intends to provide an overview of current contributions to fog computing and IoT research in the modern world, as well as future research and obstacles in integrating fog with IoT.

REFERENCES :

[1] Big data computing and clouds: Trends and future directions Assuncao M.D., Calheiros R.N., Bianchi S., Netto M.A.S., Buyya R.
Parallel Distribution and Computing, 79–80 (2015), pp. 3–15
Google Scholar
[2] A user-prole-aware policy-based management framework for greening the cloud, F. Alhaddadin, W. Liu, and J.A. Gutiérrez, Proc. IEEE 4th Int. Conf. (BdCloud), 2014, pp. 682–687.
Google Scholar
[3] Fog computing: Principles, architectures, and applications, A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya.
Google Scholar
[4] Garaghan P., Lin T., Xu J., Rovatsos M., et al. (2017) Internet Compu, 21 (pp. 16–24): fog orchestration for internet of things services
Examine in Scopus Google Scholar
[5] Yang, Y., FA2ST: Fog as a service technology, in Proceedings of the IEEE Annual Computer Software and Applications Conference, July 4–8, 2017, Turin, Italy, p. 708.
Google Scholar

[6] Mahmud R., Kotagiri R., Buyya R. A survey and recommendations for the future of fog computing Internet of Everything, pp. 103–130, Springer, Singapore (2018)
Examine in ScopusGoogle Scholar