Journal of Autonomous Intelligence (2022) Volume 5 Issue 2.
doi: 10.32629/jai.v5i2.545

Review Article

Fog Computing: Applications, Challenges, and Opportunities

Rajanikanth Aluvalu[1*], Lakshmi Muddana[2], V Uma Maheswari[1], Krishna Keerthi Channam[3], Swapna Mudrakola[4], MD Sirajuddin[5], CVR Syavasya[2]

[1] *Chaitanya Bharathi Institute of Technology, Hyderabad 500075, India*

[2] *School of Technology, GITAM, Hyderabad 502329, India*

[3] *Vasavi College of Engineering, Hyderabad 500031, India*

[4] *Matrusri College of Engineering, Hyderabad 500059, India*

[5] *VIT, Vijayawada 522002, India*

ABSTRACT

Cloud computing, is a widely accepted utility computing model. All the application processing takes place in the cloud data center managed by the cloud service provider. This includes network latency and delays in processing. Each time the application is executed, data has to be transported from node to the cloud. This will increase network traffic and is practically not feasible to transport data from node to remote cloud server and back. Fog computing, a new paradigm of cloud computing will help in overcoming this challenge. In fog computing technology, the data processing tasks are executed at the node level either completely or partially, which highly increases the speed of responses. Also, it reduces latency, processing costs, and bandwidth problems, and improves the efficiency of customer driver services with better response time. Fog is highly useful in locations where network connectivity is an issue because fog has a separate protocol suite that will support weak network connections. In this article, the various parameters of the fog computing paradigm such as challenges, application, and opportunities are studied and presented.

Keywords: *Fog Computing; Edge Computing; Customer-Driver Service; Cloud Computing*

ARTICLE INFO

Received: Feb 6, 2023
Accepted: Mar 19, 2023
Available online: Mar 30, 2023

***CORRESPONDING AUTHOR**

Rajanikanth Aluvalu
rajanikanth.aluvalu@ieee.org

CITATION

Aluvalu R, Muddana L, Uma Maheswari V, *et al.* Fog Computing: Applications, Challenges, and Opportunities. Journal of Autonomous Intelligence 2022; 5(2): 24–43. doi: 10.32629/jai.v5i2.545

1. Introduction

Cloud computing is a computing model that becomes apparent to make computing resources obtainable as paid services. Even though it is continuously developing to satisfy the increasing resource demands, it has a few boundaries and the most dominant one is the large distance between the cloud data centers and target users, which imposes the delay issue, particularly for real-time businesses like live video streaming, or latency-essential programs such as calamity tracking structures. To handle these challenges fog computing is encouraging problem-solving solutions for cloud computing which will act as an extension that provides networking resources and analytical services to the end users. Fog computing is the word first coined by CISCO in 2012, that enhances cloud services by providing processing and storage capabilities near the data sources rather than transporting data centers. The fog computing paradigm enhances the cloud services to meet the requirements of a huge amount of data generated by end-user devices. **Table 1** shows the cloud and fog computing parameters. This computing paradigm is not an alternative for cloud computing but serves as an extension to the cloud to provide low latency for real-time services. The google trend graph is shown in **Figure 1**.

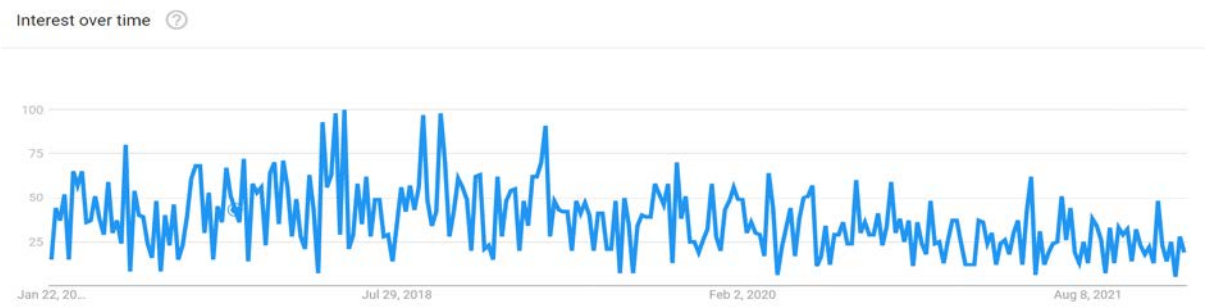

Figure 1. Worldwide popularity of the term "fog computing" on google trends.

Table 1. Comparisons of the parameters of cloud and fog computing[1]

Cloud computing and fog computing comparison		
Parameters	**Cloud computing**	**Fog computing**
Server nodes location	Within the Internet	At the edge of the network
Client and server distance	Multiple hops	Single/multiple hops
Latency	High	Low
Delay	Jitter high	Very low
Security	Less secure, undefined	More secure, can be defined
Awareness about location	No	Yes
Vulnerability	High probability	Very low probability
Geographical distribution	Centralized	Dense and distributed
Number of server nodes	Few	Very large
Realtime transactions	Supported	Supported
Connectivity	Leased line	Wireless
Mobility	Limited support	Supported

2. Related studies

The architecture of the fog computing network: to control entire data storage requires large networks in cloud computing with IoT. There are few challenges in cloud computing like latency, lagging in communication between IoT devices and cloud data. To overcome this, fog computing is introduced in IoT architecture. Fog computing is introduced between cloud and the IOT devices and introduced by Bonomi from Cisco first as shown in **Figure 2**[2]. Routers, gateways, base stations, servers of fog, access points and similar devices are called fog nodes. Fog nodes are situated at network edges with a hop distance from the end device. As we discussed, fog nodes are placed between cloud data storage and IoT devices[3] or end devices. Fog nodes are not dynamic; it undermines some of the "anytime/anywhere" benefits of cloud computing, like bus stops in some areas. Fog nodes' main concern is to give services to IoT devices and transfer the data, store the data, or compute the data that may not be permanent. IP networks are activated by the fog nodes and cloud data storage connections, communications and storage processing capabilities. Series of nodes receive data from IoT devices in real-time and compute the architecture. The data will be received from nodes in millisecond response time. The fog architecture needs more computing capabilities and speed for connecting IoT[4].

Fog computing in the network connecting nodes straight gives the records to nodes. The main advantage of fog computing is to send the data quickly to nodes. Fog computing is placed under the

physical layer in the architecture. Fog computing layers need to connect physical gadgets and transform the data. Virtualization[5] is supported by fog computing, with fog nodes connecting to more IoT devices under virtual node support. Edge devices are linked with a fog computing layer with a centralized cloud computing layer. The fog computing layer can be used in various domains like smart cities by covering huge geographical areas with large IoT networks and connected to cloud data storage with the help of centralized control. Fog nodes are stated in smart cities[6] in different places like subways, bus stops, cell towers, roads, signals, government buildings, shopping malls or can be placed in houses or small shops. The nodes in the IoT domain[7] are between edge to edge or fog to fog or fog to edge or fog to cloud nodes. For example, communication between fog nodes uses wireless sensor networks or local area networks or 5g for internet connection. The major disadvantage is that the method is costly and takes so much time.

Fog computing gives better security and is easy to access with fog nodes, and they can join or leave the network easily at any time. Developing the fog is easy. It requires the correct tool to run the machines as per the requirement of clients. Data analysis is done locally, leading to low latency[8] by using less bandwidth for round trip time, helping to make quick decisions with low latency and avoiding accidents. Data can be accessed locally and transferred to the cloud for further processing. Another disadvantage of fog nodes is high power consumption[9]. Fog computing is related to hardware costs[10] compared with cloud and edge computing. Primary issues of fog computing are security, privacy and middle man attacks.

Fog computing is required to maintain the server nodes in very large sizes[11]. In fog computing, nodes must be placed in server nodes to the local network edge. Fog servers[12] must be deployed at fixed locations where the possibility of failures in the system and natural calamities will destroy the fog servers. The fog layer cannot be placed at the computational place, which leads to a lack of security. Fog is required to place gateway devices to connect fog to clouds, which is costly. Fog consumes more power, and it is difficult for scheduling to transfer from devices to fog nodes and vice versa. Fog computing design can vary from one architecture to another because there is no fixed architecture design for fog computing.

Big data[13] classification is purely dependent on the cloud data for pre- and post-processing. In fog, the big data methods are pre-processed initially with various devices. The processed data is transferred to the cloud for future post-processing. Less number of resource properties is used in fog devices to compile the big data applications on fog.

Another issue in fog architecture is limited resources than cloud. Fog clusters are being used to process huge data to execute big data applications. Various frameworks use various architectures with different layers in the architecture[14], and discuss the usage of sequential learning algorithms in the big data analysis architecture framework in fog computing. This framework had the disadvantage of the regular speed of computing nodes without thinking of memory access times. The service-oriented architecture framework is developed with dynamic time warping and clinical speech processing chain algorithms that may not be able to achieve the speech complexity analysis to identify accuracy in speech disorder[15]. Homomorphic encryption is applied in the framework of health and wellness applications in the research of Kocabas *et al.*[16], but distributed fog computing is unavailable. The incentive mechanism is not applied in distributed resource sharing scheme[17], which applies the hybrid alternating direction method of multipliers algorithm for sharing and allocating resources in the framework. Another main issue is the security and privacy concerns of E-learning architecture with a cloud framework that uses distributed hash tables and machine learning algorithms[18].

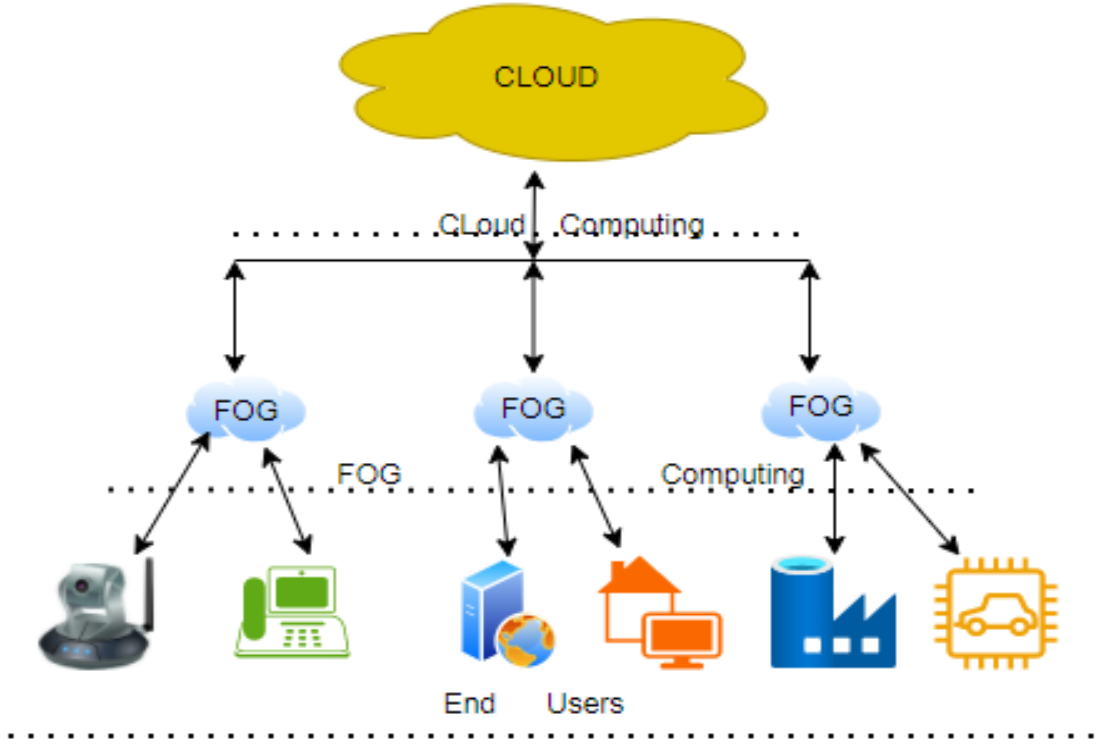

Figure 2. The fog computing architecture.

3. Challenges in fog computing

The following characteristics of fog computing pose many challenges: 1) heterogeneity in terms of the range of devices with varying capabilities, 2) communication in the network may be wired or wireless with varying speeds, 3) mobility of devices, 4) location awareness, 5) geographic distribution of devices, 6) distributed nature of computing, 7) limited capabilities of processing nodes. In addition to the issues inherited from the cloud, the above characteristics of fog bring some more challenges in terms of security, resource management, data and network management, etc.

Security and privacy. Fog computing has created a new dilemma of security and privacy-related issues due to its notable characteristics of distribution, heterogeneity, mobility, and limited resources. As fog devices have limited capabilities, it would be difficult to execute a full suite of security solutions. As fog nodes are near end-users, protection and surveillance are relatively weak and increase the probability of attacks.

In addition, fog will be an attractive target to many attacks due to its ability to obtain sensitive data from both IoT devices and the cloud.

Following are the security and privacy challenges of fog computing and the methods to overcome the threats.

- **Authentication issues:** fog services are offered at a large scale to end-users. Fog services can be from different parties like a cloud service provider, internet service provider and other parties. This flexibility complicates authentication and trust issues. Hence the conventional password-based user authentication may not ensure the identity of users. It is proposed to use biometric smart card user authentication to protect fog environment.
- **Data consistency** in the cloud can be achieved by coordinating with the cloud servers where the cloud is deployed. But it is more complex in a fog environment. Data replication is used to find the best storage locations for data replicas. It is necessary to coordinate with the back-end cloud servers, fog nodes that cached data replicas and client devices to ensure strong

consistency. But this may deteriorate the write performance. Strategies are proposed to select the right number of replicas and locations for faster data access and replica synchronization[19].

- **Forgery:** the attackers imitate their identities to deceive victims by generating fake information. This attack decreases the network performance by consuming energy, storage, and bandwidth due to the fake data packets. Hong *et al.*[20] suggested a privacy-preserving authentication scheme CLAS that provides access control for addressing the forgery attack.
- **Tampering:** the attackers modify, delay, or drop the transmitted data over the network to degrade and disrupt the performance and efficiency of fog computing. Liang *et al.*[21] suggested a reliable trust computing mechanism (RTCM) based on fog computing. The solution aims to provide a high level of integrity for the data in a fog environment.
- **Sybil** uses fake identities to control and compromise fog nodes. It generates fake crowd-sensing reports and can expose the user's personal information. Alwakeel[22] suggested a Sybil attack detection mechanism for the cloud computing environment that also could be used with fog computing.
- **Jamming:** wireless technology was viewed as the main factor responsible for the insecurity of the internet. Sniffing, spoofing, jamming, etc., are said to be the various attacks that could significantly affect fog computing between the fog nodes and the centralized devices. Mukherjee *et al.*[23] proposed data privacy and security through identity obstruction techniques. It was achieved by making fake nodes at various fog connections in conjunction with fake documents to make them look legitimate and implicitly make the unauthorized user download fake documents. An unauthorized user's system is used to locate the Mac address of the system and eventually send the content to the regional cloud to block more requests and to be able to evaluate the location of the authorized user.
- **Denial-of-Service (DoS)** attack floods the fog nodes with many fake requests to make them unavailable for legitimate users. DoS consumes network resources such as bandwidth and battery, decreasing fog performance. Priyadarshini and Barik[24] proposed novel source-based DDoS mitigating schemes that could be employed in both fog and cloud computing scenarios to eliminate these attacks. It deploys the DDoS defender module, which works on a machine learning-based detection method, present at the SDN controller. This scheme uses the network traffic data to analyze, predict, and filter incoming data to send the filtered legitimate packets to the server and block the rest.
- **Collusion:** two or more groups collude together to trick, cheat, or mislead a group of fog nodes or acquire legal advantages. Yaseen *et al.*[25] proposed a model for detecting collusion attacks in IoT environments. The fog-based model can be used for real-time monitoring of possible collusion attacks in IoT environments. Furthermore, the paper added a software-defined system (SDS) layer that offers a high degree of flexibility for configuring fog nodes. This SDS layer can collect different types of data and detect attacks. The proposed model migrates the overhead to fog nodes, which are more powerful and reliable.
- **Man-in-the-middle:** the attacker secretly relays and possibly alters the communications between the nodes without discloser to legitimate users. Aliyu *et al.*[26] investigated the possibility of applying an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for Man in the Middle (MitM) attack using IDS nodes.

Special nodes, known as IDS nodes, were introduced to the system to ensure reduced latency. Each IDS node interrogates fog nodes one-hop away and analyzes their response in terms of content, context, and arrival time.

- **Impersonation:** an attack in which the attacker behaves like a legitimate user or genuine server that offers fake or malicious services to legitimate users. Tu *et al.*[27] proposed an algorithm for impersonation detection. The Q-learning algorithm is used to find the optimal test threshold value in an impersonation attack.

Resource management. Fog nodes like routers access points or edge devices have very limited computational and storage capacity. They can be easily overloaded with a large amount of data produced by IoT. The fog resources can be broadly classified into 1) computation resources like the processors and memory, 2) storage resources like hard drives and flash devices, 3) communication resources like communication links and intermediate devices, and 4) power or energy resources like cooling devices and UPS.

A fog computing platform requires fog servers and data storage facilities near end-users to accelerate the processing. I characterize fog network 1) limited resource capabilities, 2) resource heterogeneity, 3) dynamic nature, and 4) unpredictable fog environment. These characteristics pose challenges in resource management and maintenance. Fog nodes require adequate storage and computational capabilities for completing the tasks. Resource management aims to reduce overall energy consumption, latency, and communication cost. As fog devices are geographically located, it is hard to map user tasks to appropriate nodes with enough resources.

Approaches for resource management include 1) application placement, 2) resource allocation, 3) workload balance, 4) resource provisioning, 5) task scheduling, and 6) quality of service.

4. Resource allocation methodologies

1) Data flow architectures. The classification is made based on the direction of data flow. Major models include a) aggregation, b) sharing, and c) offloading.

2) Control architectures. The classification is based on control modes like centralized and distributed.

3) Tenancy architectures. This classification is based on resource sharing and virtualizations which can be a) discovery based: these algorithms try to find out the complete set of computing resources available in the edge framework. This is done based on the different protocols, including handshaking and messaging protocols. Security concerns of new devices joining the framework is a concern. b) Computing performance benchmark: these algorithms compute performance benchmarks primarily concerning power requirements, CPU and memory performance of edge processors. c) Load balancing: the tasks distributed should be sufficiently load balanced to gain maximum system efficiency. d) Placement based: identification of the appropriate resource for executing a task. Such allocations can be dynamic as well as static.

Resource allocation issues are different in cloud and fog computing environments. Considering service priority and fairness, there is a need to efficiently assign many geographically dispersed heterogeneous fog nodes to compete IoT services with different QoS requirements. There are two approaches to resource allocation—auction-based and optimization. The auction-based resource allocation method is a market-based pricing approach that provides supply and demand fog nodes for bidding and then sells fog nodes to the highest bidders. Both IoT users and fog vendors are working to enhance their utilities through the right resource allocation methods in the market. In the optimization method, the resource allocation is modelled as a double match problem, so the cloud server and fog node are combined for IoT users. The fog node and IoT users are coupled to cloud servers.

Table 2 shows the challenges in resource management and the methods proposed by some researchers to overcome the challenge.

Table 2. Challenges in resource management and the methods to overcome the challenge

Challenges in resource management	Description	Method to overcome the challenge
Resource allocation issues[28]	The resource allocation problem of the fog computing network is formulated as a double matching problem—the cloud server and fog node are combined for the IoT user, and the fog node and the IoT user are combined for the cloud server.	Jia *et al.*[28] proposed the definition of cost efficiency, which can be used in the preference analysis among cloud data centers, fog nodes and users. Then, based on the cost efficiency, a double-matching strategy was developed based on deferred acceptance algorithm (DA-DMS). Using the DA-DMS strategy, the three participants could achieve stable results that each participant cannot change its paired partner unilaterally for more cost-efficiency. Numerical results showed that high cost-efficiency performance could be achieved by adopting the DADMS strategy.
Resource management problem in online fog computing systems[29]	Dynamic, online offloading scheme for delay-sensitive tasks	Alenizi and Rana[29] proposed a dynamic offloading threshold that allows a fog node to adjust its threshold dynamically, combining two efficient and effective algorithms: Dynamic Task Scheduling (DTS) and Dynamic Energy Control (DEC).
Load balancing[30]	Due to high loads and high energy consumption, blocking requests affect the latency.	Da Silva and da Fonseca[30] proposed Gaussian Process Regression for Fog-Cloud Allocation (GPRFCA) mechanism to answer where to run the tasks of an application. The infrastructure considered is composed of a fog layer and the cloud. Users submit requests to the fog nodes, and the workload can be executed in the fog, in the cloud or partially executed in the fog and the cloud. The GPRFCA mechanism decides where to schedule a workload to be processed, considering the resource availability and the latency overhead.
Latency and energy consumption[31]	Improving the performance and decreasing the latency and energy consumption	Mijuskovic *et al.*[31] proposed a feedback-based optimized fuzzy scheduling algorithm. The architecture introduces fuzzy-based scheduling. The client produces the ratings of VMs, and the server produces effective results using the proposed algorithm. The proposed methodology (FOFSA) has been tested with iFogSim. It is compared with the different existing dynamic algorithms and proves that it is an effective scheduling strategy and improves the QoS parameters. It also reduces the power consumption, execution time and improves the makespan of the system.
Resource utilization[32]	Placement of application modules	Taneja and Davy[32] presented a module mapping algorithm for efficiently utilizing resources in the network infrastructure by efficiently deploying application modules in fog-cloud infrastructure for IoT-based applications.
Resource allocation[33]	Intelligent resource allocation in residential buildings	Javaid *et al.*[33] proposed a C2F2C-based framework for intelligent allocation of resources in the residential buildings. This framework is based on three layers where consumers' requests have been considered constant for every hour of a day. Simulation results show that the proposed technique outperformed the prior techniques.

5. Hardware and software issues

5.1 Challenges in implementing fog nodes

Fog computing brings computational facilities very near to cloud users. It effectively reduces the network traffic and the time taken for the users to access the cloud resources. However, introducing a fog layer that consists of an "n" number of fog nodes between the cloud user and the cloud servers' results in various hardware and software challenges. The following subsections explain the hardware requirements for creating a fog node and discuss the hardware and software challenges in detail.

Hardware issues. In 2017, OpenFog Consortium Architecture Working Group released a white-paper titled "OpenFog reference architecture for fog computing", which intends to help the business leaders, system architecture, and software developers to create and maintain the fog nodes between the cloud user and cloud service providers[34]. Also, OpenFog RA elaborates the hardware and software components required to create a cost-effective fog model.

To create an efficient fog layer, OpenFog RA proposes having one or more nodes be coupled with other components. However, while coupling the hardware components together to create a layer fog node, it has to provide robust mechanical support and protection for the internal components of the fog nodes. The fog nodes' computational and storage space are comparatively less than the cloud servers. However, the cloud users expect to get a quick response from the fog nodes as they get the response from the cloud servers. Also, to survive harsh conditions and overloaded requests, the fog hardware should be robust and capable of managing any harsh situation. As per the OpenFog Reference Architecture standards, a few hardware requirements of fog nodes are listed below.

Protection from environmental factors. The prime objective of fog computing is to deploy the computational and storage resources near cloud users. For example, self-driving/autonomous vehicles use fog nodes to make quick decisions. Instead of using the cloud server, self-driving vehicles use fog nodes to reduce communication time. In some situations, considering the fast response, these fog nodes might be placed on any harsh environments, such as roads, railway tracks, underwater, and factory floors. In such conditions, the internal parts of the hardware of the fog nodes have to withstand and work perfectly. The hardware parts have to comply with the international safety and environmental responsibility standards, such as UL, LLC (Underwriters Laboratories – Limited Liability Corporation), CSA (Canadian Standard Association), and Waste Electrical and Electronic Equipment Regulation (WEEE) standards.

According to the international standards, the maximum temperature (heating issues) for the fog nodes is set as follows:

- The temperature of the fog node in commercial applications can range from 0 °C to 70 °C.
- The temperature of the fog nodes used in industrial applications can range from 40 °C to 85 °C.
- The temperature of the fog nodes used in military applications can range from 55 °C to 215 °C.

Also, in some scenarios, the fog nodes can be deployed in a very harsh environment where setting up an air exhaust is impossible. For example, air exhausts are not possible while deploying an underwater fog node. The fog node should maintain the internal temperature even if it doesn't have sufficient air exhausts. To maintain the temperature in the fog nodes, Tuli *et al.*[35] proposed an iThermoFog technique. It uses artificial intelligence (AI) and integrated Internet of Things (IoT) devices to automatically schedule the thermal profile of the fog nodes and cloud data centers (CDC). iThermoFog model uses a gaussian mixture model to derive the thermal characteristics and behaviours of the fog server. It is later used to schedule the tasks to the fog servers. Depending on the fog servers' temperate, the tasks will be assigned. High computationally intensive tasks are assigned to the fog server, with less temperature and vice versa.

Heterogeneous hardware. Most of the large-scale cloud data centers (CDC) and cloud

servers in the world have homogenous hardware setup, i.e. the hardware used to build the cloud setup is of the same type, and they are centrally managed. However, it is not practically possible to have homogenous hardware setups in a hybrid cloud setup.

On the other hand, a new hardware layer is introduced between the cloud users and the cloud servers in fog computing. The fog nodes don't need to have a homogenous hardware setup. The service providers may use hardware that different companies manufacture. An effective fog computing model should work efficiently with heterogeneous hardware setups. Integrating heterogeneous computing resources in the fog node will increase resource efficiency and reduce computational energy usages. However, integrating and maintaining the heterogeneous fog nodes is challenging and still in development. It is strongly believed that adopting heterogeneous servers in fog computing might increase the complexity of maintaining the fog nodes among the research community. Zhang *et al.*[36] proposed a Hetero Fuzz model to detect the heterogeneous hardware platforms' software applications. Also, to reduce the energy consumption of IoT devices and fog nodes, Wu *et al.*[37] proposed an energy-efficient scheduling algorithm using the Integer Linear Programming (ILP) model.

Limited scalability in fog nodes. Cloud computing is profound of unlimited scalability. The cloud data centers are enormously large. However, the fog nodes are comparatively small and have limited resource scalability. The fog framework in the service-oriented applications should support scalability at least inside the fog layers. A fog node should be allowed to access or use the nearby fog node's resources without increasing the security vulnerability. The fog framework should support different network topologies to scale the resources, such as a tree, mesh, and bus topologies. In addition, the framework should also support elasticity, enabling the service provider to extend the network to a new fog or cloud location or to remove a location from the network.

Software issues in fog computing. Introducing a fog layer between the cloud user and the cloud service provider is a novel and most recent computing paradigm. To develop an efficient fog computing-based service-oriented application, the service providers requires a new programming model. Designing effective tools and frameworks for fog computing to build dynamically executable applications on diverse fog platforms is necessary. Some of the software issues that have to be addressed in the fog computing environment are listed below.

Task scheduling in fog nodes. Unlike cloud data centers (CDC), the fog nodes have various challenges like heterogeneity, uncertainty in the resources and limited computational capacities. To overcome these issues and use the resources efficiently and optimally, proper scheduling algorithms are required. Oueis *et al.*[38] proposed a dynamic scheduling algorithm by creating a cluster of fog nodes and balancing the workloads. According to the request raised by the cloud user, the dynamic scheduling algorithm allocates the computation resources and dynamically organizes the clusters and fog nodes to serve upcoming requests. Intharawijitr *et al.*[39] came up with three strategies to minimize the latency and constraints to schedule the user's request to the fog nodes. In the first method, the user's request or tasks are randomly allocated to the nearby fog nodes. In the second method, the user's tasks are allocated to the fog nodes with low latency. In the third method, the tasks are allocated so that the resources in the fog nodes are utilized to the maximum level. Depending on the situation and resource availability, the administrator will choose any task scheduling methods mentioned above.

Migration. Migration is an important service offered by cloud service providers. It allows the data owner and the cloud users to transfer any critical services running on-premises to the cloud servers. Microsoft Azure, Google Cloud and Amazon AWS are the renowned cloud service providers that offer migration support to their users. Machen *et al.*[40] proposed a stateless and stateful migration method for fog environments. In the stateless migration method, the state of the live applications will not be moved. However, the request raised by the cloud users will be redirected to the next new server as a separate instance. On the other hand, in the stateful migration method, the state of the running applica-

tion is stored.

Privacy and security issues. Another important issue in creating a fog layer between the cloud user and the cloud data center is achieving secure and privacy-preserving computation in the fog nodes. It is mandated to achieve data privacy, user privacy and location privacy in fog computing to increase the trust among cloud users.

Data privacy. Data privacy or information privacy protects users' personal and sensitive data from those who don't have access to it. One of the prime objectives of cloud computing is to provide a privacy-preserving computing service to cloud users. However, while introducing fog nodes as a middle layer, the users' sensitive data are hopped between multiple fog nodes and cloud servers. It increases the vulnerability of sensitive data. To avoid these situations, privacy-preserving algorithms have to run and verify the integrity of the data on both fog nodes and the cloud storage. Some of the recent privacy-preserving schemes are listed in **Table 3**.

Table 3. Privacy-preserving schemes

Schemes	System model	Issues dealt	Algorithm used
Hu *et al.*[41]	A face identification and resolution framework for improving security and privacy in fog computing	Confidentiality Integrity Availability Authentication	AES symmetric key encryption SHA-1 algorithm Session key-based authentication mechanism
Koo *et al.*[42]	A data deduplication scheme using dynamic ownership management in fog nodes	Confidentiality Integrity Availability Authentication Storing duplicate data in fog nodes, i.e. data redundancy in fog nodes	Ownership proof using merkle tree User-level key management and update status Forward secrecy
Shynu *et al.*[43]	Secure data deduplication for integrated cloud-edge environment	Confidentiality Authentication Storing duplicate data in fog and edge nodes	Convergent key encryption Modified elliptic curve cryptography (MECC) algorithms SHA-512 hashing technique
Du *et al.*[44]	Renewable fog nodes and differential privacy query mode	Confidentiality Integrity Availability	Renewable fog nodes Differential privacy based query model Improved QMA model
Huang *et al.*[45]	Location-based fog computing	Location privacy identification issues Identify privacy authenticity	Location-based encryption (LBE) scheme SHA-1 algorithm Cryptographic puzzle
Yi *et al.*[46]	Fog computing environment with four entities, such as owner, cloud provider, fog node, and many users.	Keyword privacy Data confidentiality Trapdoor unlinkability	Online ABE techniques Secure index generation Searchable encryption

User Privacy. Ensuring user privacy in fog computing is another important challenge for service providers. Most IoT devices and applications that require low latency results use fog services. When IoT devices use fog resources as processing units, there is a high possibility of user privacy leakage. The fog node maintained by the third-party entities may continuously monitor the user's practice. For example, IoMT (Internet of Medical Things) used in hospitals may disclose various patient information and health conditions. Most IoMT devices use fog services to have a low latency result. However, some

third-party entities might manage these fog nodes, and they can misuse the information. Also, fog nodes are vulnerable against the man in the middle attack and may easily disclose user privacy[47]. For example, the malicious IoT data that enters the fog node can stay and analyze sensitive information generated by the other IoT devices. Malicious nodes can steal private information such as address location, and trajectories.

Location privacy. Another important issue to be addressed in the fog computing environment is location privacy leakage. An IoT device or the application that uses fog computing always communicates to its nearby fog node. Chiang[48] highlights the issues with location privacy in the fog environment and lists the challenges in achieving location privacy. Also, Kang *et al.*[49] provide secure communication and privacy preservation for an autonomous vehicle in fog computing. It aims to address the location privacy issues in the IoT.

5.2 Artificial intelligence techniques in fog layers

Artificial intelligence is a proven technology to solve complex problems, automate the process and decisions making. These are the key feature requirement in cloud environment. The cloud stack consists of the cloud plane and fog plane in the cloud architecture. The computing takes place in cloud or fog layers. Fog layers' responsibility is to acquire real-time data from sensors. Virtual sensors discover knowledge from the environment using agent concepts. Data science concepts are used for the analysis of data, reduction of data, data visualization, filtering, classification of data. Patter mining is some of the operations that occur in the fog layer[50].

Physical layer/end device layer. Input for cloud computing can be from IoT devices to read real-time data. Data is collected through embedded systems, virtual sensors, user interfaces, and edge devices. Bio-sensors input, environment monitoring sensors, and smart devices are terminal or virtual devices for computing input in AI fog plane, as shown in **Figure 3.**

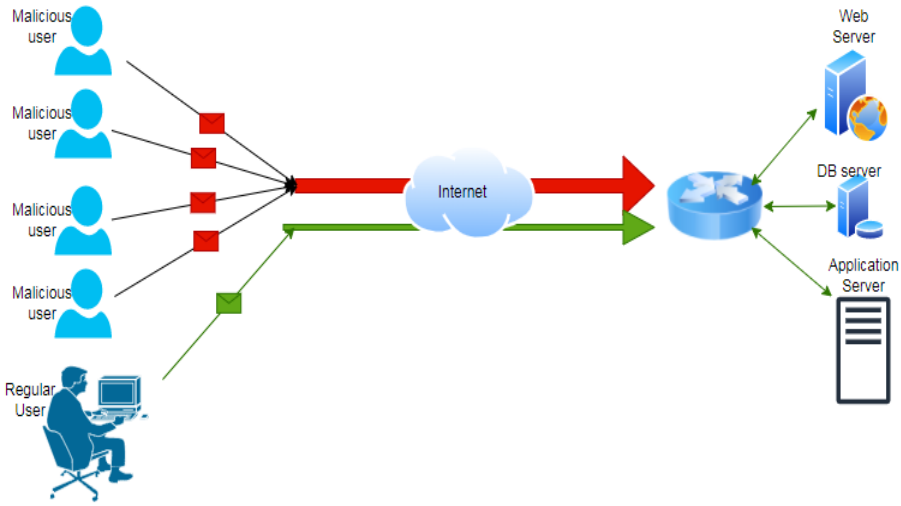

Figure 3. Communication over internet among maliciouse and regular users.

Fog communications. There are different types. Fog-to-cloud communication, fog-to-fog communication, and fog-to-things are the three communication processes, and the exchange of data occurs. The fog-to-cloud service communication will exchange service among cloud and fog. The cloud environment manages it. Cloud can talk to IoT devices through the fog-to-cloud/cloud-to-fog exchange information in the form of end-to-end service. Multiple clouds are established when we have huge cloud services. Multiple fog patches are built for storage services, multiple users, applications, and computation jobs, then fog-to-fog communication. The overall communication model is shown in

Figure 4[51].

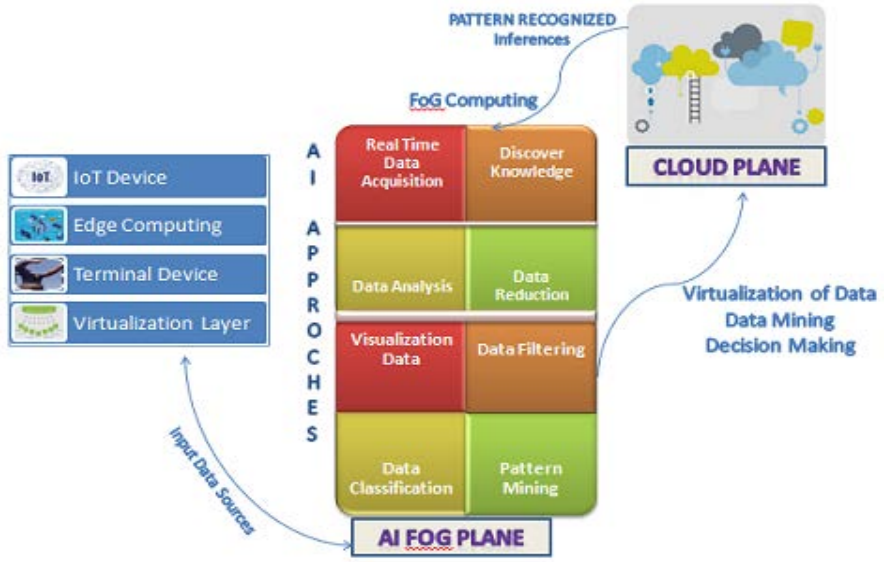

Figure 4. Artificial intelligent in fog layer over the cloud environment.

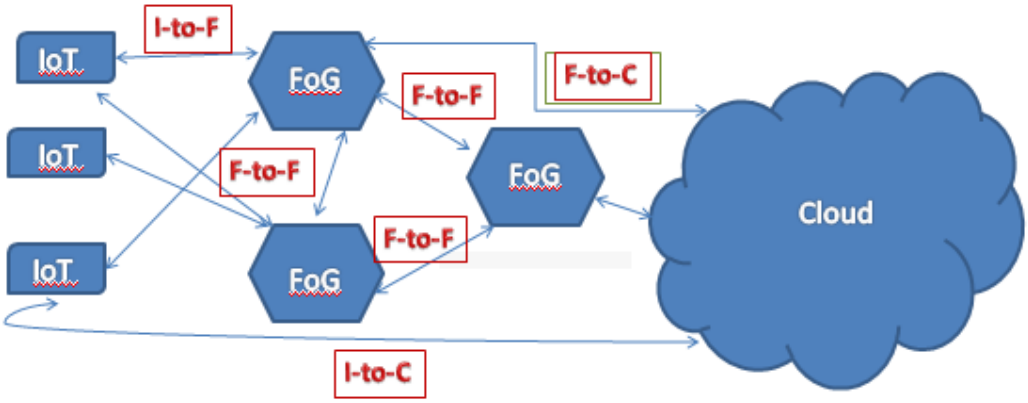

Figure 5. Different types of communication path among IoT devices, fog and cloud.

AI in fog plane. Data is collected from different fog input sources. The basic application analysis occurs on the fog plane, and results are updated to the cloud. The key advantages are that cloud switching will be no time, cloud traffic congestion can be reduced, security can be maintained locally, and local computation tasks can be performed in less time. The drawback in fog computing is that aggregated values are maintained over the cloud. The identical content is maintained on the fog plane. The real-time data is stored on the fog storage device and analyzed to obtain the patterns. The artificial intelligent concepts are applied to real-time data. The telehealth, IoT devices requirement for home need analysis, connected automated car, smart grids layout, smart traffic signals, automated train, wireless sensor and actuator networks, decentralized smart building, health care system, software networks, IoT &cyber systems and mobile computing system are the applications of the real-time fog computing.

Real-time data acquisition system and data reduction. The data from different input devices are analyzed and compressed using different algorithms for various applications. The sample applications are summarized in **Table 4**, along with the results.

Table 4. Real-time data in acquiring and compression algorithm

Real-time data acquiring for different applications using artificial intelligence					
Author details	**Application/industry**	**Input source**	**AI concepts**	**Algorithm**	**Results**
Dubey *et al.*[52]	Telehealth	Wearable sensors	Data analytics and data mining (Feature extractions) Data security	Dynamic time warping, clinical speech processing chain, compression	CLIP has 99% lossless compression. DWCP has 98% lossless compression
Singh[53]	Household energy management	Smart meters	Pre-processing, pattern mining and classification	FP—growth and Apriori algorithm. Cluster the time-stamps	Requirements are identified to execute project
Gia *et al.*[54]	IoT healthcare monitoring	Wearable medical sensors	ECG feature extraction	Wavelet transformation and threshold estimation	93% data reduction, efficiency in bandwidth and low latency
Lynn *et al.*[55]	Modern machine tools	MT connect adapter	Convert data into the frequency domain	Data preprocessing and fast Fourier transform	Manufacturing frequency data analysis for accuracy

Data Classification in fog plan. The AI, data classification methods, are used in the fog layer for security threat classification, fog route mapping and real-time traffic management, and applying deep learning concepts to provide security in 5G network. The summary of the classification algorithms used in the fog plan is shown in **Table 5**.

Table 5. Data analytics in fog plane for classification algorithm

AI classification used in fog plane					
Author details	**Application/industry**	**Input source**	**AI concepts**	**Algorithm**	**Results**
Wang *et al.*[56]	Fog plan Cloud plan Edge plan	Audio Video Text	Tensor-based big-data-driven routing	Cluster-based routing method Location-based routing method Flat routing method Tensor-based routing method	Tensor-based routing recommendation approach
Gao *et al.*[57]	Mobile–fog–cloud structure	Video/live streaming and ads dissemination	Software-defined network and delay-tolerable network (DTN)	Hybrid data dissemination framework	Success ratio depends on delay rate
Ahanger *et al.*[58]	Medical health data classification	Health sensors collect patients health condition	Data classification	Fuzzy c-means algorithm	Data of subjects can be infected or not based on the class type of health data, location data, environment data and metrological data

Pattern mining of data in fog plan. The data captured on the fog plan are analyzed using various AI concepts to know the similarity among the data available on the storage system captured through IoT devices. The summary of patter mining concepts used for various applications is shown in **Table 6**.

Table 6. Data clustering using pattern mining in fog plane

AI pattern mining used in fog plane					
Author details	**Application/industry**	**Input source**	**AI concepts**	**Algorithm**	**Results**
Barik *et al.*[59]	Cloud geographic information systems	Vector data Graph data Roaster data	Pattern mining	FogGIS framework	Intelligence in a geospatial cloud environment
Dhande[60]	Health dept	Healthcare input	Data mining	Enhanced data mining dynamic replication	Reduction of latency Response time reduced Utility of storage Usage of network
Pérez *et al.*[61]	Traffic forecasting application	Data distribution algorithm & traffic modeling approach	Deep learning and machine learning	Conditional restricted boltzmann machines	Results show that data performance is more efficient in fog than in cloud

Artificial intelligence using reinforcement learning in fog. The machine learning concepts are used in application development in predicting the next or future values. The prediction is based on the previous information lined up on the earlier values. There are three types of learning. Supervised learning is to classify the data based on the defined classes. Unsupervised learning is to classify the data based on the undefined classes. Finally, reinforcement learning is dynamic learning. The actions are taken based on the live environment. Decisions and protocols may change as per time. The real-time applications for reinforcement learning are self driving cars, automated industry, finance and trading, NLP learning, healthcare systems, recommendations of news, and real time advertising. Bidding is an example.

Table 7. Reinforcement learning in fog plane

Author details	**Application/industry**	**Input source**	**AI concepts**	**Algorithm**	**Results**
Ning *et al.*[62]	Vehicles communication using cloud	Fog input nodes	Internet of vehicles	Deep reinforcement learning in offloading redirection	Energy requirement has decreased by 60%
Pandit *et al.*[63]	Task scheduling	IoT sensors	Reinforcement learning	Neural network in fog environment	Reduces the cost of communication
Sami and Mourad[64]	Service placement	IoT input devices	Deep learning and intelligent fog and service placement	Markova decision process	Improve the quality of service

Empowering IoT through AI in fog plan. The Internet of Things is the programmable device used to capture the input data through sensors, physical equipment, and human wearable devices. The devices are programmed with artificial intelligent concepts like searching, planning, robotics, and NLP, and computer vision concepts are used to develop software in the system[65]. The face detection and recognition application can use the CNN algorithm for an intelligent decision. The self-driving robot car uses CNN, SVM, and DNN AI algorithms used at the edge cloud computing devices. The 3D hand gestures recognition applications use the CNN AI algorithm, and image recognition or hand motor

devices[66]. The F-RAN (Fog radio access network) has been developed to work with different IoT devices. The input type of data may be text, audio, video, images, etc., for higher bandwidth and low latency[67]. The artificial intelligence concept helps to bridge the gap between the fog layer and edge devices to improve the efficiency and performance of the cloud computing concepts through the fog layer.

6. Applications of fog computing

Key characteristics of fog computing like low latency, scalability supported by distributed computing, and resource utilization, bring many applications in various domains.

- Autonomous vehicles: self-driving vehicles produce a large amount of data to be processed and interpreted quickly based on traffic, presence of objects, driving conditions, and climate.
- Smart grids: data in the power distribution network is generated from many sensors. The remote data produced can be collected and processed in nearby fog nodes and then sent the filtered data to data centers for long storage. Energy networks use real-time data for the efficient management of systems. Service providers and consumers can monitor the data to control production, pricing, and consumption.
- Smart buildings: commercial buildings are equipped with various sensors. Fog nodes analyze this data to monitor the building operations like parking space occupancy, and emergency alarms.
- Real-time analytics: to detect irregularities in public places like parking, malls require real-time monitoring with strict low latency to ensure safety and security. Surveillance systems require low latency services. Surveillance cameras can be processed in fog nodes to detect irregularities immediately.
- Augmented reality requires low latency and high information handling rate. A small delay in response damages user experience and content on the screen. This requires computer vision algorithms to process real-time video frames.
- Cyber-physical systems consist of objects and processes to perform computations, communications and control systems. The devices sense, collect, send, and receive data that describe the system operations. The data is analyzed at fog nodes to make useful predictions.
- Smart transport: on the internet of vehicles, each vehicle produces data like its speed and direction. This data is transmitted to other vehicles for smooth movement of traffic.
- Agriculture and farming: precision agriculture uses sensors to monitor parameters like temperature, soil moisture, pests, and crop yield. This data can be analyzed locally in fog devices to give quick inputs to farmers to regulate water flow, control diseases and estimate crop yield.
- Health care systems: smart healthcare systems use IoT devices that produce large and complex data. Fog computing can address the issues of latency, real-time response delays, emergency medical services. Dastjerdi *et al.*[68] proposed FAST—a fog computing-based fall detection algorithm for stroke mitigation.
- Caching: social network websites have a large volume of data to be processed. Such websites performance can be improved using network edge-specific knowledge to reduce time and space[69].
- Gaming applications are complex and rely on real-time processing. Fog computing is more appropriate for such applications.
- Traffic control systems: with the increase in vehicles, an effective traffic system is necessary for cities characterized by heavy traffic and traffic congestion. A fog computing platform can acquire, analyze and process local traffic data at traffic junctions.
- Video streaming systems: large quantity of

internet usage is due to video streaming. It demands greater bandwidth and low response time. Fog computing can provide real-time communications and low latencies. Chen *et al.*[70] provided a fog architecture that provides low latencies with the good video quality.

- Linked vehicles: vehicular applications are compute-intensive and latency-sensitive. Computational resources of connected vehicles can act as fog nodes to address the latency constraints of the cloud and reduce traffic directed to the cloud.
- Surveillance: surveillance systems in public places operate 24/7, producing a large amount of data. Incidents concerning the safety and security of the public require faster data processing and quick responses. Fog-based surveillance systems can enable faster processing by localizing the data. Jain *et al.*[71] compared latency times of different scenarios.

6.1 Potentials that provide opportunities for fog computing

The major five potentials of fog computing will show the importance of why fog computing will act as an extension of cloud computing. The classification is showed in **Figure 6**.

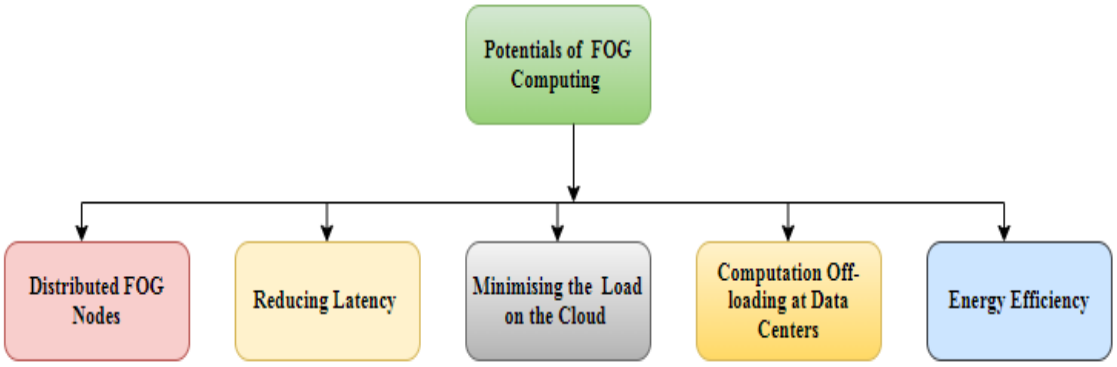

Figure 6. Classification of potentials of fog computing.

Distributed fog nodes. The fog nodes are distributed along the geographical distribution and provide mobility because the fog nodes have more proximity to the end users when compared with cloud computing.

Reducing latency. As the fog nodes are placed near the end users, these fog nodes will oppose the data transfer to the cloud and cloud to the end user node. This scenario will minimize the latency because the query generated by the end user will be answered by the fog node, not by the cloud server.

Minimizing the load on the cloud. The data generated by the IoT devices will be huge and continuous, which has to be processed by the cloud server. In this situation, the fog nodes will filter the unwanted and repeated data generated by the IoT devices; then it will be transferred to the cloud.

Computational off-loading at data centers. Social networks are generating an enormous amount of data every day. Youtube.com generates 72 hours of video data per minute, and Twitter.com generates 350,000 tweets per minute. If all these data are transferred to the cloud directly, it may cause bandwidth issues. However, introducing fog nodes between the cloud and the client devices reduces the bandwidth requirement.

Conflict of interest

The authors declared no conflict of interest.

References

1. Saharan KP, Kumar A. Fog in comparison to cloud: A survey. International Journal of Computer Applications 2015; 122(3): 10-12.
2. Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. In:

MCC '12: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing; 2012 Aug 17; Helsinki, Finland. New York: Association for Computing Machinery; 2012. p. 13-16. doi: 10.1145/2342509.2342513.

3. Hao X, Yeoh PL, Ji Z, *et al.* Stochastic analysis of double blockchain architecture in IoT communication networks. IEEE Internet of Things Journal 2022; 9(12): 9700-9711. doi: 10.1109/JIOT.2022.3142761.
4. Macedo ELC, Delicato FC, de Moraes LFM, Fortino G. Assigning trust to devices in the context of consumer IoT applications. IEEE Consumer Electronics Magazine 2022. doi: 10.1109/MCE.2022.3154357.
5. Abid MA, Afaqui N, Khan MA, *et al.* Evolution towards smart and software-defined Internet of Things. AI 2022; 3(1): 100-123. doi: 10.3390/ai3010007.
6. Chavhan S, Gupta D, Gochhayat SP, *et al.* Edge computing AI-IoT integrated energy efficient intelligent transportation system for smart cities. ACM Transactions on Internet Technology (TOIT) 2022; 22(4): 1-18. doi: 10.1145/3507906.
7. Ali O, Ishak MK, Bhatti MKL, *et al.* A comprehensive review of internet of things: Technology stack, middlewares, and fog/edge computing interface. Sensors 2022; 22(3): 995. doi: 10.3390/s22030995.
8. Talaat FM. Effective prediction and resource allocation method (EPRAM) in fog computing environment for smart healthcare system. Multimedia Tools and Applications 2022; 81: 8235-8258. doi: 10.1007/s11042-022-12223-5.
9. Farooqi AM, Alam MA, Hassan SI, Idrees SM. A fog computing model for VANET to reduce latency and delay using 5G network in smart city transportation. Applied Sciences 2022; 12(4): 2083. doi: 10.3390/app12042083.
10. Gardasu AK, Kotha RK. A fog computing solution for advanced security, storage techniques for platform infrastructure. EasyChair Prepring No. 7460. 2022.
11. Sun L, Xue G, Yu R. TAFS: A truthful auction for IoT application offloading in fog computing networks. IEEE Internet of Things Journal 2022; 10(4): 3252-3263. doi: 10.1109/JIOT.2022.3143101.
12. Almiani M, Razaque A, Alotaibi B, *et al.* An efficient data-balancing cyber-physical system paradigm for quality-of-service (QoS) provision over fog computing. Applied Sciences 2022; 12(1): 246. doi: 10.3390/app12010246.
13. Verma P, Tiwari R, Hong WC, *et al.* FETCH: A deep learning-based fog computing and IoT integrated environment for healthcare monitoring and diagnosis. IEEE Access 2022: 10: 12548-12563. doi: 10.1109/ACCESS.2022.3143793.
14. Laghari AA, He H, Halepoto IA, *et al.* Analysis of quality of experience frameworks for cloud computing. IJCSNS 2017: 17(12): 228-233.
15. Dubey H, Yang J, Constant N, *et al.* Fog data: Enhancing telehealth big data through fog computing. In: Proceedings of the ASE BigData & SocialInformatics; 2015 Oct 7-10; Kaohsiung Taiwan. New York: Association for Computing Machinery; 2015. p. 1-6. doi: 10.1145/2818869.2818889.
16. Kocabas O, Soyata T, Couderc JP, *et al.* Assessment of cloud-based health monitoring using homomorphic encryption. 2013 IEEE 31st International Conference on Computer Design (ICCD); 2013 Oct 6-9; Asheville, NC, USA. New York: IEEE; 2013. p. 443-446. doi: 10.1109/ICCD.2013.6657078.
17. Wang Q, Guo S, Wang Y, Yang Y. Incentive mechanism for edge cloud profit maximization in mobile edge computing. ICC 2019-2019 IEEE International Conference on Communications (ICC); 2019 May 20-24; Shanghai, China. New York: IEEE; 2019. p. 1-6. doi: 10.1109/ICC.2019.8761241.
18. Boyd S, Parikh N, Chu E, *et al.* Distributed optimization and statistical learning via the alternating direction method of multipliers. Foundations and Trends® in Machine learning 2011; 3(1): 1-122. doi: 10.1561/2200000016.
19. Wang L, An H, Chang Z. Security enhancement on a lightweight authentication scheme with anonymity fog computing architecture. IEEE Access 2000; 8: 97267-97278. doi: 10.1109/ACCESS.2020.2996264.
20. Hong J, Xue K, Li W. Comments on "DAC-MACS: Effective data access control for multiauthority cloud storage systems"/security analysis of attribute revocation in multiauthority data access control for cloud storage systems. IEEE Transactions on In-

formation Forensics and Security 2015; 10(6): 1315-1317. doi: 10.1109/TIFS.2015.2407327.

21. Liang J, Zhang M, Leung VC. A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud. IEEE Internet of Things Journal 2020: 7(6): 5481-5490. doi: 10.1109/JIOT.2020.2981005.
22. Alwakeel AM. An overview of fog computing and edge computing security and privacy issues. Sensors 2021: 21(24): 8226. doi: 10.3390/s21248226.
23. Mukherjee M, Matam R, Shu L, *et al.* Security and privacy in fog computing: Challenges. IEEE Access 2017: 5: 19293-19304. doi: 10.1109/ACCESS.2017.2749422.
24. Priyadarshini R, Barik RK. A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences 2022; 34(3): 825-831. doi: 10.1016/j.jksuci.2019.04.010.
25. Yaseen Q, Jararweh Y, Al-Ayyoub M, AlDwairi M. Collusion attacks in Internet of Things: Detection and mitigation using a fog based model. 2017 IEEE Sensors Applications Symposium (SAS); 2017 Mar 13-15; Glassboro, NJ, USA. New York: IEEE; 2017. p. 1-5. doi: 10.1109/SAS.2017.7894031.
26. Aliyu F, Sheltami T, Shakshuki EM. A detection and prevention technique for man in the middle attack in fog computing. Procedia Computer Science 2018: 141: 24-31. doi: 10.1016/j.procs.2018.10.125.
27. Tu S, Waqas M, Rehman SU, *et al.* Security in fog computing: A novel technique to tackle an impersonation attack. IEEE Access 2018; 6: 74993-75001. doi: 10.1109/ACCESS.2018.2884672.
28. Jia B, Hu H, Zeng Y, *et al.* Double-matching resource allocation strategy in fog computing networks based on cost efficiency. Journal of Communications and Networks 2018; 20(3): 237-246. doi: 10.1109/JCN.2018.000036.
29. Alenizi F, Rana O. Minimising delay and energy in online dynamic fog systems. arXiv preprint arXiv:2012.12745. 2020. doi: 10.48550/arXiv.2012.12745.
30. da Silva RA, da Fonseca NL. Resource allocation mechanism for a fog-cloud infrastructure. 2018 IEEE International Conference on Communications (ICC); 2018 May 20-24; Kansas City, MO, USA. New York: IEEE; 2018. p. 1-6.
31. Mijuskovic A, Chiumento A, Bemthuis R, *et al.* Resource management techniques for cloud/fog and edge computing: An evaluation framework and classification. Sensors 2021; 21(5): 1832. doi: 10.3390/s21051832.
32. Taneja M, Davy A. Resource aware placement of IoT application modules in Fog-Cloud Computing Paradigm. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM); 2017 May 8-12; Lisbon, Portugal. New York: IEEE; 2017. p. 1222-1228. doi: 10.23919/INM.2017.7987464.
33. Javaid S, Javaid N, Saba T, *et al.* Intelligent resource allocation in residential buildings using consumer to fog to cloud based framework. Energies 2019; 12(5): 815. doi: 10.3390/en12050815.
34. OpenFog Consortium Architecture Working Group. OpenFog reference architecture for fog computing. OPFRA001.020817. OpenFog Consortium Architecture Working Group; 2017.
35. Tuli S, Gill SS, Casale G, Jennings NR. iThermoFog: IoT-Fog based automatic thermal profile creation for cloud data centers using artificial intelligence techniques. Internet Technology Letters 2020; 3(5): e198. doi: 10.1002/itl2.198.
36. Zhang Q, Wang J, Kim M. Heterofuzz: Fuzz testing to detect platform dependent divergence for heterogeneous applications. In: Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering; 2021 Aug 23-28; Athens Greece. New York, United States: Association for Computing Machinery; 2021. p. 242-254. doi: 10.1145/3468264.3468610.
37. Wu HY, Lee CR. Energy efficient scheduling for heterogeneous fog computing architectures. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC); 2018 Jul 23-27; Tokyo, Japan. New York: IEEE; 2018. p. 555-560. doi: 10.1109/COMPSAC.2018.00085.
38. Oueis J, Strinati EC, Barbarossa S. The fog balancing: Load distribution for small cell cloud computing. 2015 IEEE 81st Vehicular Technology Con-

ference (VTC spring); 2015 May 11-14; Glasgow, UK. New York: IEEE; 2021. p. 1-6. doi: 10.1109/VTCSpring.2015.7146129.

39. Intharawijitr K, Iida K, Koga H. Analysis of fog model considering computing and communication latency in 5G cellular networks. 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops); 2016 Mar 14-18; Sydney, NSW, Australia. New York: IEEE; 2016. p. 1-4. doi: 10.1109/PERCOMW.2016.7457059.
40. Machen A, Wang S, Leung KK, *et al.* Live service migration in mobile edge clouds. IEEE Wireless Communications 2017; 25(1): 140-147. doi: 10.1109/MWC.2017.1700011.
41. Hu P, Ning H, Qiu T, *et al.* Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet of Things Journal 2017; 4(5): 1143-1155. doi: 10.1109/JIOT.2017.2659783.
42. Koo D, Hur J. Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing. Future Generation Computer Systems 2018; 78: 739-752. doi: 10.1016/j.future.2017.01.024.
43. Shynu PG, Nadesh RK, Menon VG, *et al.* A secure data deduplication system for integrated cloud-edge networks. Journal of Cloud Computing 2020; 9(1): 1-12. doi: 10.1186/s13677-020-00214-6.
44. Du M, Wang K, Liu X, *et al.* A differential privacy-based query model for sustainable fog data centers. IEEE Transactions on Sustainable Computing 2017; 4(2): 145-155. doi: 10.1109/TSUSC.2017.2715038.
45. Huang C, Lu R, Zhu H, *et al.* EPPD: Efficient and privacy-preserving proximity testing with differential privacy techniques. 2016 IEEE International Conference on Communications (ICC); 2016 May 22-27; Kuala Lumpur, Malaysia. New York: IEEE; 2016. p. 1-6. doi: 10.1109/ICC.2016.7511194.
46. Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: A survey. In: Xu K, Zhu H (editors). Wireless algorithms, systems, and applications. International Conference on Wireless Algorithms, Systems, and Applications; 2015 Aug 10-12; Qufu, China. Cham: Springer; 2015. p. 685-695. doi: 10.1007/978-3-319-21837-3_67.
47. Hatzivasilis G, Soultatos O, Ioannidis S, *et al.* Review of security and privacy for the Internet of Medical Things (IoMT). 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS); 2019 May 29-31; Santorini, Greece. New York: IEEE; 2019. p. 457-464. doi: 10.1109/DCOSS.2019.00091.
48. Chiang M. Fog networking: An overview on research opportunities. arXiv preprint arXiv:1601.00835. 2016. doi: 10.48550/arXiv.1601.00835.
49. Kang J, Yu R, Huang X, Zhang Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Transactions on Intelligent Transportation Systems 2017; 19(8): 2627-2637. doi: 10.1109/TITS.2017.2764095.
50. Margariti SV, Dimakopoulos VV, Tsoumanis G. Modeling and simulation tools for fog computing—A comprehensive survey from a cost perspective. Future Internet 2020; 12(5): 89. doi: 10.3390/fi12050089.
51. Shi W, Cao J, Zhang Q, *et al.* Edge computing: Vision and challenges. IEEE Internet of Things Journal 2016; 3(5): 637-646. doi: 10.1109/JIOT.2016.2579198.
52. Dubey H, Yang J, Constant N, *et al.* Fog data: Enhancing telehealth big data through fog computing. In: Proceedings of the ASE BigData & SocialInformatics; 2015 Oct 7-9; Kaohsiung Taiwan. New York: Association for Computing Machinery; 2015. p. 1-6. doi: 10.1145/2818869.2818889.
53. Singh S. Smart meters big data: Behavioral analytics via incremental data mining and visualization [PhD thesis]. Ottawa: University of Ottawa; 2016.
54. Gia TN, Jiang M, Rahmani AM, *et al.* Fog computing in healthcare internet of things: A case study on ecg feature extraction. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; 2015 Oct 26-28; Liverpool, UK. New York: IEEE; 2015. p. 356-363. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.51.

55. Lynn R, Wescoat E, Han D, Kurfess T. Embedded fog computing for high-frequency MTConnect data analytics. Manufacturing Letters 2018; 15: 135-138. doi: 10.1016/j.mfglet.2017.11.002.
56. Wang X, Yang LT, Kuang L, *et al.* A tensor-based big-data-driven routing recommendation approach for heterogeneous networks. IEEE Network 2019; 33(1): 64-69. doi: 10.1109/MNET.2018.1800192.
57. Gao L, Luan TH, Yu S, *et al.* FogRoute: DTN-based data dissemination model in fog computing. IEEE Internet of Things Journal 2016; 4(1): 225-235. doi: 10.1109/JIOT.2016.2645559.
58. Ahanger TA, Tariq U, Nusir M, *et al.* A novel IoT–fog–cloud-based healthcare system for monitoring and predicting COVID-19 outspread. The Journal of Supercomputing 2022; 78(2): 1783-1806. doi: 10.1007/s11227-021-03935-w.
59. Barik RK, Dubey H, Samaddar AB, *et al.* FogGIS: Fog Computing for geospatial big data analytics. 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON); 2016 Dec 9-11; Varanasi, India. New York: IEEE; 2017. p. 613-618. doi: 10.1109/UPCON.2016.7894725.
60. Dhande R. Dynamic replica management in fog-enabled IoT using enhanced data mining technique [Master's thesis]. Dublin: National College of Ireland; 2020.
61. Pérez JL, Gutierrez-Torre A, Berral JL, Carrera D. A resilient and distributed near real-time traffic forecasting application for Fog computing environments. Future Generation Computer Systems 2018; 87: 198-212. doi: 10.1016/j.future.2018.05.013.
62. Ning Z, Dong P, Wang X, *et al.* Deep reinforcement learning for intelligent internet of vehicles: An energy-efficient computational offloading scheme. IEEE Transactions on Cognitive Communications and Networking 2019; 5(4): 1060-1072. doi: 10.1109/TCCN.2019.2930521.
63. Pandit MK, Mir RN, Chishti MA. Adaptive task scheduling in IoT using reinforcement learning. International Journal of Intelligent Computing and Cybernetics 2020; 13(3): 261-282. doi: 10.1108/IJICC-03-2020-0021.
64. Sami H, Mourad A. Dynamic on-demand fog formation offering on-the-fly IoT service deployment. IEEE Transactions on Network and Service Management 2020; 17(2): 1026-1039. doi: 10.1109/TNSM.2019.2963643.
65. Wilkes MV. Artificial intelligence as the year 2000 approaches. Communications of the ACM 1992; 35(8): 17-23.
66. Zou Z, Jin Y, Nevalainen P, *et al.* Edge and fog computing enabled AI for IoT-an overview. 2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS); 2019 Mar 18-20; Hsinchu, Taiwan. New York: IEEE; 2019. p. 51-56. doi: 10.1109/AICAS.2019.8771621.
67. Ji W, Liang B, Wang Y, *et al.* Crowd V-IoE: Visual internet of everything architecture in ai-driven fog computing. IEEE Wireless Communications 2020; 27(2): 51-57. doi: 10.1109/MWC.001.1900349.
68. Dastjerdi AV, Gupta H, Calheiros RN, *et al.* Fog computing: Principles, architectures, and applications. Internet of Things 2016; 61-75. doi: 10.1016/B978-0-12-805395-9.00004-6.
69. Cheng X, Dale C, Liu J. Statistics and social network of youtube videos. 2008 16th International Workshop on Quality of Service; 2008 Jun 2-4; Enschede, Netherlands. New York: IEEE; 2008. p. 229-238. doi: 10.1109/IWQOS.2008.32.
70. Chen N, Chen Y, You Y, *et al.* Dynamic urban surveillance video stream processing using fog computing. 2016 IEEE Second International Conference on Multimedia Big Data (BigMM); 2016 Apr 20-22; Taipei, Taiwan. New York: IEEE; 2016. p. 105-112. doi: 10.1109/BigMM.2016.53.
71. Jain S, Gupta S, Sreelakshmi KK, Rodrigues JJ. Fog computing in enabling 5G-driven emerging technologies for development of sustainable smart city infrastructures. Cluster Computing 2022; 25: 1111-1154. doi: 10.1007/s10586-021-03496-w.