Hindawi
Security and Communication Networks
Volume 2020, Article ID 8849181, 15 pages
https://doi.org/10.1155/2020/8849181

Review Article

A Review of Techniques and Methods for IoT Applications in Collaborative Cloud-Fog Environment

Jielin Jiang, [1,2] **Zheng Li**, [1,2] **Yuan Tian**, [3] **and Najla Al-Nabhan** [4]

[1] *School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China*
[2] *Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science and Technology, Nanjing, China*
[3] *Nanjing Institute of Technology, Nanjing, China*
[4] *Department of Computer Science, King Saud University, Riyadh, Saudi Arabia*

Correspondence should be addressed to Zheng Li; lizheng@nuist.edu.cn

Received 5 August 2020; Revised 17 August 2020; Accepted 28 August 2020; Published 7 September 2020

Academic Editor: Dou Wanchun

Cloud computing is widely used for its powerful and accessible computing and storage capacity. However, with the development trend of Internet of Things (IoTs), the distance between cloud and terminal devices can no longer meet the new requirements of low latency and real-time interaction of IoTs. Fog has been proposed as a complement to the cloud which moves servers to the edge of the network, making it possible to process service requests of terminal devices locally. Despite the fact that fog computing solves many obstacles for the development of IoT, there are still many problems to be solved for its immature technology. In this paper, the concepts and characteristics of cloud and fog computing are introduced, followed by the comparison and collaboration between them. We summarize main challenges IoT faces in new application requirements (e.g., low latency, network bandwidth constraints, resource constraints of devices, stability of service, and security) and analyze fog-based solutions. The remaining challenges and research directions of fog after integrating into IoT system are discussed. In addition, the key role that fog computing based on 5G may play in the field of intelligent driving and tactile robots is prospected.

1. Introduction

Over the years, with the rapid development of distributed computing, parallel computing, grid computing, network storage, and virtual machine technique, computing resources have become more abundant, cheaper, and more accessible than ever before. The development of the Information Technology (IT) industry and the influx of electronic devices into the market have increased the demand for computing and storage resources. In this context, a new computing mode called cloud computing was proposed. In this mode, resources (such as networks, computing, storage, and applications) are provided to users to access on demand at any time. Service providers are divided into infrastructure providers that manage cloud platforms and lease resources based on pricing models and service providers that rent resources from infrastructure providers to provide services to users. Because of the maturity of cloud computing technology and its advantages such as low cost, easy access to information, rapid deployment, data backup, and automatic software integration [1, 2], cloud has been widely used.

However, in the trend of Internet of everything, the application demand of low latency and high interactivity makes the remote connection between cloud and user devices become the key factor restricting the development. At the same time, the number and types of IoT devices (such as smart headsets, mobile computers, smart home appliances, on-board networking systems, smart traffic control lights, and more connected utilities) are rapidly increasing [3]. Large-scale data transmission poses great challenges to the performance of user devices and the existing network bandwidth. In addition, the security and privacy of personal and enterprise data are questioned, because data are stored centrally in cloud servers far away from users and they cannot determine whether their data is stolen by malicious actors with interest.

Fog computing is a new computing paradigm proposed to solve these challenges. Different from centralized servers in cloud, servers in fog are moved to the edge of the network, known as fog nodes. Some delay-sensitive tasks can be processed on these nodes [4], while some computation-intensive or delay-tolerant tasks are still processed in the cloud. Therefore, the user task request will not be sent directly to the remote cloud. Instead, it is received and processed by the neighboring fog nodes [5], which requires lower network bandwidth and user equipment performance than the former. In addition, fog computing also has some other advantages like stable service, high security, and privacy.

However, the practical technology of fog computing is not mature, and some problems that fog computing faces after being integrated into IoT system still need to be solved, such as heterogeneity, mobility, data and equipment management, QoS management, security, and privacy.

The article can be described as follows. Based on the introduction of the concepts and characteristics of cloud and fog computing in Section 2, the comparison and collaboration between them are presented in Section 3, while the methods and techniques of task offloading among cloud and fog are emphatically reviewed and analyzed. Challenges that IoT face (e.g., low latency, network bandwidth constraints, resource constraints of devices, stability of service, and security) are discussed in Section 4, which are linked to surveys about fog's contribution to addressing these challenges and some specific solutions that have been proposed. Particularly, methods and technologies to reduce delays and protect security and privacy are scrutinized. In Section 5, the remaining challenges and research directions of fog after integrating into IoT system are discussed. In Section 6, the key role of 5G-based fog computing in the field of intelligent driving and tactile robots is prospected.

2. Basic Definition and Characteristic

2.1. Cloud Computing

2.1.1. Definition of Cloud Computing. Cloud computing was proposed to support ubiquitous, convenient, and on-demand network access to configurable computing resources like storage space, servers, networks, applications, and services in a shared pool. These resources can be provisioned and released rapidly with minimal service provider interaction or management effort [6]. Figure 1 shows a structure of cloud computing.

(1) Up-front investment in cloud computing is not needed because it is a pay-as-you-go pricing model that allows service providers to benefit from the cost of renting resources in the cloud without investing in infrastructure.

(2) The leasing and management of resources are flexible. Resources in the cloud can be quickly released according to the requirements of users. When service demand is low, service providers can actively release idle resources in the cloud, reducing the pressure of center load and energy consumption, and reduce costs.

(3) Data resources received by cloud data center can be collected and analyzed by infrastructure providers. Service providers access the data analysis to discover the potential business trends and determine the growth demand for services, which is the basis for them to expand their service direction and scale.

(4) Services in the cloud are easily accessible via the Internet by devices such as mobile phones, computers, and PDAs.

2.1.2. Characteristics of Cloud Computing. Cloud computing is widely used for the following characteristics [8].

2.2. Fog Computing

2.2.1. Definition of Fog Computing. Fog computing has been proposed as a layered model to support convenient access to a shared continuum of extensible computing resources. This model, consisting of physical or virtual fog nodes which are context-aware, facilitates the deployment of delay-aware and distributed applications and services. Fog nodes are located between intelligent terminal equipment and cloud services, which support common communication system and data management. The organizational form of fog nodes in the cluster is based on the specific working mode. Association and separation are supported by horizontal and vertical distribution, respectively, and can also be supported by the delay distance from the terminal devices to the fog nodes. Fog computing provides network connections to centralized services and local computing resources for terminal devices with minimizing request response time [9]. Figure 2 shows a fog-cloud system with three-layer architecture: cloud layer, fog layer, and IoT/end-users layer. The fog layer can be composed of one or more fog domains which are controlled by the same or different service providers. Each fog domain consists of the nodes including gateways, edge routers, switches, PCs, set-top boxes, and smart phones. The IoT/end-users layer is formed by two domains which include end-user devices and IoT devices, respectively [10].

2.2.2. Characteristics of Fog Computing. As a supplement to cloud computing, fog computing has several distinct characteristics from cloud computing. Cloud computing is based on social public cloud and IT operator services, while fog computing is based on small clouds such as enterprise, private, and personal clouds. Cloud computing typically consists of clusters of computing devices with high performance, while fog computing consists of more decentralized computers, each with its own function [9]. In addition, the following characteristics of fog computing are also essential.

(1) *Location Awareness and Low Latency.* Fog nodes are located between terminal devices and the cloud,

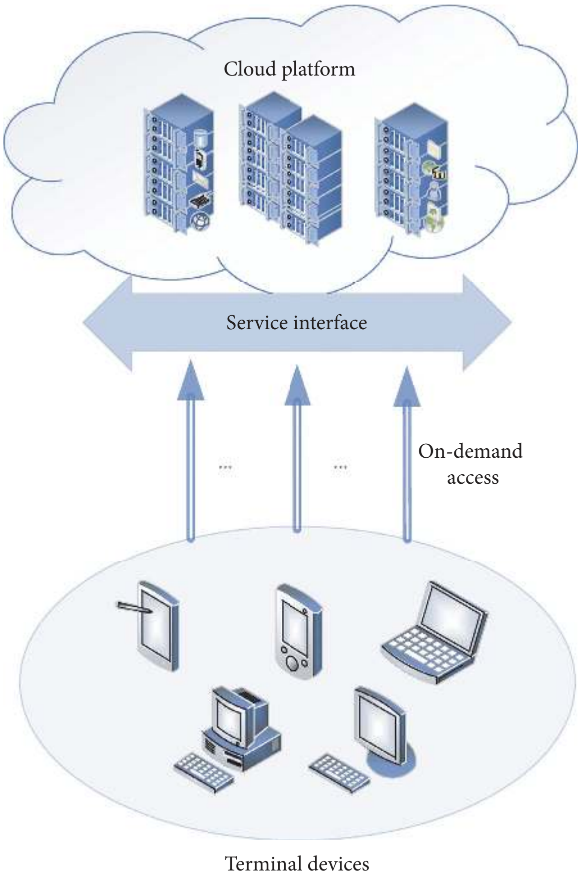

Figure 1: The structure of cloud computing [7].

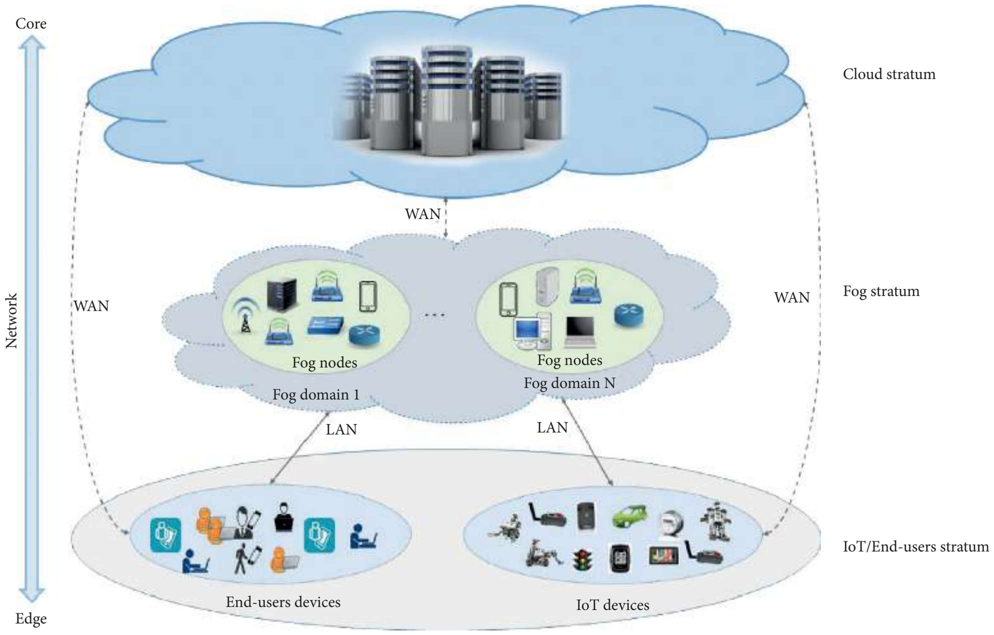

Figure 2: The structure of fog-cloud system [10].

tightly coupled to network and terminal devices, providing computing resources for them. Since the logical location of the fog node in the system and the cost of communication delays with other nodes are available, when the service requirements and data generated by the terminal device are sent to the network, the nearest available fog node will receive and process these requests and data [11]. Because fog nodes usually coexist with devices, the latency between them is much lower than the latency in cloud system [9].

(2) *Geographical Distribution*. Fog nodes provide some form of communication and data management service between the centralized cloud center and the edge of network where the terminal devices reside [3]. For example, high-quality streaming media services are provided to mobile vehicles in fog system by locating fog nodes on tracks and highways, which requires the extensive deployment of applications and target services which can identify location in fog. In order to deploy the capability to fog, the operation of geographically concentrated or dispersed fog nodes is adopted. Such geographical distribution makes fog system achieve good results in the service based on geographical location [12, 13].

(3) *Agility*. Fog nodes are distributed at the edge of the network, directly interacting with user terminals. The amount of data, network environment, and resource conditions that fog faces change constantly. Fog computing is adaptive in nature, supporting data load changes, flexible computing, resource pool, and network conditions changes at the cluster level and listing some of the adaptive features that are supported [9, 14].

(4) *Heterogeneity*. A large amount of heterogeneous data with different formats and storage forms is generated in terminal devices at the edge of the network [9]. The ability to collect, aggregate, and process these heterogeneous data is critical as the fog node acts as a base station to provide processing and storage services.

(5) *Interoperability and Federation*. Fog computing extends the powerful computing resources of the cloud to the network edge. Although the service requests of user devices can be quickly responded, the computing and storage capacity of each node is far less powerful than that of a centralized cloud center. Services requiring dense computation provided by fog to user devices may require joint support from multiple fog nodes. Therefore, interoperability of fog components and cross-domain cooperation among nodes are supported in the fog [10].

(6) *Real-Time Interactions*. The interaction between user devices and fog nodes is in real time with no long wait and transmission delays. The data sent by the user devices is received and processed by the adjacent fog node immediately. When the processing is completed, the processing results will be timely returned back to the user devices, which allows fog to support time-sensitive applications [9].

3. Cloud and Fog Computing

3.1. Comparison of Cloud and Fog Computing. As an extension of cloud computing, fog computing has many similarities and differences with cloud computing. The comparison between cloud and fog computing in this paper is made in the following aspects, which can intuitively reflect similarities and differences between them [7].

(1) *Reaction Time and Latency*. In fog system, time-sensitive data is sent to the fog node closest to data source for processing and analysis, rather than being sent directly to the distant cloud center, significantly reducing the service response time. Computation-intensive or delay-tolerant tasks can be processed in the dense area of fog nodes, which may take a few seconds. But the time to interact with the cloud can be a few minutes, minutes, or even hours [15, 16]. Thus, faster responses and more flexible choices are provided by fog computing than by cloud computing.

(2) *Node Location Distribution*. Far away from user devices, the cloud center provides users with resource-intensive computing and storage services in the form of central servers, while the fog is close to the edge of the network in the form of scattered fog nodes. Each fog node can be either individual computing devices or servers with strong capabilities [15].

(3) *Service Scope and Location Perception*. The service scope of cloud computing covers the whole world, but the cloud center is far away from the user terminal and cannot accurately perceive the location of the service. Unlike cloud computing, there are numbers of fog nodes in fog system with the capability of service location awareness [17–19]. Fog domains formed by multiple fog nodes serve user devices in local areas like city blocks. The service scope is usually determined by the density and computing power of fog nodes [15].

(4) *Vulnerability and Security*. In the cloud system, the user data is stored in the cloud computing center, far away from users and more likely to be attacked centrally. Although Xu et al. [20] proposed a fault-tolerant resource allocation method for data-intensive workflow to solve the recovery problem of failed tasks caused by the failure of a certain computing link, the possibility of systematic collapse caused by faster workflow aggregation still exists. Fog nodes are geographically dispersed and close to users, allowing users to protect the security and privacy of their data [1, 21].

3.2. Collaboration between Cloud and Fog Computing. Cloud center is far away from user terminals, and there are some problems in the application of the emerging IoTs (e.g., delay-sensitive applications). When fog extends the cloud to terminal devices on the edge of the network, these new service demands are met. So how can data sent by IoT devices be processed and analyzed in the collaboration of cloud and fog? This problem is discussed in the next two subsections.

3.2.1. Flow of Task Processing.

Figure 3 shows an example of a cloud-fog-IoT interaction model. What the fog and the cloud need to do, respectively, in the flow of task processing are introduced as follows.

(1) *The Things Fog Nodes Need to Do*. At the network edge, fog nodes receive real-time data from the terminal devices which are usually heterogeneous and dynamic. Then the analysis and real-time control of the data are carried out by running the applications supported by the IoT to achieve response within milliseconds [22]. Temporary data storage is also provided by fog nodes which usually lasts about 1 to 2 hours. After the data has been processed and analyzed, data summaries are sent to the cloud center regularly [9].

(2) *The Things Cloud Needs to Do*. Data digests sent by fog nodes are collected and integrated in the cloud platform. Then, an overall analysis and evaluation of these data are made to obtain service growth trends which are helpful for service providers to determine the direction of business development. Finally, new application rules based on the results of business evaluation are formulated by platform which are used to achieve the goal of adjusting service balance [9].

3.2.2. Task Offloading among Fog and Cloud.

Because of the limited resources, the tasks of user devices that cannot be processed locally are sent to the fog nodes. Assuming a situation where the data and service demands generated by the edge devices are only processed in the fog server, when the situation of dense service demands occurs, the computing delay will exceed the allowable range of the requester for the limited resource of fog nodes. In general, two strategies are adopted: (1) Offload tasks to cloud and process them in cloud with rich resources and powerful computing capacity. After the task completed, the required results will be returned. (2) Offload tasks to adjacent fog nodes and complete the user's service demands through distributed collaboration among the selected fog nodes. Figure 4 shows a simple task offloading model that includes both fog-to-fog and fog-to-cloud task offloading. Many scholars have investigated the two offloading strategies. They have been committed to building efficient architectures or developing smart strategies to decide whether to offload tasks to the cloud or fog nodes. In the latter case, the optimal offloading destination should be found in surrounding nodes.

Sun et al. [23] proposed a generic IoT-fog-cloud architecture. The problems of task offloading, time efficiency calculation, and allocation were turned into the problem of time and energy cost minimization. To solve this problem, they proposed an ETCORA algorithm that significantly reduces energy consumption and request completion time.

Yang et al. [14] and Du et al. [24] proposed joint offloading methods based on the existing fog-cloud framework and took various factors affecting the offloading (such as link bandwidth, latency, and computing capacity of the offloading targets) as parameters to generate mixed-integer programming. The difference is that Yang [14] proposed a greedy algorithm that maximizes operator benefits on the premise of ensuring user performance and security requirements, while Du [24] proposed a low-complexity suboptimal algorithm. The latter obtains offloading decision through randomization and semidefinite relaxation and obtained resource allocation policy using Lagrangian dual decomposition and fractional programming theory, which optimizes the time delay and energy consumption effectively.

Chen et al. [25] proposed an energy-saving offloading method. In this method, energy-saving offloading problem is formulated as a random optimization problem and random optimization technique is used to determine it.

Xu et al. [26] proposed a computation offloading method using blockchain technology. The balanced allocation strategy is generated by nondominant sorting genetic algorithm, and then the optimal offloading strategy is determined by simple additive weighting and multicriterion decision. In this way, overloaded tasks in a node can be offloaded to the most suitable adjacent node for safe and prompt processing.

Chen et al. [27] also proposed an offloading strategy. They designed an efficient online algorithm that took into account the unnecessary consumption of idle servers, combined with the computation offloading and sleep decisions of node servers, to maximize server quality and reduce energy consumption.

Nassar and Yilmaz [28] formulated the resource allocation problem as a Markov decision process and finally solved it by learning the optimal decision strategy with some reinforcement learning methods, namely, SARSA, Expected SARSA, Q-learning, and Monte Carlo. Their work can make the fog node decide the processing location of service request according to its own resources, realizing the low latency transaction offloading and processing with high performance.

Chen et al. [29] developed an energy-efficient computing offload scheme that comprehensively considers the energy-consumption components at a fog node, including the energy consumption of transmission, local computing, and waiting state. They proposed an accelerated gradient algorithm to find optimal offloading point with a high speed.

Deng et al. [30] investigated a load allocation problem that can be used to solve the optimal workload allocation between fog and cloud. They then decomposed the problem into three subproblems by using approximation method. By solving these subproblems separately, the optimal collaboration scheme with low latency and energy consumption is given. Ye et al. [31] proposed an extensible fog computing paradigm and developed a distribution strategy through genetic algorithm. This strategy enables the roadside nodes to offload computing tasks with the minimum cost within the allowable delay.

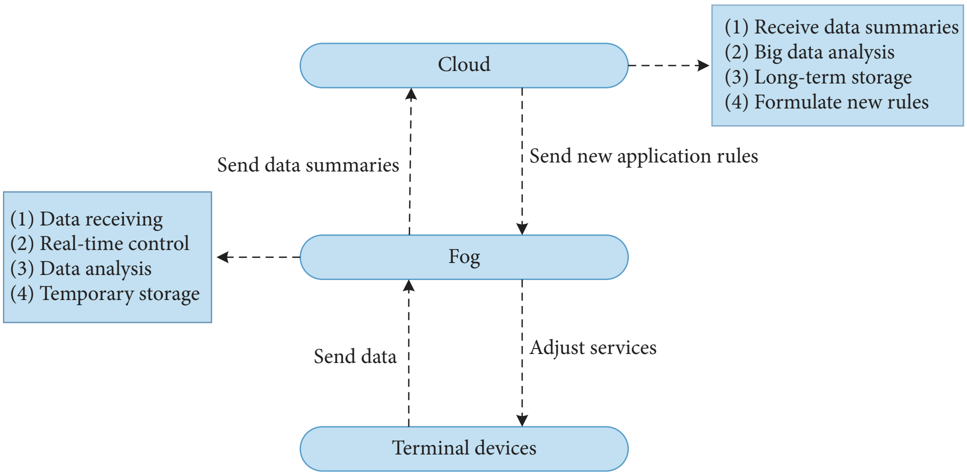

Figure 3: The interaction model of cloud-fog-IoT [7].

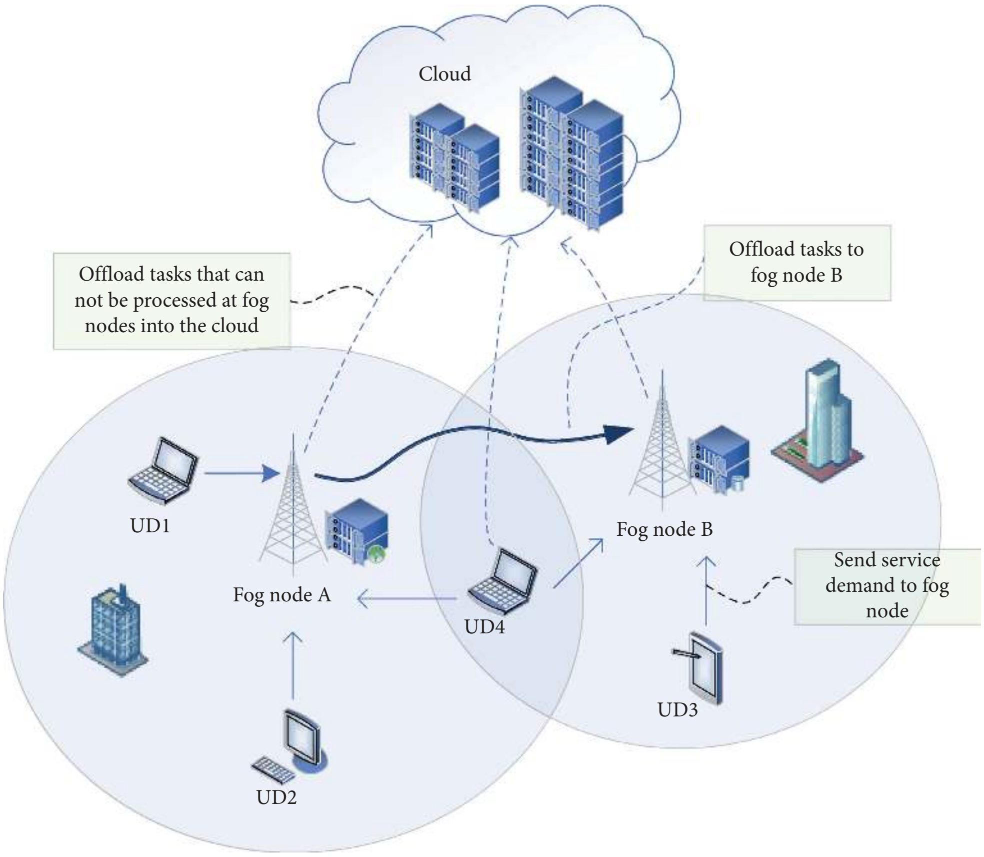
Cloud
Offload tasks that can not be processed at fog nodes into the cloud
Offload tasks to fog node B
UD1
Fog node A
UD4
Fog node B
Send service demand to fog node
UD3
UD2

Figure 4: The task offloading scheme among fog and cloud.

Table 1 is a summary of reviewed techniques or methods about task offloading among fog and cloud which contains each of the solutions and its unique advantages.

4. Fog Computing Helps on the New Challenges of IoT

Moving computing, storage, and analysis tasks to the cloud center with powerful resource has been a major solution to meet service needs over the past decades. However, the emergence of many delay-sensitive applications in the IoT has created many new application requirements, such as low latency and real-time interaction which the cloud cannot meet. The fog computing, expanding the cloud to network edge, is a better solution proposed to solve these problems. The challenges of the cloud-based IoTs and fog-based solutions with specific techniques are discussed in this section [7].

Table 1: Work summary of task offloading among fog and cloud.

Reference	Solution	Advantages
[23]	A generic IoT-fog-cloud architecture	Reduces energy consumption and request completion time
[14, 24]	A joint offloading method based on the existing fog-cloud framework	Takes various factors affecting the offloading as parameters to generate mixed-integer programming
[25]	An energy-saving offloading method	Uses random optimization technique to solve energy-saving offloading problem
[26]	A computation offloading method using blockchain	Offloads overloaded tasks to the suitable adjacent node with the optimal offloading strategy determined by simple additive weighting and multicriterion decision
[27]	An efficient online algorithm considering the unnecessary consumption of idle servers	Combines the computation offloading and sleep decisions of node servers to maximize server quality and reduces energy consumption
[28]	An optimal decision strategy with some reinforcement learning methods	Makes the fog node decide the processing location itself and realizes low-latency offloading and high-quality processing
[29]	An energy-efficient computing offload scheme	Proposes an accelerated gradient algorithm to find optimal offloading point with a high speed
[30]	An optimal collaboration scheme with low latency and energy consumption	Decomposes the load allocation problem into three subproblems by using approximation method
[31]	An extensible fog computing paradigm	Develops a distribution strategy based on genetic algorithm to enable the roadside nodes to offload computing tasks with the minimum cost

4.1. Low Latency Requirements. Nowadays, many life applications and industrial systems require end-to-end communication with low latency, such as smart home applications and virtual reality applications, especially those requiring ultralow latency and affecting personal safety like driverless car [32]. In order to minimize the latency in data transmission, fog nodes are deployed on the edge of network, allowing data to be processed, analyzed, and stored near end-users.

Due to the decentralized distribution of IoT devices, computing and service load distribution between fog nodes affect the computing and communication delay of data flows, respectively. To solve this problem, Fan and Ansari [33] proposed a workload-balancing scheme that associates the appropriate fog nodes with user devices, minimizing the data flow latency for data communication and task processing.

Xu et al. [34] introduced 5G into Internet of connected vehicles (IoCV) to improve the transmission rate of roadside equipment. They innovatively designed an adaptive computation offloading method for the prospective 5G-driven IoCV in which multiobjective evolutionary algorithm is used to generate the available solutions. The optimal solution obtained by utility evaluation effectively optimizes the task response time and resource utilization efficiency.

Li et al. [35] proposed a delay estimation framework for IoT based on fog, which can accurately predict the end-to-end delay in cloud-fog-things continuum. Mohammed et al. [36] proposed a data placement strategy for fog architecture. They solved the problem of data layout with generalized assignment and developed two solutions. These solutions reduce latency by about 86% and 60%, respectively, compared with solutions based on cloud.

Naranjo et al. [37] proposed a smart city network architecture based on fog. In order to manage the application under the premise of satisfying QoS, the communication between devices in the architecture is divided into three categories. With this approach, the nodes in the architecture can run in high efficiency and low latency.

Craciunescu et al. [38] and Cao et al. [39] proposed algorithms for medical systems in order to detect individual falls in time. Gu et al. [40] minimized communication time by optimizing resource utilization in the healthcare system.

Dragi et al. [41] proposed a new nature-inspired smart fog architecture. This architecture is a distributed intelligent system modeled using new techniques in the fields of graph theory, multicriteria decision-making, and machine learning. It can provide adaptive resource management and low decision latency by simulating the function of the human brain.

Yousefpour et al. [42] and Elbamby et al. [43] proposed task offloading strategies to reduce service latency. In paper [42], fog-to-fog communication was employed to share workload, while a clustering method was designed in [43], which groups user devices and their service nodes with common task interests and uses a matching game, where computing delay is minimized under delay and reliability constraints.

Diro et al. [44] proposed an aggregated software defined network (SDN) and fog/IoT architecture, which allocates different flow spaces for heterogeneous IoT applications according to flow categories to meet the priority-based QoS requirements. This architecture reduces the impact of packet blocking on QoS delivery through more fine-grained control.

Rahbari et al. [45] proposed a greedy scheduling algorithm based on knapsack, which allocates resource to nodes in fog considering various network parameters. Through simulation experiments, they proved that the proposed algorithm has better performance in the optimization of time delay and energy consumption.

Shi et al. [46] set up a proof-of-concept platform. They tested the face recognition application and reduced the response time from 900 milliseconds to 169 milliseconds by offloading the computing tasks from cloud to the edge. Fog also supports time-sensitive control functions in local physical systems [3].

Table 2 is a summary of techniques or methods about reducing latency based on fog for IoT applications, containing reviewed solutions and their unique advantages.

4.2. Network Bandwidth Constraints. As the number of devices connected to the network is increasing rapidly, the speed of data generation is increasing exponentially [47]. For example, a connected car can generate tens of megabytes of data per second including vehicle status (e.g., wear of vehicle components), vehicle mobility (e.g., driving speeds and routes), vehicle surroundings (e.g., weather conditions and road conditions), and videos recorded by automobile data recorder. A driverless car can generate much more data [48]. The American Smart Grid generates 1,000 gigabytes of data per year. Google trades 1 gigabyte a month and the Library of Congress generates about 2.4 gigabytes of data each month [49]. If all data is transmitted to cloud, ultrahigh-quality network bandwidth is required, which poses a heavy burden on the existing network bandwidth and even leads to congestion, obviously not advisable.

Fog nodes receive and process the data near user devices, filtering out irrelevant or inappropriate data to prevent them from traveling across the whole network [1]. Data generated by user devices is allocated to the nearest fog node for processing instead of being transmitted to cloud center, because much critical analysis does not require powerful computing and storage capabilities of the cloud. ABI Research estimated that 90% of the data generated by endpoints will be stored and processed locally, not in the cloud [47]. The way fog processes data significantly reduces the amount of data sent to the cloud, easing the burden of network bandwidth.

4.3. Resource Constraints of Devices. In IoT system, user devices with limited resources (e.g., computing, network, and storage resources) cannot interact with the cloud directly, for which sending data to the cloud is impractical [50]. It is also unrealistic to update resources for these devices at high cost.

In this case, the functions of cloud cannot be performed well, while fog nodes can handle resource-intensive tasks for these devices without requirement of high performance [51]. Fog nodes are core components in the fog computing architecture, which are either physical components (such as servers, routers, gateways, and switches) or virtual components (such as virtual machines and virtual switches). Fog nodes tightly couple with access networks or intelligent devices and provide computing resource for these devices [9]. Therefore, the complexity and resource requirements of terminal devices are reduced.

4.4. Stability of Service. When a stable connection between user device and cloud is not guaranteed, continuous service cannot be obtained from cloud. For example, when a car enters an area not covered by a stable network, the cloud service is intermittently disconnected. Some necessary services are unavailable to the on-board devices and other user devices [3].

But, unlike cloud, fog nodes are distributed geographically. Edge networks created by fog computing are located at different points to extend the isolated infrastructure in cloud. A local system formed by fog nodes which can operate autonomously, with continuous coverage of the service scope, helps to process service demands more quickly and steadily [1]. Location-based mobility requirements and diversified service are supported by the administrators of fog nodes [18, 40, 52]. Due to the decentralized distribution of IoT devices, computing and service load distribution between fog nodes affect the computing delay and stability of service, respectively. To solve this problem, Fan Qiang and Ansari Nirwan [33] proposed a workload-balancing scheme that associates the appropriate fog nodes with user devices, which minimizes the data flow latency of communication and significantly improves the stability of service.

Yousefpour et al. [53] proposed a dynamic service-provisioning framework based on QoS perception for dynamically deploying application services on fog nodes. Then a possible formula and two efficient greedy algorithms were given to address the service provision, which can provide stable and continuous service with low latency.

4.5. Security and Privacy. With the purpose of requesting a service, large amounts of data are sent to the network, including personal privacy and corporate data. For example, work logs generated by smart home appliances can be mined to reveal the work and rest rules of users, and important private information (e.g., password and possessions) can be eavesdropped from chat logs. Therefore, both the static data and the transmission process in IoT need to be protected, which requires the monitoring and automatic response of malicious attacks in the whole process [13].

In cloud computing, corporate and private data, and even confidential data, are stored centrally in cloud servers far away from users. The security and privacy of personal and enterprise data are questioned by users because they cannot determine whether their data is stolen by malicious actors with interest and whether their data will be lost in the expansion of the cloud center [1].

In fog computing, sensitive data is processed locally rather than being sent to the cloud. Local administrators can inspect and monitor the devices that collect, process, analyze, and store data [13, 51]. In the fog system, each fog node can act as a proxy for user devices which cannot adequately protect data due to resource constraints, helping update and manage the security credentials of user devices, to compensate for their security vacancies.

Abbas et al. [54] proposed an innovative fog security service to transfer confidential and sensitive data generated by IoT devices to fog nodes for processing and provide end-to-end security between them by using two mature encryption schemes, identity-based signature and identity-based encryption. Local information also can be used to

Table 2: Work summary of reducing latency based on fog for IoT applications.

Reference	Solution	Advantages
[33]	A workload-balancing scheme associating the appropriate base stations with user devices	Minimizes the data flow latency for data communication and task processing
[34]	An adaptive computation offloading method for the prospective 5G-driven IoCV	Optimizes the task response time and resource utilization efficiency with the optimal solution obtained by utility evaluation
[35]	A delay estimation framework for IoT based on fog	Accurately predicts the end-to-end delay in cloud-fog-things continuum
[36]	A data placement strategy for fog architecture	Solves data layout problem with generalized assignment problem and develops two solutions
[37]	A smart city network architecture based on fog	Divides the communication between devices into three categories to satisfy QoS
[38, 39]	Detection algorithms and fog-based medical information systems	Detects individual falls in time
[40]	A medical cyber-physical system supported by fog computing and a heuristic algorithm with two phases	Minimizes communication time by optimizing resource utilization
[41]	A new nature-inspired smart fog architecture	Provides adaptive resource management and low decision latency by simulating the function of the human brain
[42]	A task offloading strategy to reduce service latency	Employs fog-to-fog communication and share workload
[43]	A clustering method for offloading	Groups user devices and nodes and uses a matching game to minimize computing delay
[44]	An aggregated software defined network and a fog/IoT architecture	Reduces the impact of packet blocking on QoS delivery through more fine-grained control
[45]	A greedy scheduling algorithm based on knapsack	Allocates resource to fog nodes considering various network parameters, optimizing time delay and energy consumption

monitor the security status of nearby devices and detect threats immediately to ensure security [3, 55].

In recent years, some malicious code detection techniques have been proposed to solve the problem of security detection in fog environment. Zhang et al. [56] used signature-based detection technique and Martignoni et al. [57] proposed a behavior-based detection technique. However, behavior-based detection has a high cost because of resource constraints of fog nodes. Signature-based detection technology is more effective, but it is still difficult to detect variable malicious code in distributed fog nodes. In this case, a hybrid detection technology combining the two technologies was proposed to solve this problem [58]. The behavior-based detection technology in the cloud is distributed to fog nodes, and suspicious software files are detected and sent to the cloud for analysis. If the malware is new, the analysis result will be saved to the database as a new signature and the malicious signature list of each node will be updated.

Xu et al. [59–61] improved the strength Pareto evolutionary algorithm to obtain offloading schemes. The scheme proposed in paper [59] is privacy-aware, which effectively protects the privacy of training tasks offloaded to fog nodes with maintaining overall network performance, while schemes in paper [60, 61] are trust-aware. After the balanced scheme is obtained, they used the multicriterion decision technique and similarity prioritization technique of ideal solution to determine the optimal solution, which can effectively protect privacy with minimized service latency.

Thota et al. [62] proposed efficient centralized security architecture based on fog environment. Patient's medical data is transmitted seamlessly from sensors to edge devices and finally to the cloud for medical staff to access. The architecture effectively protects the privacy of patients and the security of medical data.

Chi et al. [17] proposed a service recommendation method based on amplified location-sensitive hash in order to ensure privacy security of distributed quality data from multiple platforms during cross-platform communication and proved its feasibility through experiments.

Viejo et al. [63] used new fog choreography concepts to solve the problem of reduction of service response time caused by resource constraints of the IoT. The security and efficient delivery of the service were realized successfully, which provide effective support for expensive encryption technology.

Mukherjee et al. [64] firstly designed and implemented a middleware featuring end-to-end security for cloud-fog communications. The intermittence and flexibility of middleware were proposed, respectively, by dealing with unreliable network connection and customizing the security configuration required by the application. The middleware can provide fast, light-weight, and resource-aware security for a wide variety of IoT applications.

Li et al. [65] proposed a hierarchical data aggregation scheme for efficient privacy protection. By modifying Paillier encryption, this scheme can not only resist external attacks but also prevent personal privacy data from leaking from internal devices.

Daoud et al. [66] designed a security model based on fog-IoT network. Then a comprehensive scheduling process and resource allocation mechanism were proposed based on the model. Through these efforts, they successfully introduced the active security scheme with low latency and ultra-trustworthiness into fog-IoT network.

Table 3: Work summary of security and privacy based on fog for IoT applications.

Reference	Solution	Advantages
[54]	An innovative fog security service	Uses identity-based signature and encryption to effectively protect the sensitive data transmitted to the fog node
[56, 57]	Two detection techniques	Detects malicious code attacks stably
[58]	A hybrid detection technology	Extends cloud-based detection technology to fog nodes
[59–61]	Offloading schemes driven by the improved strength Pareto evolutionary algorithm	Uses the multicriterion decision technique and similarity prioritization technique to protect privacy with minimized service delay
[62]	An efficient centralized security architecture based on fog environment	Protects the privacy of patients and the security of medical data through the device-edge-cloud transmission route
[17]	A service recommendation method based on amplified location-sensitive hash	Ensures privacy security of distributed quality data during cross-platform communication from multiple platforms
[63]	A new fog choreography concept	Realizes the security and efficient delivery of the service
[64]	A middleware featuring end-to-end security for cloud-fog communications	Uses middleware to provide fast, light-weight, and resource-aware security for a wide variety of IoT applications
[65]	A hierarchical data aggregation scheme for efficient privacy protection	Prevents personal privacy leaks while resisting external attacks
[66]	A security model based on fog-IoT network	Introduces the active security scheme with low latency and ultratrustworthiness into fog-IoT network

Table 3 is a summary of reviewed fog-based techniques or methods to protect security and latency in IoT applications, containing each solution and its unique advantages.

5. Challenges and Research Directions

5.1. Heterogeneity. In the fog, a large number of heterogeneous platforms and devices are connected to the Internet, and the services or resource requests they send are often heterogeneous, which requires all nodes in the network to dynamically identify all the request information. In fact, there has been some work to classify nodes using labels [67] or to add descriptions to resources to provide solutions for heterogeneous requests. Most of these solutions are based on static recognition and their work depends on the developers of the architecture program [68, 69], lacking flexibility and generality. In addition, data or service requests sent by IoT devices may be supported by multiple service providers, each using a mostly inconsistent service description model. More complex heterogeneous data and models will be produced for the addition of new providers, which brings about more burden to programmers.

There have been also many algorithms proposed in the fog environment to compute the capabilities of fog nodes, some of which consider the resource constraints of different devices and model the differences of capabilities between nodes, while most of which cannot meet the heterogeneous criteria [31, 70, 71]. Even so, these works are based on the different understanding of heterogeneity of nodes in network.

Therefore, semantic specifications should be defined in a clear form within the fog domain so that IoT devices or clouds connected to the fog network can share information in a commonly understood manner, which will contribute to the homogeneity of heterogeneous data at the edges and the simplification of data transfer protocols [10].

5.2. Mobility. Mobility presents significant challenges for both IoT devices and fog nodes. A large number of IoT devices are now wirelessly connected to the network and are generally mobile. The coverage of each fog domain is limited, which makes it necessary to consider service migration when the connected IoT device falls out of service scope.

How to migrate the service data from the previous fog domain to the new fog domain without interrupting the service is a challenging task. In the simplest case, IoT devices on a vehicle may move between different fog domains, making the service provided to on-board devices unstable. To solve this problem, Hassan et al. [72] recommended that service metadata be stored in the cloud so that it can be downloaded continuously after the device is migrated. But it will undoubtedly take some time to update the service information after the migration because of the difference of data between the cloud and the device. Another option being considered is to extend the existing fog architecture to support device mobility [73], which still needs to address the migration problem further. In fact, if the real-time moving trajectory of the device is obtained, machine learning technology can be used to analyze it and predict the future trajectory. Based on the predicted results, the next fog domain can update the service information of the device before it reaches the edge of the fog domain.

In addition, how to allocate the available resources/tasks that a fog node carries when it joins/leaves a fog domain is a complex issue. Song et al. [74] investigated this problem, hoping to realize dynamic load balancing in the fog region during node migration. Even so, how to achieve load balancing in a short time with affecting fewest nodes is still an optimal-solution problem to be explored.

5.3. Data and Equipment Management. Billions of devices (e.g., mobile phones, computers, palmtops, and smart appliances) are connected to the fog and the scale is growing. Different faults caused by various heterogeneous devices may occur anywhere. But tracking the fault information of hardware and providing software patches for maintenance in time are complex works, which need a sound fault detection and analysis mechanism and can locate the location of the fault in time. In addition, the Internet Data Center (IDC) estimated that the amount of data generated by IoT devices will reach 44 zettabytes in 2020 [75]. How to store such a huge amount of data in fog nodes with limited resources is another problem that must be solved.

Open fog suggests using machine learning technology to develop a framework with fault comprehensive feature detection and fault tolerance [76], especially in systems involving critical applications of life, such as anomaly detection in the medical field. There is also a data management scheme proposed in [67], which uses the labeling method to add labels for different types of data to facilitate access. This method can be used in the management of IoT devices. However, many management schemes do not take the resource availability into account, which has a great impact on the workload that devices can share in fog. Therefore, the expected research scheme should be based on the dynamic update of the connected devices, rather than simply assuming that the devices are fixed.

5.4. QoS Management. SLA management is an unavoidable direction to study QoS management. There are a number of cloud-based SLA management schemes that effectively reduce transmission latency, guarantee transmission bandwidth, and reduce packet loss rates (e.g., [77–82]) by reducing SLA violation rates or improving QoS.

In the fog, however, few SLA-managed schemes have been proposed, which are critical to maintaining desired QoS in the fog, where distributed services are dynamically provided. Among the papers reviewed in this article, only Yousefpour et al. [53] proposed a dynamic service-provisioning framework based on QoS perception for dynamically deploying application services on fog nodes, while it is only sensitive to the measure of delay, which is the same as many other strategies that meet QoS standards.

Although latency is certainly an important indicator of a system, there are many other important performance indicators to consider, such as bandwidth, resource utilization, and energy consumption. These indicators should be integrated as targets for future research strategies rather than as constraints alone. For example, Yang et al. [14] and Du et al. [24] proposed a joint offloading method that takes the link bandwidth and latency as parameters, but their method is only an optimization under time delay constraints rather than multiobjective optimization.

In fact, cloud-based QoS management technology has been relatively mature. The new SLA management solution could be an extension of the cloud-based SLA management technology with additional considerations for the uniqueness of fog [10] (such as resource constraints, low latency, and geographic distribution). Although the services are more diversified due to the large amount of heterogeneous data in fog, it is not difficult to solve the fog-based integrated QoS optimization if the semantic specification mentioned in Section 5.1 can be completed to solve the problem of heterogeneity.

5.5. Security and Privacy. As mentioned in Section 4.5, fog nodes act as agents to provide secure selection for resource-constrained devices and encrypt the transmission before the data leaves the edge [3]. But, to put it in another way, fog nodes are scattered on the edge of network where the environment is much worse than the cloud center [83, 84]. Because many fog nodes are in public places, the safety of physical equipment is difficult to guarantee. Moreover, lack of sufficient resources and computing power makes fog nodes unable to perform some complex security algorithms, so fog systems are more vulnerable to attack, such as session hijacking, session riding, and SQL injection [85].

The security and privacy challenges of the fog can be divided into four points: (1) A trust model and mutual authentication trust mechanism are necessary to guarantee the reliability and security of fog network [86]. (2) Traditional certificate and public key infrastructure (PKI) authentication mechanisms are difficult to be used by resource-constrained devices. [87]. (3) The messages sent by IoT devices cannot be encrypted symmetrically. In addition, asymmetrical encryption technology has great challenges, including resource and environment constraints, overhead constraints, and maintenance of the PKI [86]. (4) Location privacy in fog is vulnerable to leakage. While fog nodes are location-aware, collecting location information of IoT devices has become much easier than before [88]. In addition, frequent interaction among the three layers of fog architecture will increase the possibility of privacy disclosure. Without proper security measures, the performance of fog system may be seriously damaged.

6. Prospects

The rise of 5G technology promotes the application of fog computing technology. We expect fog computing technology based on 5G network to play a key role in the fields of intelligent driving and tactile robots.

Intelligent driving is an important technology to solve traffic congestion in the future, including automatic driving and human intervention. Fog nodes are distributed on the roadside, which can reduce the delay of data transmission between vehicles and nodes. But 4G network-based communication is far from being capable of transmitting the huge amount of data that cars generate while driving, and the delay is far from the requirement of automatic driving. 5G network is the key enabler to realize intelligent driving in fog system, which can provide ultrastable and ultrafast data transmission. When the vehicle is under automatic driving, roadside sensors and on-board equipment collect real-time road and vehicle information and send it to the roadside fog nodes for processing and analysis. Applying sophisticated machine learning techniques to fog nodes is necessary, which can learn to recognize all possible road conditions and send correct response instructions to driving system. Based on the same principle, the attitude detection of the driver during manual intervention can also help to improve the safety of driving.

Traditional robots are usually operated by command. It is difficult to break the technical bottleneck of remote control for transmission delay. But if the robot system architecture is deployed on the fog, the sensing equipment of the remote robot and the control equipment with tactile sensation are taken as the user terminal equipment, and the service nodes supporting the tactile command processing and analysis of the robot are brought into the fog layer. With the support of 5G ultrahigh transmission rate and tactile Internet [89, 90], real-time control of the robot can be realized. This work can be extended to the field of telemedicine and disaster relief with great research prospects. These works need to be based on completing the challenges of Section 5.

7. Conclusion

This article surveys the literature on cloud computing, fog computing, and IoT. Based on the concept and characterization description of cloud computing and fog computing, the comparison and collaboration between them are elaborated and some proposed task offloading methods are introduced emphatically. By surveying proposed techniques and methods, the contribution of fog computing to solving the challenges of IoT applications is introduced. Then the remaining challenges and research directions of fog after integrating into IoT system are discussed. In addition, the key role of 5G-based fog computing in the field of intelligent driving and tactile robots is prospected.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Authors' Contributions

Jielin Jiang, Zheng Li, Yuan Tian, and Najla Al-Nabhan conceived and designed the review. Zheng Li wrote the paper. All authors reviewed and edited the manuscript. All authors read and approved the final manuscript.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61601235 and in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20160972. Meanwhile, the authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RG-1441-331.

References

[1] K. Saharan and A. Kumar, "Fog in comparison to cloud: a survey," *International Journal of Computer Applications*, vol. 122, pp. 10–12, 2015.

[2] T. CAI, J. Li, A. S. Mian, R. li, T. Sellis, and J. X. Yu, "Target-aware holistic influence maximization in spatial social networks fluence maximization in spatial social networks," *IEEE Transactions on Knowledge and Data Engineering*, p. 1, 2020.

[3] M. Chiang and T. Zhang, "Fog and iot: an overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[4] P. Lai, Q. He, M. Abdelrazek, and F. Chen, "Optimal edge user allocation in edge computing with variable sized vector bin packing," *Service-Oriented Computing*, Springer, Berlin, Germany, pp. 230–245, 2018.

[5] X. Xia, F. Chen, and Q. He, "Cost-effective app data distribution in edge computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 31–44, 2020.

[6] P. M. Mell and T. Grance, *The Nist Definition of Cloud Computing*, CSRC, Beijing, China, 2011.

[7] Z. Li and Y. Wang, "An introduction and comparison of the application of cloud and fog in iot," in *Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications*, pp. 63–75, Springer, Cham, Switzerland, 2020.

[8] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[9] M. lorga, L. Feldman, and R. Barton, *Fog Computing Conceptual Model*, NIST, Gaithersburg, MD, USA, 2018.

[10] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: state-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[11] X. Xu, B. Shen, X. Yin et al., "Edge server quantification and placement for offloading social media services in industrial cognitive IoVfication and placement for offloading social media services in industrial cognitive iov," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[12] Q. He, G. Cui, X. Zhang et al., "A game-theoretical approach for user allocation in edge computing environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 515–529, 2020.

[13] P. Vinod, M. Chetan, and K. Sangramsing, "A review-fog computing and its role in the internet of things," *International Journal of Engineering Research and Applications*, vol. 6, pp. 2248–2267, 2016.

[14] Y. Yang, X. Chang, Z. Han, and L. Li, "Delay-aware secure computation offloading mechanism in a fog-cloud framework," in *Proceedings of the 2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications*, pp. 346–353, Melbourne, Australia, December 2018.

[15] F. Mohamed, G. Osman, and H. Suhaidi, "Fog computing: will it be the future of cloud computing?" in *Proceedings of The Third International Conference on Informatics and Applications*, Kuala Terengganu, Malaysia, October 2014.

[16] C. Systems, *Fog Computing and the Internet of Things: Extend the Cloud to where the Things Are*, ACM, New York, NY, USA, 2015.

[17] X. Chi, C. Yan, H. Wang, W. Rafique, and L. Qi, "Amplified locality-sensitive hashing-based recommender systems with privacy protectionfied locality-sensitive hashing-based recommender systems with privacy protection," *Concurrency and Computation: Practice and Experience*, p. 5681, 2020.

[18] L. Wang, X. Zhang, R. Wang, C. Yan, H. Kou, and L. Qi, "Diversified service recommendation with high accuracy and efficiencyfied service recommendation with high accuracy and efficiency," *Knowledge-Based Systems*, vol. 204, p. 106196, 2020.

[19] W. Zhong, X. Yin, X. Zhang et al., "Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment," *Computer Communications*, vol. 157, pp. 116–123, 2020.

[20] X. Xu, R. Mo, F. Dai, W. Lin, S. Wan, and W. Dou, "Dynamic resource provisioning with fault tolerance for data-intensive meteorological workflows in cloudflows in cloud," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6172–6181, 2020.

[21] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y.-q. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Transactions on Services Computing*, vol. 13, pp. 289–300, 2020.

[22] H. Liu, H. Kou, C. Yan, and L. Qi, "Keywords-driven and popularity-aware paper recommendation based on undirected paper citation graph," *Complexity*, vol. 2020, Article ID 2085638, 15 pages, 2020.

[23] H. Sun, H. Yu, G. Fan, and L. Chen, "Energy and time efficient task offloading and resource allocation on the generic IoT-fog-cloud architecture," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 548–563, 2020.

[24] J. Du, L. Zhao, J. Feng, and X. Chu, "Computation offloading and resource allocation in mixed fog/cloud computing systems with min-max fairness guarantee," *IEEE Transactions on Communications*, vol. 66, no. 4, pp. 1594–1608, 2018.

[25] Y. Chen, N. Zhang, Y. Zhang, X. Chen, W. Wu, and X. S. Shen, "TOFFEE: task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing," *IEEE Transactions on Cloud Computing*, p. 1, 2019.

[26] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: blockchain-enabled computation offloading for iot in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2020.

[27] L. Chen, S. Zhou, and J. Xu, "Energy efficient mobile edge computing in dense cellular networks," 2017, http://arxiv.org/abs/1701.07405.

[28] A. T. Nassar and Y. Yilmaz, "Reinforcement learning-based resource allocation in fog ran for iot with heterogeneous latency requirements," 2018, http://arxiv.org/abs/1806–04582.

[29] S. Chen, Y. Zheng, K. Wang, and W. Lu, "Delay guaranteed energy-efficient computation offloading for industrial iot in fog computing," in *Proceedings of the 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, Shanghai, China, May 2019.

[30] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, "Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1171–1181, 2016.

[31] D. Ye, M. Wu, S. Tang, and R. Yu, "Scalable fog computing with service offloading in bus networks," in *Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 247–251, Beijing, China, June 2016.

[32] C. Shi, Z. Ren, K. Yang et al., "Ultra-low latency cloud-fog computing for industrial internet of things," in *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, April 2018.

[33] Q. Fan and N. Ansari, "Towards workload balancing in fog computing empowered iot," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 253–262, 2020.

[34] X. Xu, Q. Wu, L. Qi, W. Dou, S.-B. Tsai, and M. Z. A. Bhuiyan, "Trust-aware service offloading for video surveillance in edge computing enabled internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2020.

[35] J. Li, T. Zhang, J. Jin, Y. Yang, D. Yuan, and L. Gao, "Latency estimation for fog-based internet of things," in *Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6, Melbourne, Australia, November 2017.

[36] M. I. Naas, P. R. Parvedy, J. Boukhobza, and L. Lemarchand, "iFogstor: an iot data placement strategy for fog infrastructure," in *Proceedings of the 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, pp. 97–104, Madrid, Spain, May 2017.

[37] P. G. V. Naranjo, Z. Pooranian, M. Shojafar, M. Conti, and R. Buyya, "Focan: a fog-supported smart city network architecture for management of applications in the internet of everything environments," 2019, http://arxiv.org/abs/1710.01801.

[38] R. Craciunescu, A. Mihovska, M. Mihaylov, S. Kyriazakos, R. Prasad, and S. Halunga, "Implementation of fog computing for reliable e-health applications," in *Proceedings of the 2015 49th Asilomar Conference on Signals, Systems and Computers*, pp. 459–463, Pacific Grove, CA, USA, November 2015.

[39] Y. Cao, S. Chen, P. Hou, and D. Brown, "Fast: a fog computing assisted distributed analytics system to monitor fall for stroke mitigation," in *Proceedings of the 2015 IEEE International Conference on Networking, Architecture and Storage (NAS)*, pp. 2–11, Boston, MA, USA, August 2015.

[40] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost efficient resource management in fog computing supported medical cyber-physical system," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 1, pp. 108–119, 2017.

[41] D. Kimovski, H. Ijaz, N. Saurabh, and R. Prodan, "Adaptive nature-inspired fog architecture," in *Proceedings of the 2018 IEEE 2nd International Conference on Fog and Edge Computing (ICFEC)*, pp. 1–8, Washington, DC, USA, May 2018.

[42] A. Yousefpour, G. Ishigaki, R. Gour, and J. P. Jue, "On reducing iot service delay via fog offloading," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 998–1010, 2018.

[43] M. S. Elbamby, M. Bennis, and W. Saad, "Proactive edge computing in latency-constrained fog networks," in *Proceedings of the 2017 European Conference on Networks and Communications (EuCNC)*, pp. 1–6, Oulu, Finland, June 2017.

[44] A. A. Diro, H. T. Reda, and N. Chilamkurti, "Differential flow space allocation scheme in SDN based fog computing for IoT applicationsfferential flow space allocation scheme in sdn based fog computing for iot applications," *Journal of Ambient Intelligence and Humanized Computing*, 2018.

[45] D. Rahabri and M. Nickray, "Low-latency and energy-efficient scheduling in fog-based iot applications," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 27, pp. 1406–1427, 2019.

[46] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[47] R. Kelly, "Internet of things data to top 1.6 zettabytes by 2022," *Campus Technology*, vol. 9, pp. 1536–1233, 2016.

[48] L. Mearian, "Self-driving cars could create 1gb of data a second," *Computerworld*, vol. 23, 2013.

[49] N. Cochrane, "US smart grid to generate 1000 petabytes of data a year," *Expert Systems with Applications*, 2016.

[50] V. Mushunuri, A. Kattepur, H. K. Rath, and A. Simha, "Resource optimization in fog enabled iot deployments," in *Proceedings of the 2017 Second International Conference on Fog and Mobile Edge Computing*, pp. 6–13, Valencia, Spain, May 2017.

[51] C. Zhou, A. Li, A. Hou et al., "Modeling methodology for early warning of chronic heart failure based on real medical big data," *Expert Systems with Applications*, vol. 151, Article ID 113361, 2020.

[52] J. Li, T. Cai, K. Deng, X. Wang, T. Sellis, and F. Xia, "Community-diversified influence maximization in social networksfied influence maximization in social networks," *Information Systems*, vol. 92, p. 101522, 2020.

[53] A. Yousefpour, A. Patil, G. Ishigaki, I. Kim, and X. e.a. Wang, "Qos-aware dynamic fog service provisioning," 2018, http://arxiv.org/abs/1802.00800.

[54] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing iot-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 16, 2019.

[55] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-Enabled accountability mechanism against information leakage in vertical industry services," *IEEE Transactions on Network Science and Engineering*, p. 1, 2020.

[56] M. Zhang, Y. Duan, H. Yin, and Z. Zhao, "Semantics-aware android malware classification using weighted contextual API dependency graphsfication using weighted contextual api dependency graphs," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security-CCS'14*, pp. 1105–1116, Scottsdale, AZ, USA, November 2014.

[57] L. Martignoni, R. Paleari, and D. Bruschi, "A framework for behavior-based malware analysis in the cloud," in *Information Systems Security*, pp. 178–192, Springer, Berlin, Heidelberg, 2009.

[58] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported internet of things environment," in *Proceedings of the 2015 6th International Conference on the Network of the Future (NOF)*, pp. 1–3, Montreal, Canada, September 2015.

[59] X. Xu, X. Liu, X. Yin, S. Wang, Q. Qi, and L. Qi, "Privacy-aware offloading for training tasks of generative adversarial network in edge computing," *Information Sciences*, vol. 532, pp. 1–15, 2020.

[60] X. Xu, X. Zhang, X. Liu, J. Jiang, L. Qi, and M. Z. A. Bhuiyan, "Adaptive computation offloading with edge for 5G-envisioned internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2020.

[61] X. Xu, X. Liu, Z. Xu, F. Dai, X. Zhang, and L. Qi, "Trust-oriented iot service placement for smart cities in edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4084–4091, 2020.

[62] C. Thota, R. Sundarasekar, G. Manogaran, R. Varatharajan, and M. K. Priyan, "Centralized fog computing security platform for IoT and cloud in healthcare system," in *Fog Computing*, pp. 365–378, Springer, Berlin, Heidelberg, 2018.

[63] A. Viejo and D. Sánchez, "Secure and privacy-preserving orchestration and delivery of fog-enabled iot services," *Ad Hoc Networks*, vol. 82, pp. 113–125, 2019.

[64] B. Mukherjee, R. Neupane, and P. Calyam, "End-to-end Iot security middleware for cloud-fog communication," in *Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 151–156, 2017.

[65] Y. Li, S. Chen, C. Zhao, and W. Lu, "Layered data aggregation with efficient privacy preservation for fog-assisted Iot," *International Journal of Communication Systems*, vol. 33, no. 9, p. 4381, 2020.

[66] W. B. Daoud and M. S. Obaidat, "Tacrm: trust access control and resource management mechanism in fog computing," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 28, 2019.

[67] N. K. Giang, M. Blackstock, R. Lea, and V. C. M. Leung, "Developing iot applications in the fog: a distributed dataflow approach," in *Proceedings of the 2015 5th International Conference on the Internet of Things (IOT)*, pp. 155–162, Seoul, South Korea, October 2015.

[68] M. Zhanikeev, "A cloud visitation platform to facilitate cloud federation and fog computing," *Computer*, vol. 48, no. 5, pp. 80–83, 2015.

[69] T. N. Gia, M. Jiang, A. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare internet of things: a case study on ecg feature extraction," in *Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 356–363, Liverpool, UK, October 2015.

[70] D. Zeng, L. Gu, S. Guo, Z. Cheng, and S. Yu, "Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded systemfined embedded system," *IEEE Transactions on Computers*, vol. 65, no. 12, pp. 3702–3712, 2016.

[71] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: a green computing paradigm to support iot applications," *IET Networks*, vol. 5, no. 2, pp. 23–29, 2016.

[72] M. A. Hassan, M. Xiao, Q. Wei, and S. Chen, "Help your mobile applications with fog computing," in *Proceedings of the 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops)*, pp. 1–6, Seattle, WA, USA, June 2015.

[73] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 1202–1207, Ottawa, Canada, May 2015.

[74] S. Ningning, G. Chao, A. Xingshuo, and Z. Qiang, "Fog computing dynamic load balancing mechanism based on graph repartitioning," *China Communications*, vol. 13, no. 3, p. 156, 2016.

[75] C. MacGillivray, L. Lamy, R. Segal, and M. Torchia, *Idc Futurescape: Worldwide Internet of Things 2017 Predictions*, IDC, Framingham, MA, USA, 2016.

[76] A. V. Dastjerdi and R. Buyya, "Fog computing: helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[77] S. Singh, I. Chana, and R. Buyya, "Star: sla-aware autonomic management of cloud resources," *IEEE Transactions on Cloud Computing*, p. 1, 2017.

[78] S. Mustafa, K. Bilal, S. U. R. Malik, and S. A. Madani, "Sla-aware energy efficient resource management for cloud environments," *IEEE Access*, vol. 6, pp. 15004–15020, 2018.

[79] Y. Wang, Q. He, D. Ye, and Y. Yang, "Formulating criticality-based cost-effective fault tolerance strategies for multi-tenant service-based systems effective fault tolerance strategies for multi-tenant service-based systems," *IEEE Transactions on Software Engineering*, vol. 44, no. 3, pp. 291–307, 2018.

[80] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, "A qos-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems," *World Wide Web*, vol. 23, no. 2, p. 1275, 2019.

[81] J. Bi, H. Yuan, M. Tie, and W. Tan, "Sla-based optimisation of virtualised resource for multi-tier web applications in cloud data centres," *Enterprise Information Systems*, vol. 9, no. 7, pp. 743–767, 2015.

[82] H. Shah-Mansouri and V. W. S. Wong, "Hierarchical fog-cloud computing for iot systems: a computation offloading

game," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3246–3257, 2018.

[83] I. Stojmenovic and S. Wen, "The fog computing paradigm: scenarios and security issues," in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, pp. 1–8, Szczecin, Poland, September 2014.

[84] J. Li, J. Jin, D. Yuan, M. Palaniswami, and K. Moessner, "Ehopes: data-centered fog platform for smart living," in *Proceedings of the 2015 International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 308–313, Sydney, Australia, November 2015.

[85] A. Dasgupta and A. Q. Gill, "Fog computing challenges: a systematic review," in *Proceedings of the Australasian Conference on Information Systems*, Hobart, Australia, December 2017, https://aisel.aisnet.org/acis2017/79.

[86] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2227–2241, 2017.

[87] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 Workshop on Mobile Big Data*, pp. 37–42, New York, NY, USA, June 2015.

[88] L. M. Vaquero and L. Rodero-Merino, "Finding your Way in the Fogfinition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[89] A. Aijaz, M. Dohler, A. H. Aghvami, V. Friderikos, and M. Frodigh, "Realizing the tactile internet: haptic communications over next generation 5g cellular networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 82–89, 2017.

[90] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "5g-enabled tactile internet," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 460–473, 2016.