Received September 24, 2019, accepted October 3, 2019, date of publication October 15, 2019, date of current version October 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2947542

A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues

KARRAR HAMEED ABDULKAREEM[1], MAZIN ABED MOHAMMED[2], SARASWATHY SHAMINI GUNASEKARAN[3], MOHAMMED NASSER AL-MHIQANI[4], AMMAR AWAD MUTLAG[5], SALAMA A. MOSTAFA[6], NABEEL SALIH ALI[7], AND DHEYAA AHMED IBRAHIM[8]

[1]College of Agriculture, Al-Muthanna University, Samawah 66001, Iraq
[2]College of Computer Science and Information Technology, University of Anbar, Anbar 31001, Iraq
[3]College of Computing and Informatics, Universiti Tenaga Nasional, Selangor 43000, Malaysia
[4]Information Security and Networking Research Group (InFORSNET), Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Durian Tunggal 76100, Malaysia
[5]Biomedical Computing and Engineering Technologies (BIOCORE) Applied Research Group, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Durian Tunggal 76100, Malaysia
[6]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor 86400, Malaysia
[7]Information Technology Research and Development Centre, University of Kufa, Kufa 54003, Iraq
[8]Computer Engineering Techniques Department, Imam Ja'afar Al-Sadiq University, Baghdad 54003, Iraq

Corresponding author: Mazin Abed Mohammed (mazinalshujeary@uoanbar.edu.iq)

This work was supported by the Universiti Tenaga Nasional under Internal Research Grant OPEX type: RJO10436494-iRMC.

ABSTRACT Systems based on fog computing produce massive amounts of data; accordingly, an increasing number of fog computing apps and services are emerging. In addition, machine learning (ML), which is an essential area, has gained considerable progress in various research domains, including robotics, neuromorphic computing, computer graphics, natural language processing (NLP), decision-making, and speech recognition. Several researches have been proposed that study how to employ ML to settle fog computing problems. In recent years, an increasing trend has been observed in adopting ML to enhance fog computing applications and provide fog services, like efficient resource management, security, mitigating latency and energy consumption, and traffic modeling. Based on our understanding and knowledge, there is no study has yet investigated the role of ML in the fog computing paradigm. Accordingly, the current research shed light on presenting an overview of the ML functions in fog computing area. The ML application for fog computing become strong end-user and high layers services to gain profound analytics and more smart responses for needed tasks. We present a comprehensive review to underline the latest improvements in ML techniques that are associated with three aspects of fog computing: management of resource, accuracy, and security. The role of ML in edge computing is also highlighted. Moreover, other perspectives related to the ML domain, such as types of application support, technique, and dataset are provided. Lastly, research challenges and open issues are discussed.

INDEX TERMS Fog computing, machine learning, Internet of Things (IoT), applications.

I. INTRODUCTION

The Digital Age has experienced a rise in the daily utilize of intelligent devices and computers by organizations and individuals [1]. Electronic devices are used to generate data through applications and sensors. Consequently, many organizations must assume the responsibility of regularly storing huge amounts of data [2]. At present, a dynamic information technology infrastructure is required by organizations due to the shift to cloud computing, which provides advantages in terms of scalability, accessibility, and pay-per-use features. Cloud computing has made available different types of common services, such as Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS)—all of which are heading toward "Anything" as a Service [3].However, certain big data generated by sensors cannot be transferred to and processed by cloud. Moreover, faster processing is required by several Internet of Things (IoT) applications, but current cloud capability will be unable to process such applications. This problem is solved using the fog computing paradigm, in which the processing power of devices close to a user (i.e., idle

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Alawneh.

computing power) is harnessed to facilitate storage, networking at the edge, and processing [4]. Diverse goals perform via Fog computing such as efficiency improvement, data size-reduction that required to be transported to the cloud in multi-purposes of data like data processing, analysis, and storage. This is often done for performance causes, but it may also be carried out for security and compliance reasons [5]. Recently the AI algorithms are introduced into the IoT data analytic procedures [6]–[8].

A low layer network exhibits many undesirable features, such as an inadequate onboard memory, an unreliable low-bandwidth communication network, and processing power and heterogeneous hardware that are dissimilar to the cloud infrastructure [9]. Computing technologies in different areas, such as artificial intelligence (AI), GPU computing, cloud computing, and other hardware enhancements, have advanced in the last decade [10], with machine learning (ML) being regarded as the most popular AI algorithm used in various fields. In several previous studies, researchers have examined how ML can be used to solve networking problems, such as resource allocation, routing, security, and traffic engineering [11]–[15]. Accordingly, ML plays as a key technology in autonomous intelligent/smart environment concerning management and operation aspects.

Furthermore, the relevance of ML extends to IoT, because without ML, IoT will not be possible regardless of whether it is used to perform functional (e.g., routing), monitoring (e.g., anomaly detection), or preprocessing tasks. Thus, discussing ML within the context of fog, cloud, and edge computing for distributing and implementing IoT applications is important [16]. However, in high-level fog nodes, Weka [17] and Scikit-learn [18], are different libraries and frameworks that can be used to implement numerous AI applications. The implementation of capabilities to analyze data found on network devices like routers and switches is easy using current technologies, such as Cisco's IOS XR. An investigation of ML was conducted within the context of actuators, sensors, and low-level fog nodes [19]. ML is used to execute and optimize functional tasks, such as clustering, routing, duty-cycle scheduling, data aggregation, and medium access control (MAC) [20].

The management of relevant processes in fog nodes is difficult because the majority of these processes are rapidly evolving into complex, heterogeneous, and dynamic structures. Moreover, fog nodes services should be improved concerning diversity and efficiency to engage more users. In many previous researches, ML has been successfully applied to fog computing paradigm; hence, fog computing (node-server) can benefit from ML in various ways. For example, deep analytics can be obtained by beneficiaries through the application of ML to fog computing. Meanwhile, efficient intelligent fog computing applications can be developed because feasible solutions can be provided by ML. These solutions enable the mining of information and features hidden in captured data.

In this work, different major contributions are summarized as follows.

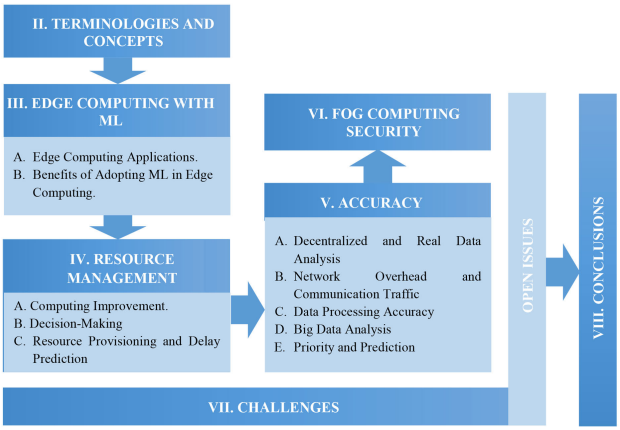

FIGURE 1. Review methodology.

TABLE 1. Fog computing characteristics.

Feature	Description
Heterogeneity	Located at the edge of a network with rich and heterogeneous end-user support.
Capability	Supports a wide range of industrial applications due to its instant response capability.
Storage and Services	Has its own computing, storage, and networking services.
Operation Areas	Operates locally (single hop from a device to a fog node).
Platform	Has a highly virtualized platform
Additional Features	Offers inexpensive, flexible, and portable deployment in terms of hardware and software.

- We review studies that adopted ML to address each of resource management, accuracy, and security problems in fog computing paradigm.
- We highlight the ML role in some of edge computing applications
- The challenges and open issues are discuss in fog computing concerning resource management, accuracy, and security.

The remaining article sections are presented in detail in Figure 1.

II. TERMINOLOGIES AND CONCEPTS

Cisco considered as a pioneers in deploying the fog computing model through which cloud platform is extended and brought closer to the devices of end users. In this manner, various issues, such as latency sensitivity, geographical distribution support, and quality-of-service (QoS)-aware IoT applications [21], are solved. Fog computing is a novel paradigm through which the cloud platform model is extended by using network edges to back up computing resources. Similar to the cloud platform, fog computing provides data storage and application services [22].

A fog system has several features as listed in Table 1 [23].

In addition to the features listed in Table 1, different aspects distinguish a fog system from cloud computing, and each

TABLE 2. Fog versus cloud computing in different aspects.

Aspects	Fog Computing vs. Cloud Computing
Resources	A fog system will have relatively smaller computing resources (e.g., memory, processing, and storage) than a cloud system, but the resources can be increased on demand.
Capability	Both can process data generated from a diverse set of devices.
Distribution Strategies	Both can be densely or sparsely distributed on the basis of geographical location.
Connectivity	Both support machine-to-machine communication and wireless connectivity.
Flexibility	A fog system can be installed on low specification devices, such as switches and Internet protocol cameras.
Usability	One of their primary uses is currently for mobile and portable devices.

feature has its advantages and disadvantages. Table 2 presents several popular aspects [24]–[26].

The terms ''fog computing'' and ''edge computing'' are used interchangeably in industry and academia. In this paper we discriminate between two mentioned terms. Although they serve the same purpose, namely, to decrease network congestion and end-to-end delay, the difference between fog computing and edge computing is the manner in which data are processed and handled and the locations of computing power and intelligence power. In other word, the major difference between the two is that fog computing is decentralized, (i.e. It does not involve centralized computing). Briefly, the processing and storage of data are performed in a decentralized computing architecture between the source and the cloud infrastructure [22]. The central concept of edge computing involves ''pushing'' a computation facility toward data sources, such as mobile devices, sensors, and actuators [27], [28]. Edge components play individual roles in processing data locally, instead of sending them toward the cloud. Meanwhile, the decision regarding whether to process data from multiple sources or send them to the cloud is made by a fog node, which uses its resources to make such decisions. Moreover, edge computing does not offer any support to many services, such as SaaS, IaaS, PaaS, and other cloud-related services. By contrast, fog computing supports all these services. In summary, edge computing [27]–[29] is entirely edge localized, but communication and computing resources are extended toward a network's edge see figure 2.

III. EDGE COMPUTING WITH ML

In IoT systems, edge networks, equipment, and sensors are found throughout the network. Requirements for bandwidth, latency, and network security are imposed on many IoT applications. However, cloud computing fails to meet these requirements. An existing technology that can fulfill such requirements is edge computing [30]. For example, virtual

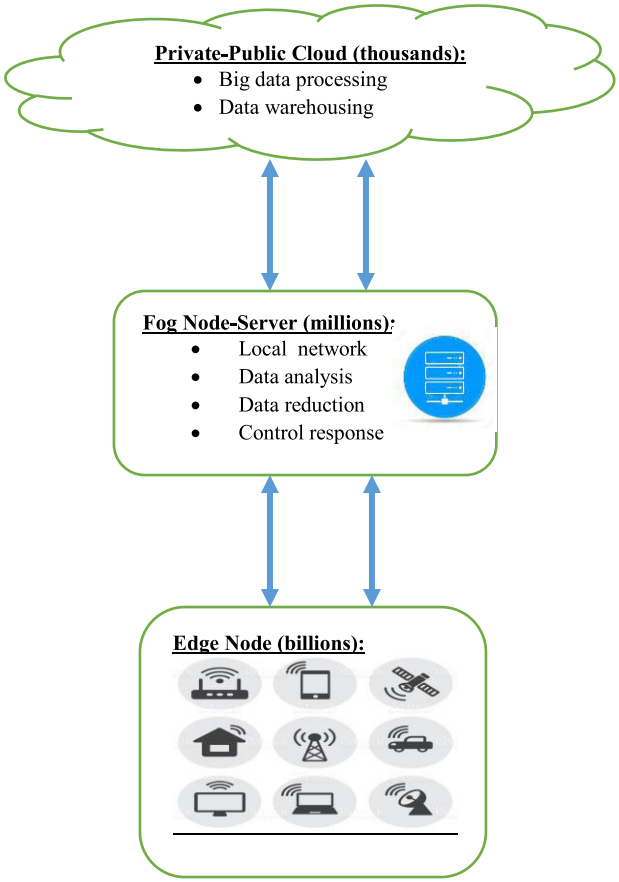

FIGURE 2. Cloud, fog, and edge computing.

reality and augmented reality apps that necessitate high bandwidth can procure contents from an edge network; in another example, data commutation by vehicles can be achieved through edge networks, and vehicles on a road move in a coordinated manner to enhance user proficiency [31]. The model of the edge computing issue in IoT networks is shown in Figure 3. The model allows the analysis of data from traffic and sensors. Many methods have been used in ML to classify data obtained from the features extracted from data sources. The utilization of results can be monitored in intrusion detection, disease identification, recognition of imaging, and traffic engineering. Thus, Table 3 provides an illustration of the studies reviewed in this work.

A. EDGE COMPUTING APPLICATIONS

A new framework that involved a number of wearable devices was proposed in Borthakur at al. [32]. These authors recommended the use of edge computing devices although these devices have fewer resources. In addition, they provided a description for a proposed novel telehealth computing architecture that involved decentralized services at an edge network. Apart from speech signal recognition algorithms used in telehealth monitoring, Parkinson's disease was recognized using k-means clustering. Similarly [33] proposed a PreCog system that recognizes images rapidly through catching and prefetching on edge devices. The proposed system comprises

TABLE 3. Current ML-based edge computing studies.

Reference	Problem	Technique	Data/Signal	Accuracy (%)
[32]	Parkinson's disease Identification in edge computing	Clustering approach	Speech data	-
[33]	Image recognition in edge networks	Markov model	Image dataset	90
[34]	Arrhythmia detection	Support vector machine (SVM)	ECG of patients	93.6
[35]	Parking availability evaluation	Cascade classifier	Video captured by a smartphone	-
[36]	Service recommendation in mobile edge computing	Collaborative filtering	User mobility information	64.4
[37]	Anomaly detection	SVM	Sensor data	90
[38]	Anomaly detection	Federated learning	Sensor data	95–98
[39]	Distributed attack detection	DL approach	Traffic data	92
[40]	Privacy protection during data aggregation	Linear regression technique	Sensor data	90
[41]	Traffic engineering	Bayesian network technique	Path latency traces	80–90

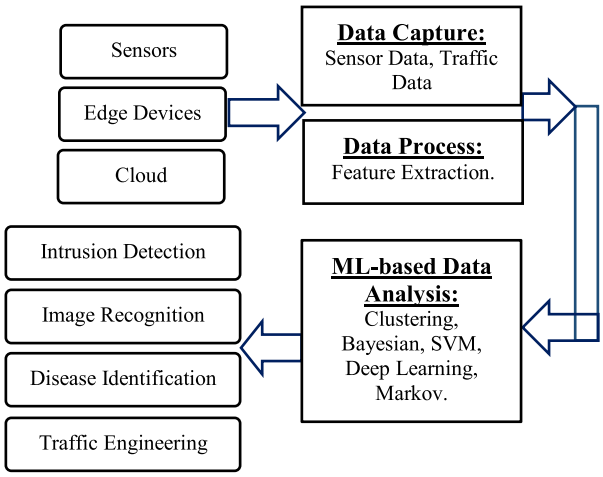

FIGURE 3. Role of ML in edge computing.

multi-parts that collaborate with the system (i.e., edge server, cloud server, and devices). PreCog utilizes computing resources on the devices as well as the cloud server because of the complexities involved in computing and the bulk of the data included in image recognition. This process differs from the aforementioned edge computing solutions that involve completing computing activities on the edge server.

A recognition cache is used by the edge server and the devices to store important parts of the proposed model. Furthermore, the devices prefetch a fraction of the trained classifiers that are set to be utilized subsequently; a HiCH which stand for a hierarchical computing architecture for an IoT network in healthcare was posited by [34]. Current ML methods in architecture are distributed among separate layers of a fog network. For instance, sensor devices can perform diverse functions such as sensing and monitoring; the cloud is responsible for large training processes, while the edge is in charge of local decision-making and system management.

A system based on IBM's Monitor-Analyze-Plan-Execute-Knowledge model was devised by authors and focused on the detection of arrhythmia. As depicted in the results, HiCH functions were more effective than those of conventional systems in terms of response time, bandwidth usage, and storage despite the acceptable accuracy [34]. A low-budget crowdsourcing architecture, called ParkMaster, was developed by Grassi et al. [35]. ParkMaster is responsible for the visual analytics of appraising parking availability. In contrast with the conventional centralized monitoring system that uses smartphones inside a car, ParkMaster captures a video along a street also compute the number of cars detected after the video processing via using ML approaches. The uploading of the ParkMaster cloud is performed with the results processed from multiple cars. Data are processed, and a parking slot is recommended to each driver. Want et al. [36] conducted a system which aimed to work as a service recommendation that depend on prediction of QoS in a smartphone edge computing settings. In contrast with several context-aware service recommendation systems, the suggested system considers mobility. It then endorses services to other users with the aid of collaborative filtering algorithms on the basis of mobility information. As depicted by the results of a series of experiments using data from Shanghai Telecom, high prediction accuracy could be achieved by the new system.

B. BENEFITS OF ADOPTING ML IN EDGE COMPUTING

In [37], Zissis presented an intelligent intrusion detection system to obtain the core of edge computing infrastructure. The conventional ''self-protecting'' system developed by IBM was improved using this system. The proposed IDS smartly identifies anomalies in devices that can be detrimental to the entire system by collecting data from sensors while utilizing the newest unsupervised ML approach. Lastly, evidence that the concept system developed by [37] the author(s) can detect incongruities in the real world was found.

Another system for detecting anomalies in edge computing environments was established by Schneible et al. [38] by integrating simulated neural networks. The presented model are assembled in a particular place (for instance the centralized cloud) in a conventional neural network. Latencies and congestions are observed near the travel path due to this feature. The core of the new system is federated learning,

during which the training data are divided among the edge devices and a duplicate training model is stored by each edge device. Then, the training results derived from the edge devices are computed by the centralized cloud repository. Enhanced bandwidth, latency, and full usage of computation power via edge networks can be achieved through the federated learning mechanism. The problems in distributed attack detection were further investigated by Abeshu and Chilamkurti [39] and then compared with those in nondistributed attack detection. Such investigation is more challenging to perform. The mechanisms of traditional ML are considered to exhibit lower precision and less scalability in edge computing environments because of the complexities of and variation in devices. A new scheme based on deep learning (DL) proposed by [39] has gained popularity because of GPU hardware improvement and deep neural network theory. As shown by the results, the DL-based mechanism is superior to conventional approaches. Apart from security concerns, another crucial aspect of the fog computing environment is privacy. A privacy protection mechanism based on ML was proposed by Yang et al. [40] for computing data concerning sensors and devices in a fog computing architecture. The proposed approach is supported by this new mechanism; hence, many data sources can be accepted. In addition, the distribution of computationally huge tasks to the network edge is achieved by the system; thus, the system is more scalable than a centralized system. As indicated by the experiment results, high precision is achieved by the system without compromising user privacy. An explanation for traffic engineering in edge networks was provided by Hogan et al. [41]. Manifold end-to-end paths may subsist in edge networks with each path having separate delay and bandwidth. However, the choice was mentioned is one that perfectly suits users' requirements is of utmost concern. The proposed study provided a solution by computing the results on the basis of portfolio theory, maximizing the expected return, and considering the level of risk (i.e., representation of the expected throughput the lifetime). Considering the model, ML was used by the [41] to appraise the risk level for each path. Finally, the suggested solution was compared with other methods using real-world latency traces. Improved performance was achieved as predicted by the solution.

IV. RESOURCE MANAGEMENT IN FOG COMPUTING

Various types of fog computing devices, sensors, and objects are available, and all of them produce a huge amount of data that require processing. Real-time processing may be necessary in certain situations. Devices, sensors, and objects will fully utilize resources by making requests [42]. Hence, resource management is required in fog computing and should be carefully implemented [43]. In this section, we reviewed studies that used ML in fog computing resource management.

A. COMPUTING IMPROVEMENT

The authors of [9] presented a balanced and faster computation at a network's edge to prevent sending raw data to the cloud through Edge SGD, a decentralized ML algorithm; a large linear regression problem at the edge of a network is solved through this computation. Similarly, a novel IoT-based approach was proposed in [44] by considering a local paradigm that supports ML algorithms while automating the management of the system's components in the computing section. In [45], ML algorithms were implemented in cloud servers to recognize and understand music and write the score automatically using ML methods. The authors adopted the proposed architecture to achieve an efficient allocation of computing resources. To solve the problem of big data, the authors of [46] used DL by shifting the computational burden from the central server to the fog nodes. Their results showed that their proposed system is capable of processing big data. Similarly, an algorithm for data distribution was introduced in [47] for floating car data (FCD). Its design enables the proposed algorithm to be immune to the problem of backhaul connectivity, and thus data loss can be avoided during periods of connectivity outage. In addition, distributed data modeling in the fog is favored by the design of the algorithm; that is, the design allows the feeding of data collected by the data distribution algorithm to a distributed set of conditional restricted Boltzmann machines (CRBMs). In [48], wavelength transform and principal component analysis (PCA) were used in compressed learning to convert mid-infrared spectroscopy (MIRS) data into compressed data. Fog computing and big data processing can benefit considerably from compressed learning with MIRS because they support the preservation of computation and communication energy, the reduction of application latency, the minimization of the required memory and storage spaces, and the preservation of scarce rural network bandwidths. Cognition-based communications, which originate from communication advancements and AI-based computing, were proposed in [49]. Network analytics, such as cognitive analytics in a network and a networking problem, were also provided by implementing ML. In their work, network application is inclusive of the allocation of resources for virtualized networks and energy-efficient network operations. Similarly, the authors of [50] exerted effort to reduce energy consumption and latency in fog computing by using ML to detect user behavior and provide low-latency adaptive MAC-layer scheduling among sensor devices. A HiCH was proposed in [34] for IoT-based health monitoring systems. Hierarchical partitioning can be performed by using the proposed computing architecture while ML-based data analytics is executed. Table 4 provides a summary of studies that used ML to enhance computing.

In conclusion, supervised ML techniques (particularly classification) have been mostly used in time-critical and healthcare applications, while unsupervised ML techniques, (particularly clustering) have been used in diverse IoT applications, such as smart farming and traffic. The primary objective of implementing supervised and unsupervised ML is to improve the role played by fog computing at a network's edge. The majority of the problems highlighted in Table 4 exhibit an association with the improvement of computing

TABLE 4. Studies that used ML to enhance computing.

Reference	Problem	Technique	Data	Application
[9]	Edge device communication	Supervised (linear regression)	Real-world seismic data traced from Parkfield, California	Seismic imaging
[44]	Continuous and real-time patient monitoring	Supervised (classification - SVM)	Data provided in Physiobank as "The Long-term ST Database" and ECG with arrhythmia in the middle of a normal ECG signal.	Healthcare–patient monitoring
[45]	Automatically generates musical score from a huge amount of music data in an IoT network	Unsupervised (clustering - hidden Markov model)	Audio files or record audio signals in real time	Music cognition
[46]	Large amount of IoT sensor data adopted in industrial productions	DL	A total of 10 categories, each of which has 200 images for the training process and 50 test images for network testing.	Smart industry
[47]	Centralized data processing	Unsupervised (density estimation - CRBMs)	One week of FCD generated in Barcelona City	Traffic modeling
[48]	Centralized data processing	Unsupervised (clustering - PCA)	MIRS dataset	Smart dairy farming
[49]	higher Quality of Experience (QoE), and higher energy e□ciency for users' applications demands	Cognition-Based Communications	Real-Time data flows in the network environment	User-Centric Cognitive Communications, and Cognitive Internet of Vehicles
[50]	Energy efficiency and latency requirements for time-critical IoT	Supervised (classification - SVM, decision tree, and Gaussian naïve Bayes)	Sensor data from real human subjects	Time-critical IoT applications
[34]	Accuracy and adaptability of data analytics on the edge of a network	Supervised (classification - SVM)	"Long-term ST Database"	Health monitoring systems

related to the problems of edge device communication, accurate and energy-efficient edge computing, and centralized computation.

B. DECISION-MAKING

SmartFog was proposed in [51]. It demonstrates low-latency decision-making and adaptive resource management through a nature-inspired fog architecture. The function of the human brain can be emulated using ML through SmartFog. The authors of [52] focused on situational awareness and the selection of an optimal path by combining ML with a Markov logic network. Using the proposed directional mesh network (DMN) framework, time-sensitive signal data are analyzed near the signal source through diverse ML techniques. Similarly, the fog device can make a ''smart'' decision regarding when the data should be uploaded to cloud back end and when not to. This decision is achieved with the aid of low-resource ML on fog devices found near wearables for smart telehealth. ML techniques were used in the Smart Cargo concept in [53]. The aim of applying ML was to allow the evolution of cognition over time by means of decisions made during various events. Table 5 presents related studies that were reviewed in this work. In these studies, the authors improved decision-making in a fog computing environment using ML.

From Table 5, we can conclude that most of the studies used unsupervised ML techniques (particularly clustering) and no supervised ML technique was used. Moreover, unsupervised ML techniques have been used to enhance the decision-making ability of fog computing. Most of the problems addressed are concerned with computation loads with limited resources and unexpected situations.

C. RESOURCE PROVISIONING AND DELAY PREDICTION

The authors of [54] proposed an optimum resource provisioning of the distribution and parallelization aspects of an edge-based DL framework using off-the-shelf components. Considering these aspects, the resources required by applications are analyzed. These resources include processing speed and memory for optimum resource utilization. Similarly, the authors of [55] focused on provisioning of resources in multimedia fog computing. They proposed an efficient algorithm based on sophisticated ML algorithms. The primary function of this algorithm is predicting the available resources of fog devices. However, it can also perform other tasks, such as verifying the accuracy of the rendered results and optimizing the extent of replicated job assignments. Meanwhile, the authors of [56] focused on proactive network association and open-loop wireless communication through ML; anticipatory mobility management is enabled in this study. Another study [57] was conducted to predict end-to-end delay, such as the total amount of time used from the processing to the transmission of data, along with link utilization for different workloads related to image processing [57]. The authors created a realistic fog computing sandbox using an image processing ensemble of services in GENI infrastructure. In [58], the authors solved the energy and communication problems between end devices with limited resources by proposing Message Queuing Telemetry Transport, the standard IoT communication protocol. Real sensor measurements were predicted using four types of ML algorithm. Meanwhile,

TABLE 5. Studies on the improvement of decision-making.

Reference	Problem	Technique	Data	Application
[51]	Unpredictable load patterns of distributed IoT applications	Unsupervised (clustering - spectral clustering)	Based on simulated iFogSim data	IoT network or applications
[52]	Limited radio spectrum resources	Unsupervised (clustering - PCA)	----	DMN
[53]	Real-time response to detected unexpected situations	-----	Smart Cargo scenario	Smart Cargo

TABLE 6. Studies on resource provisioning and delay prediction.

Reference	Problem	Technique	Data	Application
[54]	Latency of analyzing large amounts of data	DL	Triaxial accelerometer data for activities of daily living	Smart city
[55]	Predicting the completion time of each rendering job	Supervised (classification - random forest, gradient boosting tree, SVM)	Render five jobs using a real fog rendering service	Animation rendering
[56]	Ultralow latency mobile networking for AVS	Supervised (classification - naïve Bayesian classifier)	A taxi dataset consisting of 12,000 vehicles running over 1 month	Mobile network
[57]	Network quality, accuracy, and operational overhead	Supervised (regression)	700 instances of transmission dataset and 1600 instances of processing dataset	Image processing service
[58]	Energy of end devices, communication among resource-constrained devices	Supervised, neural network, decision tree - linear regression	Public dataset that contains measurements taken from a combined cycle power plant	Industry 4.0 factories
[59]	Energy consumption of centralized data processing		Data acquired by CC2650 TI Sensor Tag	Environment measurement (accelerometer, gyroscope, magnetometer, thermometer, hygrometer, and barometer).

the authors of [59] demonstrated that energy consumption can be reduced by selecting a valid combination of layers to implement various steps of ML techniques. Different steps are involved in ML techniques used in ubiquitous computing applications; these steps can be implemented in various layers. Table 6 describes studies that used ML to predict processing delay and provide resources in fog computing.

From Table 6, a conclusion can be drawn that none of the studies used unsupervised ML techniques. Instead, supervised ML techniques (particularly classification) were used. Enhancing resource provisioning, delay prediction, and energy consumption in fog computing is the primary objective in using supervised ML techniques. The problems addressed were related to resource provisioning, delay prediction, and energy consumption concerning latency and predicting computation completion time, operational overhead, and energy consumption.

V. ACCURACY IN FOG COMPUTING

Accuracy issues are improved through fog computing because its senses, processes, and presents information in real time. Therefore, fog computing frequently uses data that reflect of real-time situations [60]. ML techniques contribute significantly to inaccuracy issues [61]. The combination of fog computing and ML techniques can solve the accuracy problem, particularly at the edge of a network. The major issue that researchers are focusing on is enhancing the accuracy of fog computing by implementing ML techniques as shown in Figure 4.

A. DECENTRALIZED AND REAL DATA ANALYSIS

In [62], the primary objective of the authors was exploring accuracy against traffic trade-off. They proposed a distributed hypothesis transfer learning (HTL) with the assumption that data are moved to a variable number of data collectors where

TABLE 7. Previous studies that focused on solving the problem of analyzing decentralized and real data.

Reference	Problem	Technique	Data	Application
[62]	Knowledge extraction from raw IoT data	Supervised (classification - SVM)	10,000 records	Human activity recognition
[63]	Processing large amounts of data at an edge network		205 parturient women diagnosed with a hypertensive disorder during pregnancy	Healthcare
[64]	Processing huge amounts of data	Supervised (classification - SVM)	19,229 points (≈ 2700 points per class) of forest area	Smart cities and factories
[65]	Handling massive amounts of real-time data streams	DL	----------	IoT network

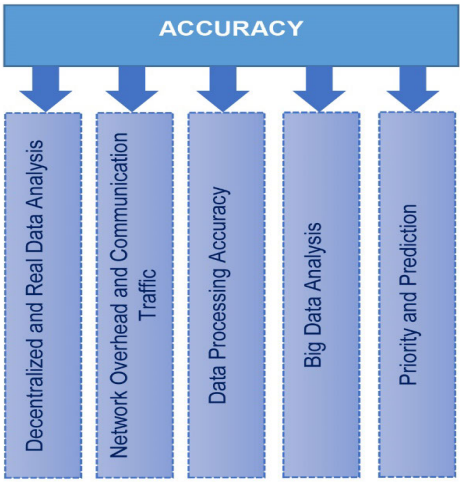

FIGURE 4. Major issues in accuracy.

partial learning is performed. In [63], the authors intended to solve the issue related to the processing of large amounts of data close to the edge of a network. They proposed an ML technique, referred to as one-dependence estimators, for the real-time analysis of pregnancy data obtained from IoT devices and gateways. In [64], the authors improved the processing of large data generated from smart industries and cities. They used a popular distributed ML framework (i.e., HTL) and analyzed data on mobile nodes passing through IoT devices and fog gateways at the edge of network infrastructure. In another study conducted by the same authors [65], DL was adopted to explore how large amounts of real-time data streams generated from cyber-physical systems (CPS) can be handled by edge analytics and cloud and fog computing. To elucidate previous studies that used ML to solve the problem of analyzing decentralized and real data, Table 7 summarizes associated problems, techniques, data, and apps.

Only supervised ML techniques, particularly classification (SVM), were used in these studies based on Table 5. Supervised learning and DL have been applied in various ways to improve decentralized and real-data analysis in fog computing in terms of knowledge extraction and processing huge amounts of data in real time.

B. NETWORK OVERHEAD AND COMMUNICATION TRAFFIC

In [66], the authors focused on computation speed because of the amount of in-the-wild aging data. They proposed a highly efficient age estimation system combined with the joint optimization of an age estimation algorithm and a DL system. Such combination was presented with the architecture of three-tier fog computing, which includes fog, edge, and cloud layers. In [67], the authors addressed network latency and bandwidth problems. A universal healthcare framework, known as UbeHealth, was proposed. Network traffic is predicted using big data, deep learning, and high-performance computing. The results are used by the cloudlet and network layers to optimize data rates, routing decisions, and data caching. Similarly, the authors of [68] proposed a distributed learning framework that involves performing partial data analytics directly on nodes that are responsible for generating data or nearby ones through distributed ML techniques. In [69], the authors aimed to solve the problem of detecting and processing at the sensor level. An early warning system was proposed to facilitate the detection of wild animals close to a railway or road such that oncoming vehicles can be alerted about possible crossing animals. Images captured at the edge of devices can be classified using ML. Moreover, ML supports the prediction of different time-varying traffic profiles. Table 8 summarizes related studies that use ML to overcome network overhead and communication traffic in fog computing.

From Table 8, DL and supervised ML techniques (particularly classification) were adopted to solve network overhead and communication traffic problems in fog computing, such as computation speed with low network bandwidth and detection problems in huge amounts of data. DL and supervised ML techniques were used in IoT applications, such as smart cities and healthcare.

C. DATA PROCESSING ACCURACY

The authors of [70] proposed a new in-network self-learning algorithm that can be used in a building energy management system through a collaborative fog platform to improve data processing results. This new algorithm can facilitate

TABLE 8. Studies relevant to overcoming network overhead and communication traffic.

Reference	Problem	Technique	Data	Application
[66]	Computation speed	DL	IMDB-WIKI and AgeDB datasets	Age estimation
[67]	Bandwidth and network latency	DL	ISPDSL-II, Waikato-VIII, and Wide-18 datasets	Healthcare
[68]	Processing huge amounts of data	Supervised (classification - linear and learning SVM)	HAPT and MNIST datasets	Smart cities
[69]	Detection and processing	(Supervised - classification)	Generate a set of traffic data samples using lognormal distribution	Movement of animals to warn humans

TABLE 9. Studies relevant to data processing accuracy.

Reference	Problem	Technique	Data	Application
[70]	Data processing and communication volume	Supervised (classification - nearest neighbor)	48 temperature sensors in a single floor with an area of 1400 m^2	Energy-efficient environment
[71]	Emotion recognition and interaction experience	DL (VGG-Net and Alex-Net)	Tests of facial expression recognition concurrency from 1 to 60 times and speech emotion recognition concurrency from 1 to 35 times	Human–machine interaction application

the reduction of the total data processing/communication volume required in entire IoT networks. In [71], two DL algorithms, called Alex-Net and VGG-Net, were presented for speech emotion and facial expression recognition, respectively. A new AI-enabled affective experience management (AIEM) was proposed. The composition and architecture of this AIEM were based on three aspects: the accurate management of emotion recognition, the intelligent management of emotion data collection, and the real-time management of emotion interaction. Table 9 summarizes related studies that use ML to enhance data processing accuracy in fog computing.

Table 9 shows that DL and supervised ML techniques (particularly classification) have been applied to improve data processing accuracy in fog computing in terms of communication volume and recognition problems. IoT is the foremost significant application.

D. BIG DATA ANALYSIS

In [72], an innovative system based on cloud and fog computing technologies combined with big data platforms and IoT was proposed. In this study, novel opportunities for the provision of new and innovative services were provided to address the problem of sleep apnea while overcoming the present shortcomings. The characteristics of the ML module were furnished with the MLlib, Apache SparkSQL, and Scikit-learn 0.18.0 libraries described in the big data analyzer architecture modules. Another framework was proposed in [73] for the early reduction of data from the customer side. This framework also presents a business model for end-to-end data reduction in enterprise applications. The results of this study showed that privacy, trust between enterprises and customers, secure data sharing, and utilization cost were improved. Table 10 presents related studies that used ML to analyze big data in fog computing.

From Table 10, a conclusion can be drawn that supervised ML techniques (classification) and unsupervised ML techniques (dimensionality reduction) have contributed significantly to big data analysis, which a key problem in fog is computing. Big data reduction and real-time preprocessing are the major problems addressed in medical care and sustainable enterprises.

E. PRIORITY AND PREDICTION

In [74], a framework for cyber-healthcare and its implementation were introduced. The framework, which is fog-based with a multilayer architecture, focuses on a patient's condition recognition system that uses ML techniques as a major constituent of the framework. To support the handling of complex data in terms of speed, variety, and latency, the researchers in [75] introduced a patient-centric IoT e-health ecosystem with a multiplayer architecture that consists of (1) a device, (2) fog computing, and (3) cloud. This system is based on hierarchical temporal memory (HTM), which is a biologically inspired ML unsupervised intelligence technology. The HTM ML module is fed with the generated sparse

TABLE 10. Related studies that analyzed big data.

Reference	Problem	Technique	Data	Application
[72]	Preprocessing of IoT data to detect events in real time	Supervised (classification, logistic regression, linear regression)	Steps counter (185 records) Snoring (177 records) Sleep track (185 records) Heart rate (13,450 records) Temperature (13,450 records) Humidity (13,450 records) Weather (4248 records) Pollutants (4248 records)	Medical care
[73]	Big data reduction	Unsupervised (dimensionality reduction)		Sustainable enterprises

TABLE 11. Summary of related studies on prediction and priority problems.

Reference	Problem	Technique	Data	Application
[74]	Recognition of patient's condition	Supervised (regression - multivariate linear regression and multivariate logistic regression; classification - deep neural network and single hidden layer neural network)	Medical record history of patients	Healthcare
[75]	Aging population with chronic diseases	Unsupervised (HTM)		Healthcare

distributed representations. Moreover, GraphLab, which is a scalable and fast ML platform, was used in big data analytics. Table 11 summarizes related studies that used ML to solve prediction and priority problems in fog computing.

As shown in Table 11, supervised (e.g., regression and classification) and unsupervised (e.g., HTM) ML techniques can solve the priority and prediction problems in fog computing. In this section, researchers addressed the problems of healthcare applications in terms of recognizing the condition of patients with chronic diseases.

VI. FOG COMPUTING SECURITY

Users are expected to be provided with secure and reliable services when they use IoT networks; that is, trust should exist among all the devices in a fog network [21]. Cloud or fog is considered a suitable location by data services to analyze and identify which data require a certain action, and thus increase security by making the data anonymous. The prevalence of cyber threats is high in distributed systems, and the tendency of developers to prioritize supporting functional systems before incorporating security features heightens such threats [22]. The security levels of fog computing and the corresponding ML solutions are divided into device security, network security, and data security. Furthermore, we classified the existing literature by highlighting the problem, ML technique, dataset, application, accuracy, and attack type in each article listed in Table 12.

Several authors have proposed approaches associated with the protection of data privacy. Yang et al. [40] used a linear regression algorithm to propose a privacy protection mechanism based on ML. This mechanism can support a variety of data sources because it has a provision for a multifunctional data aggregation method [40]. By using this new mechanism, computationally heavy tasks are distributed to the network's edge to improve the scalability of a system. The experimental results indicated that a high accuracy of 90% was achieved by the proposed system without compromising user privacy. To enhance the efficiency of query evaluation, Zhu et al. [79] applied a neural network, linear regression, boost, ensemble bag, and SVM with differential privacy on simulated and real datasets. Their results demonstrated that the use of a prediction model facilitated the elimination of the mean absolute error and the preservation of data privacy. With a target to provide end-to-end security at the fog layer for IoT devices, in [84] author have presented a novel Fog Security Service (FSS) based on two cryptographic schemes, identity-based encryption, and identity-based signature. Number of services have provided by FSS such as authentication, confidentiality, and non-repudiation. The FSS have evaluated and implemented in an OPNET simulator using a single network topology with different traffic loads. In [85] a novel security ''toolbox'' have proposed, the main goal was to strengthen the integrity, security, and privacy of SCADA-based IoT critical infrastructure at the fog layer.

TABLE 12. Reviewed literature based on several aspects.

Reference	Problem	Technique	Data	Application	Accuracy	Types of attack	Security level
[40]	Data privacy protection	Linear regression algorithm	REDD and MHEALTH	Energy reduction and healthcare systems	90%	Data breaches, data loss	Data security
[76]	Disease prediction and privacy protection	Fuzzy set theory and k-nearest neighbor	Indian Liver Patient Dataset	Healthcare systems	96.74%	Access control issues, data breaches, data loss	Data security
[77]	Disease prediction and privacy protection	Neural network and a privacy-preserving piecewise polynomial calculation	Breast Cancer Wisconsin Dataset	Healthcare systems	97.4%	Data breaches, data loss	Data security
[78]	Ransomware threat detection	Long short-term memory (LSTM) and convolutional neural network (CNN)	Ransomware and goodware samples	Data storage	99.6%	System and application vulnerabilities	Data security
[79]	Data privacy protection	Linear regression, neutral network, ensemble bag, boost, and SVM	Four real case datasets with one simulated dataset	CPS	N/A	Data breaches, data loss	Data security
[37]	Anomaly detection	SVM - supervised learning	Real world vessel sensor data streams	Network monitoring	N/A (90)	Advance persistent threat (APT), denial of service (DoS)	Device security
[80]	Phishing detection	Artificial neural network (multilayer feedforward neural network) and fuzzy logic	Real phishing cases		98.36%	Account hijacking	Device security
[81]	Anomaly detection	Fuzzy C-means clustering and extreme learning machine - unsupervised learning	NSL-KDD dataset	App identification	86.53%	APT, DoS	Network security
[82]	Communication protection	Supervised ML performed in two phases: (i) off- and (ii) online	Own experiment	IoT applications	N/A	Tampering, eavesdropping	Network security
[83]	Intrusion detection	Multilayer Perceptron (MLP)	Australian Defense Force Academy Linux Dataset and Australian Defense Force Academy Windows Dataset.	IoT applications	94% in ADFA-LD and 74% in ADFA-WD	Hydra-FTP, Hydra-SSH, Adduser, JavaMeterpreter, Meter-preter, and Webshell	Network security

The toolbox integrates two key features: on the cloud level a cryptographic-based access approach have used and signature schemes at the fog layer. In terms of evaluation for the proposed work, authors presented a prototype to prove the suitability of the suggested platform in a real-world application.

In summary, the databases of social IoT systems must be protected from cyberattacks. Efficient privacy protection can be achieved using advanced differential privacy approaches that can provide data immunity against vulnerabilities and enhance query evaluation while supporting ML algorithms [77].

With regard to data availability, deep ransomware threat hunting and intelligence system (DRTHIS) was proposed in [78] to facilitate the detection of ransomware while identifying its family within the first 10 s that the application is executed. The proposed system can be deployed on the fog layer to function as a completely automated mechanism of ransomware detection. In DRTHIS, two DL techniques (LSTM and CNN), are commonly used for classification using the softmax algorithm. In the experiments, the DRTHIS was trained using 220 Cerber, 220 Locky, and 200 TeslaCrypt ransomeware samples and 219 goodware samples. The results showed that DRTHIS achieved an F-measure of 99.6% during evaluations and a true positive rate of 97.2% in the classification of ransomware cases.

With regard to suspect surveillance and communication protection, the authors in [37], [80], [81], [83] intrusion detection systems have introduced, using real world vessel sensor data streams and real phishing cases in [37], [80], the accuracy that have is achieved 90% by SVM classifier and 98.4% accuracy for phishing detection using fuzzy logic and multilayer feedforward neural network and. However, [81], [83] used synthetic dataset to evaluate their proposed methods. In the same time the accuracy with 86.53% have achieved on NSL-KDD dataset in [82] and 94% in ADFA-LD and 74% in ADFA-WD in [84], respectively. Finally, in [82] a solution of communication protection have proposed by using a supervised ML that performed in two phases offline and online.

In terms of privacy protection and disease prediction, the authors of [76] used fuzzy k-nearest neighbor–case-based reasoning to develop a privacy-aware disease prediction support system, which is capable of protecting the sensitive information of patients from unauthorized users. Paillier's homomorphic cryptosystem was adopted to fortify the security of the system by encrypting sensitive patient information. An experiment was then conducted using the Indian Liver Patient Dataset. The results showed that high sensitivity, accuracy, and specificity of 90.42%, 99.28%, and 96.74%, respectively, were achieved by the proposed system. Meanwhile, a hybrid privacy-preserving clinical decision support system was developed for use in cloud and fog computing environment. This system was designed based on a neural network, Paillier's encryption with threshold decryption, and another building block that can facilitate the secure monitoring of patients' health condition is real-time settings. The Breast Cancer Wisconsin (Diagnostic) Dataset from the University of California, Irvine ML repository was used in the experiment. The experimental result reported that a prediction rate and an error rate of 97% and 0.2%, respectively, were achieved by the system.

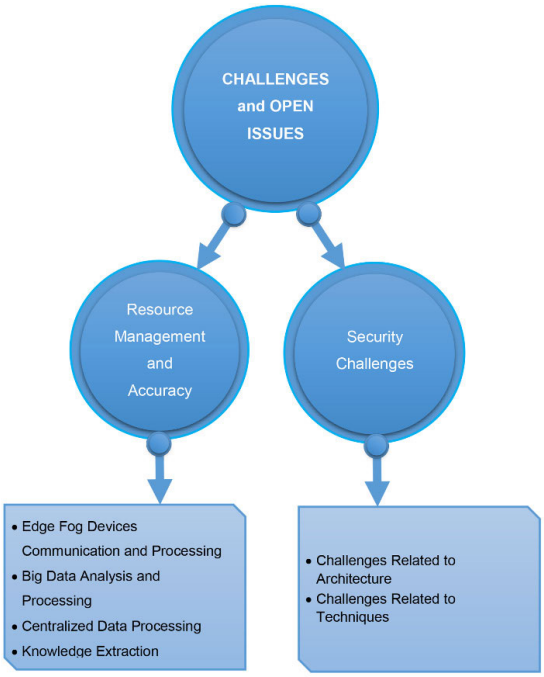

FIGURE 5. Fog computing challenges and open issues.

VII. CHALLENGES AND OPEN ISSUES

In fog computing, different types of data from the edge network environment and heterogeneous sensors comprise data sources. Collected data may consist of several types, including ambiguous and incomplete data, which complicate a system.

Figure 5 lists the challenges in fog computing that are relevant to resource management, accuracy, and security. Additional details are provided in the next subsections.

A. RESOURCE MANAGEMENT AND ACCURACY CHALLENGES

The majority of applications worldwide are facing the challenge of managing data processing at the edge of a network (fog). Although fog computing has overcome many processing problems by providing preprocessing and shifting processing to the edge of a network instead of relying on central processing, various problems in fog computing should still be overcome. ML has contributed considerably to the management of data processing. An appropriate application of ML to fog computing will significantly improve the overall system. Subsequently, we summarize the challenges and open issues in processing and computation management in fog computing.

1) COMMUNICATION AND PROCESSING OF EDGE AND FOG DEVICES

The emergence of fog computing as a novel paradigm has enabled the processing, storage, analytics, and networking of data. Analytics is performed closer to the edge of applications and devices [9]. DL, ML, and AI should be implemented in time-critical applications in fog computing networks to enhance latency, energy efficiency, and reliability requirements in terms of processing and communication issues [50], [67]. Adaptability and accuracy levels may be reduced when data are completely outsourced to a fog network because of the limitation in computational capacity of edge nodes [34]. A fog architecture should be capable of scaling and adapting to overcome the unpredictable loads of distributed applications [51]. The growing number of sensors and data demands increases constraints in communication and energy, and thus produce new challenges that require efficient IoT cloud architectures [58]. Extant DL platforms have limited computational speed, which leads to processing and communication problems, particularly with the increasing amount of in-the-wild data [66]. The energy consumed by edge devices and end-to-end delay can be reduced when processing is performed at the sensor level [69]. Data processing results can be improved significantly by using a self-learning algorithm, and the total data processing/communication volume required in the entire IoT network can be reduced [70]. New opportunities for the development of novel and innovative services can emerge if fog and cloud computing technologies are combined with big data and IoT platforms [72].

2) BIG DATA ANALYSIS AND PROCESSING

A huge amount of data that require processing and analysis are generated by IoT. A major challenge is the lack of cognitive ability and domain knowledge of computers [45]. Moreover, one of the challenges associated with the adoption of numerous sensors is that good performance and processing efficiency are not guaranteed by the existing inspection system [46]. Processing and analyzing large amounts of data at a network's edge, where these data are generated, require real-time data analysis. To perform such an analysis, an ML technique referred to as averaged one-dependence estimators must be implemented. The aforementioned problems can be solved by combining DL with fog computing [54], [63]. The distribution of IoT and personal mobile devices will produce a huge amount of data, and centralized cloud-based analysis will be insufficient and unable to handle that much data [64]. The accurate and scalable extraction of multiscale features in multilevel representation from large-scale unlabeled signals required for the output of the system remains as a major challenge that should be addressed [65]. Big data reduction at a fog network will overcome the problem of processing resources and considerably reduce the cost and energy of using cloud-based analysis [73].

3) CENTRALIZED DATA PROCESSING

Centralized cloud-based processing causes latency. By contrast, real-time data distribution in fog rather than being centralized in cloud contributes substantially to data processing latency, particularly with the use of ML analytics for prediction [47]. Similarly, the transfer of raw data to a centralized cloud for processing is currently infeasible due to the lack of Internet connectivity and the huge amount of data generated from various applications [48]. One of the aforementioned applications is telehealth, in which medical big data are generated. Transferring these big data to cloud is time-consuming and may cause a delay in processing, which is undesirable, particularly for medical data [32]. Energy is another important issue that should be considered in processing data. Given that big data require considerable processing power, cloud computing can process huge amounts of data but will consume a substantial amount of energy [59]. Therefore, when the control of computing applications, data, and services is eliminated from the central ''cloud'' and transferred to the fog using of ML and DL techniques, then the ability to handle critical situations and provide real-time processing will be improved [53].

4) KNOWLEDGE EXTRACTION

Knowledge extraction from raw data collected by sensors may be achieved in cloud computing. However, with the rapid increase in the number of sensors, which will produce a huge amount of data, this approach may become challenging. The decentralization of computation (fog) for data analysis, with the aid of ML, will overcome these issues [62]. A combination of cloud and fog computing nodes with DL algorithms can also contribute significantly to knowledge extraction and create good user experience [71]. In healthcare systems, a transition from clinic-centric treatment to patient-centric healthcare and the extraction of quantitative vital signs is crucial for determining a patient's medical condition [74], [75].

B. SECURITY CHALLENGES

This Section discusses the challenges and open issues of Fog computing security regarding architecture and techniques terms. To get a comprehensive view of the challenges and constraints of Fog computing security issues and their categories. Figure 6 presents Fog computing security and their challenges and open issues.

1) CHALLENGES RELATED TO ARCHITECTURE

a: TRUST

Fog computing devices are frequently deployed without strict monitoring and protection, and thus they are exposed to all types of security threats. Accordingly, the primary challenge is increasing the trust aspect at the fog level. One of the techniques that can partially solve this issue is a public key infrastructure. In addition, the trusted execution environment may exhibit a potential in fog [86]–[89]. The open network

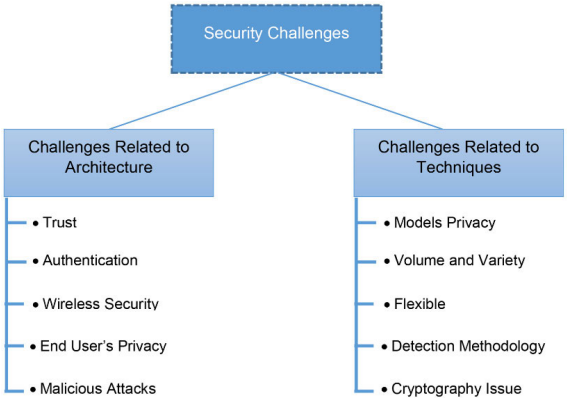

FIGURE 6. Security challenges in fog computing.

environment of fog allows malicious procedures to spread easily to intelligent devices and pose a serious threat to user data [90]. Controlling and avoiding the spread of malicious procedures are critical for a trusted execution environment [40], [76], [79].

b: AUTHENTICATION

Authentication is a serious problem in fog computing security because services are offered to massive-scale end users by front fog nodes. To access fog network services, a device has to first become part of the network by authenticating itself in the fog network. This step is essential to prevent the entry of unauthorized nodes. It also poses a formidable challenge because the devices involved in a network are constrained in various ways, including power, processing, and storage [21], [40], [76]–[79].

c: WIRELESS SECURITY

Fog computing platforms consist of wireless sensors and IoT devices. Thus, ensuring fog network security is difficult due to the volume and visibility of wireless devices. If it is not hidden and secured, then a wireless network provides unprecedented freedom to attackers to intercept sensitive data during transmission. Therefore, internal and external wireless communications with end-user devices in the fog platform should minimize packet sniffing, rogue access points, and similar challenges by implementing encryption and authentication procedures [77].

d: END USER'S PRIVACY

Nowadays, the concerns of users have been raised in terms of breaching to their private information such as personal data, location, and other information [91]. Thus, such information elicits attention when end users use services, such as cloud computing, wireless networks, and IoT. Hence, preserving privacy in fog is facing different challenges because the fog nodes located within the vicinity of end users can collect more sensitive information than a remote cloud in the core network. Privacy preservation is challenging in fog computing because fog nodes within the vicinity of end users may collect sensitive data regarding the identity, usage of utilities (e.g., smart grids), or location of end users. Moreover, centralized control becomes difficult because fog nodes are scattered in large areas. A poorly secured edge node can function as the entry point to the network for an intruder. Once inside the network, the intruder can mine and steal user's private data that are exchanged among entities [21], [76].

e: MALICIOUS ATTACKS

The fog computing environment can be subjected to numerous malicious attacks, and thus without convenient security measures in place, the capabilities of a network may be severely undermined. A DoS attack is a malicious attack. Given that the majority of devices connected to a network are not mutually authenticated, launching a DoS attack is easy. Another way to launch a DoS attack is to spoof the addresses of multiple devices and send fake processing/storage requests. Existing defense strategies for other types of networks are unsuitable for the fog computing environment because of the openness of its network. The first major challenge is the size of a network. Hundreds and thousands of nodes that form an IoT network potentially avail of fog/cloud services to overcome computation and storage limitations and enhance performance [21].

2) CHALLENGES RELATED TO TECHNIQUES

a: MODEL PRIVACY

To reduce local computation overhead, classification models provided by a health service provider can be outsourced to cloud or fog servers for decision-making purpose. Given that classification models are considered assets by health service providers, models should also be protected [77].

b: VOLUME AND VARIETY

ML is crucial for fog computing security due to data volume and variety. AI and ML are fast-growing fields, and IoT data analysis should be on par with the latest trends in these areas. A review of several ML techniques and different IoT examples indicates that analyzing data in near real time at the proximity of a node is important. Therefore, research on ML that does not require a large memory and can process a huge amount of time series data should be conducted [5].

c: FLEXIBLE

Supervised ML has been used to reduce subsets of appropriate security schemes by prioritizing various trade-offs involved in IoT applications. The manner in which flexible security is handled is a major problem. Flexible security allows a user to select the most appropriate security with a high level of flexibility. The primary objective of using flexible security is to secure an IoT-based application depending on the requirements of the users and the constraints of the edge resources [82].

d: DETECTION METHODOLOGY

Two classes of attack detection are used in IoT: anomaly-based and signature-based detection. Signature-based detection involves identifying an attack by collecting specific data from a device and then comparing these data with a set of rules or patterns referred to as a signature. Anomaly-based detection involves building a model that contains samples of normal behavior and that deviates from the model for identifying suspicious behavior or attack on a device [92]. However, zero-day attacks cannot be detected using these approaches. The major concern is the detection of attacks whose signatures cannot be found in the set of predetermined rules or patterns [81].

e: CRYPTOGRAPHY ISSUE

In general, extant cryptosystems are specifically developed for the encryption of integer values. They can also perform a few simple calculations that may influence the results and may even lead to incorrect diagnosis. One of the biggest challenges in this area is obtaining secure and accurate diagnosis [77]. In the majority of recent studies, cryptography has been used to preserve the privacy of sensors [93], [94]. Nevertheless, cryptography should maintain the encryption keys, but it is unable to handle situations wherein data sharing with the public is required. At present, differential privacy is widely adopted to address issues associated with privacy [95]. The key concept behind differential privacy is to release query results instead of distributing datasets to clients. However, this procedure may be unsuitable for CPS because a large amount of queries or information must be exchanged daily between the system and its clients. In such case, a large volume of noise has to be introduced into the released queries; this condition poses an obstacle to the implementation of differential privacy in CPS [79].

VIII. CONCLUSION

ML exhibits an excessively high potential to be the key technology in many domains. It can be considered a powerful analytic tool for fog computing applications. Despite the latest success of ML applications in fog computing, the literature on ML with regard to its role in fog computing services and systems remains scarce. The current work investigates this gap. To the best of our knowledge, no study has been conducted yet to examine the role of ML in the fog computing area. Accordingly, our research presents the involvement of ML in three aspects of fog computing: resource management, accuracy, and security. In contrast with accuracy and security, ML has been widely adopted to address many problems pertinent to resource management in fog computing. As a part of cloud computing layers, edge computing with ML has also been included. Numerous challenges and open issues have been addressed in this work. However, the more challenging aspect is security because fog computing shares many properties with cloud computing. The most popular ML task adopted in fog computing is supervised learning. In terms of application, ML with fog computing has been widely applied in the healthcare domain. Lastly, ML considerably impacts the improvement of fog computing applications and services. Therefore, researchers and developers should consider the advantages of ML to address various problems and challenges in diverse applications of fog computing.

REFERENCES

[1] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang, and R. Ranjan, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018.

[2] M. D. Assunção, R. N. Calheiros, S. Bianchi, M. A. Netto, and R. Buyya, "Big data computing and clouds: Trends and future directions," *J. Parallel Distrib. Comput.*, vol. 79, pp. 3–15, May 2015.

[3] F. Alhaddadin, W. Liu, and J. A. Gutiérrez, "A user profile-aware policy-based management framework for greening the cloud," in *Proc. IEEE 4th Int. Conf. Big Data Cloud Comput.*, Dec. 2014, pp. 682–687.

[4] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog computing: Principles, architectures, and applications," in *Internet of Things*. Amsterdam, The Netherlands: Elsevier, 2016, pp. 61–75.

[5] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[6] D. H. Chau, A. Kittur, J. I. Hong, and C. Faloutsos, "Apolo: Making sense of large network data by combining rich user interaction and machine learning," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. (CHI)*, Vancouver, BC, Canada, 2011, pp. 167–176.

[7] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza, "A survey of machine learning techniques applied to self-organizing cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2392–2431, 4th Quart., 2017.

[8] S. Suthaharan, "Big data classification: Problems and challenges in network intrusion prediction with machine learning," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 41, no. 4, pp. 70–73, 2014.

[9] G. Kamath, P. Agnihotri, M. Valero, K. Sarker, and W.-Z. Song, "Pushing analytics to the edge," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[10] M. Usama, J. Qadir, A. Raza, H. Arif, K.-L. A. Yau, Y. Elkhatib, A. Hussain, and A. Al-Fuqaha, "Unsupervised machine learning for networking: Techniques, applications and research challenges," 2017, *arXiv:1709.06599*. [Online]. Available: https://arxiv.org/abs/1709.06599

[11] S. Ayoubi, N. Limam, M. A. Salahuddin, N. Shahriar, R. Boutaba, and F. Estrada-Solano, "Machine learning for cognitive network management," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 158–165, Jan. 2018.

[12] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2432–2455, 1st Quart., 2017.

[13] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, "Machine learning for networking: Workflow, advances and opportunities," *IEEE Netw.*, vol. 32, no. 2, pp. 92–99, Mar./Apr. 2018.

[14] C. A. Hammerschmidt, S. Garcia, S. Verwer, and R. State, "Reliable machine learning for networking: Key issues and approaches," in *Proc. IEEE 42nd Conf. Local Comput. Netw. (LCN)*, Oct. 2017, pp. 167–170.

[15] P. Casas, J. Vanerio, and K. Fukuda, "GML learning, a generic machine learning model for network measurements analysis," in *Proc. 13th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2017, pp. 1–9.

[16] K. Bierzynski, A. Escobar, and M. Eberl, "Cloud, fog and edge: Cooperation for the future?" in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2017, pp. 62–67.

[17] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: An update," *ACM SIGKDD Explor. Newslett.*, vol. 11, no. 1, pp. 10–18, 2009.

[18] F. G. Pedregosa Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, and J. Vanderplas, "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Oct. 2011.

[19] Products and Services. (Mar. 22, 2019). *Cisco IOx Network Infrastructure Products*. [Online]. Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/iox/index.html
[20] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.
[21] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
[22] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput., Adv., Syst. Appl.*, vol. 6, no. 1, p. 19, 2017.
[23] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.
[24] P. Sareen and P. Kumar, "The fog computing paradigm," *Int. J. Emerg. Technol. Eng. Res.*, vol. 4, no. 8, pp. 55–60, 2016.
[25] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014.
[26] K. P. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *Int. J. Comput. Appl.*, vol. 122, no. 3, pp. 10–12, 2015.
[27] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2016, pp. 20–26.
[28] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[29] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of Everything*. Singapore: Springer, 2018, pp. 103–130.
[30] A. Davis, J. Parikh, and W. E. Weihl, "Edgecomputing: Extending enterprise applications to the edge of the Internet," in *Proc. Int. Conf. World Wide Web-Alternate Track Papers Posters (WWW)*, New York, NY, USA, 2004, pp. 180–187
[31] D. Grewe, M. Wagner, M. Arumaithurai, I. Psaras, and D. Kutscher, "Information-centric mobile edge computing for connected vehicle environments: Challenges and research directions," in *Proc. Workshop Mobile Edge Commun.*, Los Angeles, CA, USA, 2017, pp. 7–12.
[32] D. Borthakur, H. Dubey, N. Constant, L. Mahler, and K. Mankodiya, "Smart fog: Fog computing framework for unsupervised clustering analytics in wearable Internet of Things," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Montreal, QC, Canada, Nov. 2017, pp. 472–476.
[33] U. Drolia, K. Guo, and P. Narasimhan, "Precog: Prefetching for image recognition applications at the edge," in *Proc. 2nd ACM/IEEE Symp. Edge Comput.*, San Jose, CA, USA, 2017, pp. 1–13.
[34] I. Azimi, A. Anzanpour, A. M. Rahmani, T. Pahikkala, M. Levorato, P. Liljeberg, and N. Dutt, "HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT," *ACM Trans. Embedded Comput. Syst.* vol. 16, no. 5s, p. 174, 2107.
[35] G. Grassi, M. Sammarco, P. Bahl, K. Jamieson, and G. Pau, "Poster: Parkmaster: Leveraging edge computing in visual analytics," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. New York, NY, USA: 2015, pp. 257–259. doi: 10.1145/2789168.2795174.
[36] S. Wang, Y. Zhao, L. Huang, J. Xu, and C.-H. Hsu, "QoS prediction for service recommendations in mobile edge computing," *J. Parallel Distrib. Comput.*, vol. 127, pp. 134–144, May 2017. doi: 10.1016/j.jpdc.2017.09.014.
[37] D. Zissis, "Intelligent security on the edge of the cloud," in *Proc. Int. Conf. Eng., Technol. Innov.*, Funchal, Portugal, Jun. 2017, pp. 1066–1070.
[38] J. Schneible and A. Lu, "Anomaly detection on the edge," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 678–682.
[39] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 169–175, Feb. 2018.
[40] M. Yang, T. Zhu, B. Liu, Y. Xiang, and W. Zhou, "Machine learning differential privacy with multifunctional aggregation in a fog computing architecture," *IEEE Access*, vol. 6, pp. 17119–17129, 2018. doi: 10.1109/ACCESS.2018.2817523.
[41] M. Hogan and F. Esposito, "Stochastic delay forecasts for edge traffic engineering via Bayesian networks," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl.*, Cambridge, MA, USA, Oct./Nov. 2017, pp. 1–4.
[42] A. A. Mutlag, M. K. A. Ghani, N. Arunkumar, M. A. Mohamed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Gener. Comput. Syst.*, vol. 90, pp. 62–78, Jan. 2019.
[43] Y. Sun and F. Lin, "Non-cooperative differential game for incentive to contribute resource-based crowd funding in fog computing," *Bol. Tec. Bull.*, vol. 55, no. 8, pp. 69–77, 2017.
[44] I. Azimi, A. Anzanpour, A. M. Rahmani, P. Liljeberg, and T. Salakoski, "Medical warning system based on Internet of Things using fog computing," in *Proc. Int. Workshop Big Data Inf. Secur. (IWBIS)*, 2016, pp. 19–24.
[45] L. Lu, L. Xu, B. Xu, G. Li, and H. Cai, "Fog computing approach for music cognition system based on machine learning algorithm," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 1142–1151, Dec. 2018.
[46] L. Li, K. Ota, and M. Dong, "Deep learning for smart industry: Efficient manufacture inspection system with fog computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4665–4673, Oct. 2018.
[47] J. L. Pérez, A. Gutierrez-Torre, J. L. Berral, and D. Carrera, "A resilient and distributed near real-time traffic forecasting application for Fog computing environments," *Future Gener. Comput. Syst.*, vol. 87, pp. 198–212, Oct. 2018.
[48] D. Vimalajeewa, C. Kulatunga, and D. P. Berry, "Learning in the compressed data domain: Application to milk quality prediction," *Inf. Sci.*, vol. 459, pp. 149–167, Aug. 2018.
[49] M. Chen and V. Leung, "From cloud-based communications to cognition-based communications: A computing perspective," *Comput. Commun.*, vol. 128, pp. 74–79, Sep. 2018.
[50] Q. D. La, M. V. Ngo, T. Q. Dinh, T. Q. S. Quek, and H. Shin, "Enabling intelligence in fog computing to achieve energy and latency reduction," *Digit. Commun. Netw.*, vol. 5, no. 1, pp. 3–9, 2018.
[51] D. Kimovski, H. Ijaz, N. Saurabh, and R. Prodan, "Adaptive nature-inspired fog architecture," in *Proc. IEEE 2nd Int. Conf. Fog Edge Comput. (ICFEC)*, May 2018, pp. 1–8.
[52] J. Lu, X. Xiang, D. Shen, G. Chen, N. Chen, E. Blasch, K. Pham, and Y. Chen, "Artificial intelligence based directional mesh network design for spectrum efficiency," in *Proc. IEEE Aerosp. Conf.*, Mar. 2018, pp. 1–9.
[53] R. Costa, R. Jardim-Goncalves, P. Figueiras, M. Forcolin, M. Jermol, and R. Stevens, "Smart cargo for multimodal freight transport: When 'Cloud' becomes 'Fog,'" *IFAC-PapersOnLine*, vol. 49, no. 12, pp. 121–126, 2016.
[54] S. Dey and A. Mukherjee, "Implementing deep learning and inferencing on fog and edge computing systems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2018, pp. 178–183.
[55] H.-J. Hong, J.-C. Chuang, and C.-H. Hsu, "Animation rendering on multimedia fog computing platforms," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2017, pp. 336–343.
[56] K.-C. Chen, T. Zhang, R. D. Gitlin, and G. Fettweis, "Ultra-low latency mobile networking," *IEEE Netw.*, vol. 33, no. 2, pp. 181–187, Mar./Apr. 2019.
[57] J. Patman, M. Alfarhood, S. Islam, M. Lemus, P. Calyam, and K. Palaniappan, "Predictive analytics for fog computing using machine learning and GENI," in *Proc. IEEE INFOCOM IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 790–795.
[58] G. Peralta, M. Iglesias-Urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, "Fog computing based efficient IoT scheme for the Industry 4.0," in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Their Appl. Mechtron. (ECMSM)*, May 2017, pp. 1–6.
[59] S. Saraswat, H. P. Gupta, and T. Dutta, "Fog based energy efficient ubiquitous systems," in *Proc. 10th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2018, pp. 439–442.
[60] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervasive Mobile Comput.*, vol. 52, pp. 71–99, Jan. 2019.
[61] R. Garg, S. Prabhakaran, J. L. Holl, Y. Luo, R. Faigle, K. Kording, and A. M. Naidech, "Improving the accuracy of scores to predict gastrostomy after intracerebral hemorrhage with machine learning," *J. Stroke Cerebrovascular Diseases*, vol. 27, no. 12, pp. 3570–3574, 2018.
[62] L. Valerio, A. Passarella, and M. Conti, "Accuracy vs. traffic trade-off of learning IoT data patterns at the edge with hypothesis transfer learning," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–6.
[63] M. W. L. Moreira, J. J. P. C. Rodrigues, V. Furtado, N. Kumar, and V. V. Korotaev, "Averaged one-dependence estimators on edge devices for smart pregnancy data analysis," *Comput. Elect. Eng.*, vol. 7, pp. 435–444, Jul. 2018.
[64] L. Valerio, M. Conti, and A. Passarella, "Energy efficient distributed analytics at the edge of the network for IoT environments," *Pervasive Mobile Comput.*, vol. 51, pp. 27–42, Dec. 2018.

[65] M. Roopaei, P. Rad, and M. Jamshidi, "Deep learning control for complex and large scale cloud systems," *Intell. Autom. Soft Comput.*, vol. 23, no. 3, pp. 389–391, 2017.

[66] Z. Hu, P. Sun, and Y. Wen, "Speeding-up age estimation in intelligent demographics system via network optimization," in *Proc. IEEE Int. Conf. Commun.*, May 2018, pp. 1–7.

[67] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.

[68] L. Valerio, A. Passarella, and M. Conti, "A communication efficient distributed learning framework for smart environments," *Pervas. Mobile Comput.*, vol. 41, pp. 46–68, Oct. 2017.

[69] S. K. Singh, F. Carpio, and A. Jukan, "Improving animal-human cohabitation with machine learning in fiber-wireless networks," *J. Sens. Actuator Netw.*, vol. 7, no. 3, p. 35, 2018.

[70] Z. Shen, K. Yokota, J. Jin, A. Tagami, and T. Higashino, "In-network self-learning algorithms for BEMS through a collaborative fog platform," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 1162–1169.

[71] Y. Qian, J. Lu, Y. Miao, W. Ji, R. Jin, and E. Song, "AIEM: AI-enabled affective experience management," *Future Gener. Comput. Syst.*, vol. 89, pp. 438–445, Dec. 2018.

[72] D. Yacchirema, D. Sarabia-Jácome, C. E. Palau, and M. Esteve, "System for monitoring and supporting the treatment of sleep apnea using IoT and big data," *Pervas. Mobile Comput.*, vol. 50, pp. 25–40, Oct. 2018.

[73] M. H. ur Rehman, V. Chang, A. Batool, and T. Y. Wah, "Big data reduction framework for value creation in sustainable enterprises," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 917–928, 2016.

[74] A. Bagula, M. Mandava, and H. Bagula, "A framework for healthcare support in the rural and low income areas of the developing world," *J. Netw. Comput. Appl.*, vol. 120, pp. 17–29, Oct. 2018.

[75] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generat. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.

[76] D. Malathi, R. Logesh, V. Subramaniyaswamy, V. Vijayakumar, and A. K. Sangaiah, "Hybrid reasoning-based privacy-aware disease prediction support system," *Comput. Elect. Eng.*, vol. 73, pp. 114–127, Jan. 2019.

[77] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 825–837, Jan. 2018.

[78] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K. R. Choo, and D. E. Newton, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Gener. Comput. Syst.*, vol. 90, pp. 94–104, Jan. 2019.

[79] T. Zhu, P. Xiong, G. Li, W. Zhou, and S. Y. Philip, "Differentially private model publishing in cyber physical systems," *Future Gener. Comput. Syst.*, to be published.

[80] C. Pham, L. A. T. Nguyen, N. H. Tran, E.-N. Huh, and C. S. Hong, "Phishing-aware: A neuro-fuzzy approach for anti-phishing on fog networks," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 3, pp. 1076–1089, Sep. 2018.

[81] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl. Soft Comput.*, vol. 72, pp. 79–89, Nov. 2018.

[82] B. Mukherjee, S. Wang, W. Lu, R. L. Neupane, D. Dunn, Y. Ren, Q. Su, and P. Calyam, "Flexible IoT security middleware for end-to-end cloud–fog communication," *Future Gener. Comput. Syst.*, vol. 87, pp. 688–703, Oct. 2018.

[83] B. S. Khater, A. A. Wahab, M. Idris, M. A. Hussain, and A. A. Ibrahim, "A lightweight perceptron-based intrusion detection system for fog computing," *Appl. Sci.*, vol. 9, no. 1, p. 178, 2019.

[84] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *J. Sensor Actuator Netw.*, vol. 8, no. 1, p. 16, 2019.

[85] T. Baker, M. Asim, Á. MacDermott, F. Iqbal, F. Kamoun, B. Shah, O. Alfandi, and M. Hammoudeh, "A secure fog-based platform for SCADA-based IoT critical infrastructure," *Softw., Pract. Exper.*, 2019.

[86] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in Internet of healthcare things," *IEEE Access*, vol. 4, pp. 8418–8441, 2016.

[87] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.

[88] C. Chen, H. Raj, S. Saroiu, and A. Wolman, "cTPM: A cloud {TPM} for cross-device trusted applications," in *Proc. 11th USENIX Symp. Networked Syst. Design Implement. (NSDI)*, 2014, pp. 1–16.

[89] C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun, "Smartphones as practical and secure location verification tokens for payments," in *Proc. NDSS*, Feb. 2014, pp. 23–26.

[90] Z. Li, X. Zhou, Y. Liu, H. Xu, and L. Miao, "A non-cooperative differential game-based security model in fog computing," *China Commun.*, vol. 14, no. 1, pp. 180–189, 2017.

[91] N. Tariq, M. Asim, F. Al-Obeidat, M. F. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[92] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security and privacy," Jul. 2017, *arXiv:1707.01879*. [Online]. Available: https://arxiv.org/abs/1707.01879

[93] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2018.

[94] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[95] C. Dwork, "A firm foundation for private data analysis," *Commun. ACM*, vol. 54, no. 1, pp. 86–95, 2011.

KARRAR HAMEED ABDULKAREEM received the B.S. degree in computer science (artificial intelligence) from the University of Technology, Iraq, in 2007, and the M.S. degree in computer science (internetworking technology) from the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia, in 2016. He is currently pursuing the Ph.D. degree in computer science and information technology with the Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests multicriteria decision making, image dehazing, and computer security.

MAZIN ABED MOHAMMED received the B.Sc. degree in computer science from the University of Anbar, Iraq, in 2008, the M.Sc. degree in information technology from UNITEN, Malaysia, in 2011, and the Ph.D. degree in information technology from UTeM, Malaysia, in 2018. He is currently a Lecturer with the College of Computer Science and Information Technology, University of Anbar, Iraq. His research interests include artificial intelligence, biomedical computing, and optimization.

SARASWATHY SHAMINI GUNASEKARAN received the M.Sc. and Ph.D. degrees in information and communication technology from UPM and Universiti Tenaga Nasional (UNITEN), Malaysia, in 2013 and 2017, respectively, where she is currently a Senior Lecturer with the College of Computing and Informatics. Her research interest is in the field of artificial intelligence. She looks forward for collaboration possibilities in the areas of agent technology, essentially in the field of social commerce and smart sustainable cities.

MOHAMMED NASSER AL-MHIQANI received the B.Sc. degree in computer science (computer networking), in 2014, and the M.Sc. degree in computer science (internetworking technology) from the Universiti Teknikal Malaysia Melaka (UTeM), in 2015, where he is currently pursuing the Ph.D. degree. His research interests include cyber security, cyber-physical system security, insider threats, machine learning, and image processing.

AMMAR AWAD MUTLAG was born in Iraq, Baghdad, in 1985. He received the B.Sc. degree in computer science from the College of Information Technology, Imam Sadiq University, Iraq, in 2009, and the M.Sc. degree in information technology from Andhra University, India, in 2015. He is currently pursuing the Ph.D. degree with the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. His current research interests include artificial intelligence, cloud computing, fog computing, machine learning, the IoT, and biomedical computing.

SALAMA A. MOSTAFA received the B.Sc. degree in computer science from the University of Mosul, Iraq, in 2003, and the M.Sc. and Ph.D. degrees in information and communication technology from Universiti Tenaga Nasional (UNITEN), Malaysia, in 2011 and 2016, respectively. He is currently a Lecturer with the Department of Software Engineering, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM). His research interests are in the area of soft computing, data mining, software agents, and intelligent autonomous systems.

NABEEL SALIH ALI received the B.Sc. degree in computer science from the University of Technology, Baghdad, Iraq, in 2003, and the M.Sc. degree in computer science (internetworking technology) from the University Technical Malaysia Melaka (UTeM), Malaysia, in July 2015. His research works are in web applications security techniques to improve the security and survivability of computer systems, including the healthcare monitoring systems and the Internet of Things (IoT).

DHEYAA AHMED IBRAHIM received the B.Sc. degree in computer science from the College of Computer, University of Anbar, Iraq, in 2009, and the M.Sc. degree in computer science from the College of Computer, University of Anbar, in 2012. He is currently pursuing the Ph.D. degree in information and communications technology with the Computer Engineering Techniques Department, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq. His current research interests include artificial intelligence, biomedical computing, medical image processing, and optimization methods.