

The fog computing for internet of things: review, characteristics and challenges, and open issues

Mahmood A. Al-Shareeda¹, Abeer Abdullah Alsadhan², Hamzah H. Qasim^{1,3}, Selvakumar Manickam⁴

¹Department of Communication Engineering, Iraq University College, Basrah, Iraq

²Department of Computer Science, Applied College, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

³Department of Oil and Gas Engineering, Basrah University Oil and Gas, Basrah, Iraq

⁴National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

Article Info

Article history:

Received Dec 18, 2022

Revised May 24, 2023

Accepted Jun 5, 2023

Keywords:

Challenges and review

FC-IoT open issues

FC-IoT review

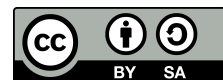
Fog computing

Internet of things

ABSTRACT

The internet of things (IoT) research envisions a world in which common place objects are linked to the internet and trade, store, process, and gather data from their surroundings. Due to their inherent resource limitations, IoT devices are typically unable to directly host application services, despite their increasing importance for facilitating the supply of data to enable electronic services. Since it can survive and work in tandem with centralized cloud systems and extends the latter toward the network edge, fog computing (FC) may be an appropriate paradigm to get around these restrictions. This paper reviews the overview of the IoT in terms of application and design parameters and FC. Meanwhile, this paper presents the architecture of fog computing for IoT (FC-IoT) in terms of communication, security, data quality, sensing and actuation management, codification, analysis, and decision-making. Additionally, this review provides several characteristics and challenges of FC-IoT. Finally, open issues for this paper have been discussed.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

11800 USM, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

The internet of things (IoT) is one of the most talked-about innovations because of the numerous benefits it could bring to modern life. As the IoT continues to advance, an increasing number of objects in our surroundings will be able to connect to the Internet and communicate with one another automatically, without any intervention from humans [1], [2]. The original motivation behind the IoT was to eliminate the need for manual data entry by replacing it with a network of interconnected devices equipped with sensors to collect data from their surroundings.

The integration of the IoT and cloud computing offers numerous advantages for a wide range of IoT applications. However, given to the rising number of IoT developments with varying platforms, the development of new IoT applications is a difficult task [3], [4]. This is because massive amounts of data are produced by IoT apps due to the use of sensors and other IoT devices. The next step is to evaluate these massive data sets in order to settle on a course of action. The amount of bandwidth needed to upload all of this information to the cloud is excessive [3]. These issues are handled by implementing fog computing.

The phrase fog computing was first used by Cisco [5]. It's state-of-the-art hardware, and it has many uses beyond just the IoT. Fog computing provides similar data processing and storage capabilities to IoT consumers as the cloud [6], [7]. Instead of sending data to a remote server in the cloud, fog devices can process and store data locally. Similar communication, processing, and storage capacities are provided by fog and the cloud [8].

Fog computing is used in the IoT to improve performance and efficiency while reducing the amount of data that must be sent to the cloud for processing, analysis, and storage. Data collected by sensors will be sent to network edge devices for temporary storage and operation to reduce network traffic and delay [9].

This paper provides a synopsis of research into the merits, traits, and current state of the art of fog computing (FC) in relation to the IoT, which is referred to here as FC-IoT. In this article, we explore the integration of the FC-IoT, focusing on its benefits, new applications, and challenges. There are related concepts and papers that discuss how to combine the IoT with the fog. Unanswered questions about the IoT and fog computing are discussed as well.

Section 2 describes FC and the IoT. Section 3 presents the architecture of FC-IoT. Section 4 provides characteristics and challenges of FC-IoT. Section 5 provides open issues for this paper. Finally, this paper is concluded in section 6.

2. FOG COMPUTING AND INTERNET OF THINGS

2.1. Fog computing

In reference to the industrial revolution, fog computing, often known as fogging, is a more advanced version of cloud computing that provides service and application and (highest process and lowest delay) to independent, diverse devices located in an industry [10]. The purpose is to place intelligence control, operating, and storage close to data devices. Real-time applications with highest information operating, extreme ability, and scalability are crucial for Industry 4.0. Due to its many advantages over cloud computing, fog computing offers the finest options for this kind of setting. By introducing the concept of network edge computing, the extension of cloud computing seeks to reduce the load on the cloud.

The lowest delay and improved cache memory are necessary for the industrial automation of real-time services and decision-making processes. Applications of real-time, movement, lowest delay, position consciousness, quantity of users, and cache-based edge nodes are required performance requirements on this basis of distribution. Between internet cloud infrastructure and end-user devices are virtualized nodes, sometimes referred to as cloudlets or fog nodes. Fog computing offers similar applications and services as the cloud does but with superior quality of service (QoS) matrices performance that addresses crucial IoT requirements. Fog computing has several key benefits that affect how it is used in the IoT, including:

- By storing information at the network's periphery rather than in far clouds, transmission lags can be eliminated.
- Fog computing provides quicker data processing and analysis for IoT applications.
- Data storage on edge nodes will cut down on processing and computation time.
- When caching is enabled on nodes, the network will not send out duplicate information.
- Can deal with all IoT applications, such as vehicular ad-hoc networks (VANETs), smart grids, smart cities, and device-to-device (D2D), which rely on edge networking.
- Permits a limited two-way dialogue between cloud providers and client devices.

For the vast array of smart IoT devices that will be used in the near future, fog computing is the cornerstone of the solutions that it will offer for more effective, efficient, and managed communication methods. A prospective supporter of industrial automation is fog computing, which offers more features than cloud computing with regard to delay, safety, position consciousness, the quantity of server devices, real-time application, and movement.

2.2. Internet of things

Smart devices and processes must constantly exchange information on the appearance of defects, elements, stocking, various demands, and various instructions to increase activity, chase, ability, production quality, and industry expansion. Intelligent cities, intelligent factories, and intelligent products are significant IoT-useful instances, according to this perspective.

2.2.1. IoT-applications

Every stage, from the detection of errors through the use of communication and networking technologies to address them, has to be streamlined and offers the possibility for further study. These applications are referred to as smart in the literature because they have qualities like intelligence, efficiency, dependability, sustainability, confidentiality, and safety.

- Smart city applications: in 2050, the population of the world's cities is projected to be around 6 billion [11]. With the development of technology infrastructure, the demand for services would rise along with the population growth. Enormous data is the name given to this big data origination. There are numerous domains that need to be intelligent in order to construct a future intelligent city, including the intelligent home, intelligent transportation, intelligent institution, intelligent office, intelligent agriculture, and intelligent health-care facilities.
- Smart factory applications: robotics and distributed automated systems make up smart industries. Machine learning (ML) algorithms and artificial intelligence (AI) technology make it possible for this futuristic smart factory floor. Controllers, autonomous systems, microchips, actuators, and sensors are built into these automated devices.
- Smart product applications: Industry 4.0 development is fueled by IoT, production time, big data, and cloud computing. Industry 4.0 items are intelligent because sensors and microchips are built right into them.

2.2.2. Design parameters of IoT

The manufacturing sector is currently having difficulty attaining its objectives due to the rising customer and market demands. The concept of industry-wide automation that increases manufacturing process flexibility was developed by Industry 4.0. These design parameters are:

- Latency: there should be a restriction to prevent any delays of any kind, including processing, propagation, transmission, and computing, as some IoT applications are time-sensitive.
- Performance: these QoS needs will always trade off in terms of performance. The elements affecting performance should be balanced in a way that is optimal, helpful, and effective. Future automation will demand performance maintenance solutions.
- Low cost: low-cost smart devices should be employed for IoT applications to avoid affecting CAPEX/OPEX. The amount of deployment required for Industry 4.0 shouldn't be so high as to hurt sales.
- Energy and long battery life: for more effective results, the network's overall energy should be kept. The battery capacity of smart gadgets should be sufficient to enable extended use.
- Security, safety, and privacy: these are highly strict requirements that must be met by all IoT applications. For instance, privacy and security indoor an intelligent factory should be such that no one may access the sensitive data.
- Reliability: applications using the IoT necessitate dependable real-time connectivity.
- Standardization: such network standardization does not yet exist, making it an open research problem.
- Network topology: how many smart devices and servers (cloud, fog, and e-nodes) should be distributed throughout a network to meet QoS requirements?
- Monitoring network: mobility, the environment, and wireless. The network topology may vary due to natural events, necessitating regular system management and monitoring.

3. ARCHITECTURE OF FC-IOT

As shown in Figure 1, a conceptual architecture for a cloud-fog-IoT application is presented in this section. This architecture has six layers as follows.

3.1. Communication

The communication viewpoint facilitates communication among the various network nodes, and it is widely acknowledged as a crucial core capability [12], [13]. The usage of network virtualization in current IoT systems and in the FC-IoT is yet in its nonage, despite the fact that it is a very hot issue (by containing both

SDN and virtualization-based network function). This is supported by the scant literature on the subject and the scant attention other review initiatives in the fog area, such [14], have paid to this dimension.

- Standardization: the protocol being utilized is one of the most important factors in ensuring proper combination and relationship between IoT nodes and services. These protocols enable programmers to build IoT systems with infrastructure compatibility [15]-[17].
- Semantics of network: the network semantics of the connection standard is a crucial component. For important systems, this feature is crucial since it ensures that the data transmitted by the network's various nodes gets received. Currently, a variety of mechanisms, including retransmission, handshake, and multicasting, can be employed to ensure the semantics of the network [18], [19].
- Low-latency: when fog computing is used up to the network's edge, it makes it easier to offer lowest delay replies, provided that it is used in conjunction with suitable data connection protocols. To enhance the response between nodes (cloud or fog), or among nodes and devices, various protocols may be applied. To achieve low-latency, some of the previously examined protocols have been applied and modified [20], [21].
- Mobility: the great mobility of certain of the devices used in IoT applications is what distinguishes them [22], [23]. To accommodate this mobility, several protocols use routing and resource discovery techniques. The task of creating and maintaining routes between distant nodes is performed by routing mechanisms.

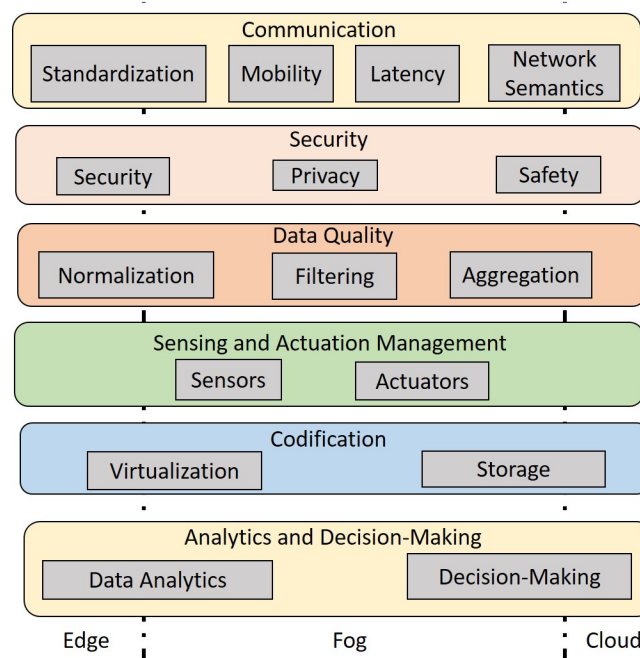


Figure 1. Architecture of fog computing for IoT

3.2. Security

The security perspective has an impact on the entire architecture due to all transmission, information, and actions should be conducted in a way that ensures system security in a broad sense, particularly in accordance with the requirements for data quality, security, and dependability. Although reviews on FC often place a stronger confirmation on information computer and technology (ICT) elements [24], standards (such as the security perspective in the OpenFog reference architecture [25]) and surveys on fog computing identify security as a core capability. It has been acknowledged the need to broaden the security perspective in the context of fog for IoT to cover not only ICT problems but also security problems that may develop since the use of sensors-based physical and actuators [26].

- Safety: for vital IoT systems, safety is a crucial characteristic. Normally, the principles and action reasons of IoT communication must include provisions for safety. However, foggy conditions should aid in the creation of such regulations [27], [28].

- Security: IoT system security typically rests on at least four fundamental pillars: (i) integrity (detection and prevention of unauthorized information alteration); (ii) confidentiality (ensuring that data is delivered to the intended recipient while preventing disclosure to unauthorized parties); (iii) data loss (preventing information loss during transmission); and (iv) intrusion detection (determine if an unlawful node is attempting to access to the network) [29], [30].
- Privacy: controlling data access and attempting to prevent fraudulent or unauthorized users from obtaining user information is the key strategy for ensuring the privacy of the data [31].

3.3. Data quality

Although this perspective is occasionally considered or incorporated as a part of other perspectives (e.g., in the OpenFog data, analytics, and control perspective), it is crucial for IoT requirements to separate out a full-fledged data quality perspective [32]. His viewpoint is responsible for processing all the realized and obtained aggregation to improve their quality while also lowering the volume of data that needs to be delivered by IoT nodes or kept in fog/cloud users. Three distinct elements make up this perspective, which are sometimes carried out in order: information filtering, information normalization, and information aggregation [33].

- Data normalization: FC-IoT are very diverse in their makeup. The coverage of sensors can vary, ranging from weak to strong, with differences in orders of magnitude. Similar to this, fog nodes have a heterogeneous nature and can offer various services. Therefore, in order to facilitate data transmission, all sensed and given information should be standardized [34].
- Filtering of information: filtering of information is a feature designed to cut down on the amount of information delivered by removing redundant, incorrect, or flawed data. Since limiting the data traffic as fast as feasible, data filtering techniques should be put into use as close to the edge as practicable. Although sensors may employ lightweight filtering, more robust and advanced information filtering algorithms are still needed to remove some disturbances during the data collection phase [35].
- Data aggregation: the further reduction of the gathered data was the main goal of the data aggregation component. To do this, it employs a variety of complimentary processes centered on data fusion, hierarchical aggregation, and enhancing system security through data aggregation [36]. In an effort to lower the size of the data collection and create a special data flow, data fusion techniques attempt to combine various types of data. To achieve this, several arithmetic procedures (to obtain more representative values) and spatial-temporal techniques (to score information in accordance with their position/timing) can be used. The result is the production of more consistent and representative values for a large sample [37].

3.4. Sensing and actuation management

The equipment (both physical and virtual) in charge of detecting the environment and acting in specified circumstances or pursuant to orders make up the sensing and actuation management viewpoint. This viewpoint spans all domains because while physical devices are a component of the network setup to ensure the proper functioning of the application, virtual sensors or actuators may be included in fog and cloud nodes. Additionally, it is a specialization of the management functionality that is usually found in all major associated fog standards and surveys [38]-[40].

- Sensors: most IoT devices have the ability to sense in order to comprehend their surroundings and determine whether or not their business objectives are being met. This element can handle two different types of sensors: sensors based physically, which use specialized hardware to collect data directly from the environment, and virtual sensors, which get their data from other sources [41], [42].
- Actuators: other systems, however, are built on a strong actuation phase and a sensing phase. As a result, the actuators have the ability to modify the environment in order to fully or partially automate the achievement of the intended objectives [43], [44].

3.5. Cloudification

In the architecture of the fog, cloudification functions as a little distributed cloud. With the help of this viewpoint, constrained cloud services and resources could be brought nearer to the edge, decreasing needless global-scope interactions that are well-known in fog computing [45]-[47]. Virtualization techniques are necessary to enable the deployment of a cloud inside a fog node and the integration of several applications into a single node. Additionally, the many instances and services might be combined in order to create more complicated functionalities.

- Virtualization: fog nodes can build virtual machines (VM) to enable particular IoT services, creating isolated environments thanks to virtualization. As a result, a fog node, for example, may have various VMs supporting various systems installed. The approach utilized to enclose the IoT method and the way that virtual pictures are moved from one node to another, offering the node's need for movement, as well as the network's reliability, are the two primary aspects that must be taken into consideration [48], [49].
- Storage: to hasten to process, decrease data transfer latency, and boost system stability, data can be initially kept on edge or fog nodes. Various methods are being used to store this data on fog nodes or on various network infrastructure components [13], [50].

3.6. Decision-making and analytics

The decision-making and analytics viewpoint, which is widely acknowledged as a key component of fog computing [6], [51], [52], is in charge of analyzing the stored data in order to produce various analytics and detect particular scenarios. The set of short-term analytics in the fog and long-term analytics in the cloud can enable both proactive and reactive decision-making in ubiquitous environments, enhancing system scalability and encompassing a wider range of IoT applications. In these environments, a large number of sensors continuously collect data and transmit it to the fog.

- Information analytics: applying cutting-edge analytics methods to data sets in order to uncover particular circumstances is known as data analytics. We can categorize this element into small information analytics, Big information analytics, and hierarchical information analytics by concentrating on where data are analyzed [53].
- Decision-making: the agility in making decisions to activate certain business processes and regulations at the correct time is vital and has a clear impact on resource utilization and customer satisfaction, just as the speed at which the obtained data must be delivered and processed [54], [55].

4. CHARACTERISTICS AND CHALLENGES

This section shows several characteristics and the challenges for fog computing in IoT. We focus on low latency, large-scale applications, mobility of devices, decentralization, low capability of devices, and geographic distribution. The description of these issues are as follows.

- Low latency: there are several challenges to the characteristic of low latency, as follows. Identity authentication, intrusion detection, access control, lightweight protocols design, secure data sharing, secure data search, verifiable computation, privacy-preserving data aggregation, decentralized and salable secure infrastructure.
- Large-scale applications: there are several challenges to the characteristic of large-scale applications, as follows. Identity authentication, intrusion detection, sensitive data identification and protection, secure data sharing, detection of rogue fog nodes and IoT devices, resilience to Sybil attacks, secure content distribution, secure big data analysis, privacy-preserving packet forwarding, and decentralized and salable secure infrastructure.
- Mobility of devices: there are several challenges to the characteristic of mobility of devices, as follows. Identity authentication, data integrity protection, trust management, secure data search, resilience to Sybil attacks, secure content distribution, privacy-preserving data aggregation, privacy-preserving packet forwarding, decentralized and salable secure infrastructure.
- Decentralization: there are several challenges to the characteristic of decentralization, as follows. Intrusion detection, access control, sensitive information protection and identification, trust management, detection of rogue IoT devices and fog nodes, data integrity protection, resilience to Sybil attacks, secure data search, secure data sharing, privacy-preserving data aggregation, privacy exposure in data combination, decentralized and scalable secure infrastructure.
- Low capability of devices: there are several challenges to the characteristic of low capability of devices, as follows. Lightweight protocols design, secure data sharing, secure data search, secure aided computation, and secure big data analysis.
- Location awareness: there are several challenges to the characteristic of location awareness, as follows. Location privacy leakage, privacy-preserving packet forwarding, and decentralized and scalable secure infrastructure.

- Geographic distribution: there are several challenges to the characteristic of geographic distribution, as follows. Location privacy leakage, privacy-preserving packet forwarding, decentralized and scalable secure infrastructure.

5. OPEN ISSUES

This section discusses several open issues in fog computing for IoT. These issues are the preservation of location privacy, rogue fog node, and IoT device detection, exposure to privacy in data combination, and secure infrastructure that is decentralized and scalable. These issues are provided as follows.

- Preservation of location privacy: local real-time services, local data management, and local content dissemination all benefit from the location awareness and spatial spread of fog computing. In order to enable a user to find friends within the same fog node's coverage region, Huo *et al.* [56] devised a location difference-based proximity detection mechanism. In order to stop an attacker from deliberately claiming a fake position for service access, Yang *et al.* [57] suggested that fog nodes' locations be verified. Fog computing thereby increases the allure of numerous location-based services and features. Unfortunately, the localization component of fog computing exposes users' whereabouts without their knowledge. For instance, a wearable gadget uploads its acquired data to a fog node, which then sends the data or a summary of the data to the cloud.
- Rogue fog node and IoT device detection: the fog computing architecture leaves fog nodes and IoT devices open to a wide variety of cyber-attacks. The compromised IoT devices and fog nodes may seem to be reliable connections in an effort to trick users into establishing contact with them. Fog nodes have been shown by Roman *et al.* [58] to be susceptible to various DoS attacks, including wireless and dispersed DoS assaults. Fog nodes' lack of resources compared to the cloud can cause jamming. In fog computing, Liang *et al.* [59] demonstrated the viability of man-in-the-middle attacks in the event that the gateway has been compromised or substituted with a false one. The user's secret key can be retrieved from the digital certificate if the device is compromised or hacked. In addition, even if the IoT devices and fog nodes are safe, they may still turn into rogue nodes if they are financially motivated to do so. For instance, an evil fog node may be used to spread lies and deceit to unsuspecting motorists.
- Exposure to privacy in data combination: in IoT applications, devices serve as data producers, generating and processing data at varied granularities. Some data may be inherently sensitive, such as that from a heart rate sensor, while other data may be completely safe. The gathered data may not seem very sensitive individually, but when combined, they pose serious threats to privacy and security [60]. The use of fog computing for IoT exacerbates this issue because one of its primary goals is to enable explicit collaboration among fog nodes that can gather and process data from several IoT devices. For illustration, a patient purchases certain medications from a drugstore and pays by using a credit card (confidential patient information). If the pharmacy lacks personal computers, its options are limited in knowledge about the patient, including recalling the face and the patient's credit card information.
- Secure infrastructure that is decentralized and scalable: fog computing is a distributed, scalable, and adaptable approach that welcomes and encourages the addition and removal of IoT devices and fog nodes as needed. The lack of a centralised server makes it challenging to build a secure architecture in a distributed framework.

6. CONCLUSION




Industry 4.0 will be a revolutionary period with a vast array of smart devices that will facilitate IoT applications across all industries. The implementation of smart devices will alter perspectives in all spheres of human life. One of the ideas that have gained increased significance and impact is fog computing. There are numerous options available right now for enhancing device connectivity, data security and privacy, data quality, or even how apps respond to the environment. This paper describes FC and the IoT. Also, this paper presents the architecture of FC-IoT and provides characteristics challenges, and open issues for FC-IoT. We are currently working to expand the number of solutions that have been analysed and the IoT contexts in which they are used. For example, smart connected vehicles, smart buildings, and other key environments are where many IoT applications are being developed. We are currently analysing how various approaches and solutions are being used in these situations. This paper can be used as a starting point for thinking about how to improve FC-IoT security and privacy.

REFERENCES




- [1] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - IoTBDS*, 2017, pp. 254–260, doi: 10.5220/0006292602540260.
- [2] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 1, pp. 518–526, 2023, doi: 10.11591/ijeecs.v29.i1.pp518-526.
- [3] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: a primer," *Digital Communications and Networks*, vol. 4, no. 2, pp. 77–86, Apr. 2018, doi: 10.1016/j.dcan.2017.07.001.
- [4] M. A. Al-Shareeda et al., "Proposed Efficient Conditional Privacy-Preserving Authentication Scheme for V2V and V2I Communications Based on Elliptic Curve Cryptography in Vehicular Ad Hoc Networks," *Communications in Computer and Information Science*, vol. 1347, pp. 588–603, 2021, doi: 10.1007/978-981-33-6835-4_39.
- [5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, New York, NY, USA: ACM, Aug. 2012, pp. 13–16. doi: 10.1145/2342509.2342513.
- [6] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.
- [7] O. Salman, I. Elhadj, A. Chehab, and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Computer Networks*, vol. 143, pp. 221–246, Oct. 2018, doi: 10.1016/j.comnet.2018.07.020.
- [8] N. Peter, "Fog computing and its real time applications," *International Journal of Emerging Technology and Advanced Engineering*, vol. 5, no. 6, pp. 266–269, 2015.
- [9] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," *IEEE Internet Computing*, vol. 21, no. 2, pp. 16–24, Mar. 2017, doi: 10.1109/MIC.2017.36.
- [10] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, Oct. 2014, doi: 10.1145/2677046.2677052.
- [11] P. P. Rogers, K. F. Jalal, and J. A. Boyd, *An Introduction to Sustainable Development*. Routledge, Earthscan, 2008.
- [12] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, 2017, doi: 10.1016/j.jnca.2017.09.002.
- [13] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," *Mobidata 2015 - Proceedings of the 2015 Workshop on Mobile Big Data, co-located with MobiHoc 2015*, vol. 2015-June, pp. 37–42, 2015, doi: 10.1145/2757384.2757397.
- [14] R. K. Naha et al., "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018, doi: 10.1109/ACCESS.2018.2866491.
- [15] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog Computing in Healthcare-A Review and Discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017, doi: 10.1109/ACCESS.2017.2704100.
- [16] B. Costa, J. Bachiega, L. R. Carvalho, M. Rosa, and A. Araujo, "Monitoring fog computing: A review, taxonomy and open challenges," *Computer Networks*, vol. 215, 2022, doi: 10.1016/j.comnet.2022.109189.
- [17] M. Antonini, M. Vecchio, and F. Antonelli, "Fog Computing Architectures: A Reference for Practitioners," *IEEE Internet of Things Magazine*, vol. 2, no. 3, pp. 19–25, 2020, doi: 10.1109/iotm.0001.1900029.
- [18] M. A. Rahman, M. S. Hossain, E. Hassanain, and G. Muhammad, "Semantic Multimedia Fog Computing and IoT Environment: Sustainability Perspective," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 80–87, 2018, doi: 10.1109/MCOM.2018.1700907.
- [19] N. Petrovic and M. Tosic, "SMADA-Fog: Semantic model driven approach to deployment and adaptivity in fog computing," *Simulation Modelling Practice and Theory*, vol. 101, 2020, doi: 10.1016/j.simpat.2019.102033.
- [20] P. O'Donovan, C. Gallagher, K. Bruton, and D. T. J. O'Sullivan, "A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications," *Manufacturing Letters*, vol. 15, pp. 139–142, 2018, doi: 10.1016/j.mfglet.2018.01.005.
- [21] M. Losada, A. Cortés, A. Irizar, J. Cejudo, and A. Pérez, "A flexible fog computing design for low-power consumption and low latency applications," *Electronics (Switzerland)*, vol. 10, no. 1, pp. 1–23, 2021, doi: 10.3390/electronics10010057.
- [22] C. Puliafito et al., "MobFogSim: Simulation of mobility and migration for fog computing," *Simulation Modelling Practice and Theory*, vol. 101, 2020, doi: 10.1016/j.simpat.2019.102062.
- [23] J. Pereira, L. Ricardo, M. Luís, C. Senna, and S. Sargento, "Assessing the reliability of fog computing for smart mobility applications in VANETs," *Future Generation Computer Systems*, vol. 94, pp. 317–332, 2019, doi: 10.1016/j.future.2018.11.043.
- [24] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9204, pp. 685–695, 2015, doi: 10.1007/978-3-319-21837-3_67.
- [25] Z. Á. Mann, "Notions of architecture in fog computing," *Computing*, vol. 103, no. 1, pp. 51–73, Jan. 2021, doi: 10.1007/s00607-020-00848-z.
- [26] K. Fu et al., "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things," 2020, [Online]. Available: <http://arxiv.org/abs/2008.00017>
- [27] H. Sabireen and V. Neelanarayanan, "A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges," *ICT Express*, vol. 7, no. 2, pp. 162–176, 2021, doi: 10.1016/j.ict.2021.05.004.
- [28] S. A. Syed et al., "QoS Aware and Fault Tolerance Based Software-Defined Vehicular Networks Using Cloud-Fog Computing," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010401.
- [29] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030927.
- [30] V. K. Quy, N. V. Hau, D. V. Anh, and L. A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges," *Complex and Intelligent Systems*, 2021, doi: 10.1007/s40747-021-00582-9.
- [31] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Insights into security and privacy towards fog computing evolution," *Computers and Security*, vol. 120, 2022, doi: 10.1016/j.cose.2022.102822.

- [32] A. Bhardwaj, K. Kaushik, and M. Kumar, "Taxonomy of Security Attacks on Internet of Things," *Security and Privacy in Cyberspace*, pp. 1–24, 2022, doi: 10.1007/978-981-19-1960-2_1.
- [33] B. Costa, J. Bachiega, L. R. de Carvalho, and A. P. F. Araujo, "Orchestration in Fog Computing: A Comprehensive Survey," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1–34, Feb. 2023, doi: 10.1145/3486221.
- [34] A. Telikani, J. Shen, J. Yang, and P. Wang, "Industrial IoT Intrusion Detection via Evolutionary Cost-Sensitive Learning and Fog Computing," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 23260–23271, 2022, doi: 10.1109/JIOT.2022.3188224.
- [35] H. J. de Moura Costa, C. A. da Costa, R. da R. Righi, and R. S. Antunes, "Fog computing in health: A systematic literature review," *Health and Technology*, vol. 10, no. 5, pp. 1025–1044, 2020, doi: 10.1007/s12553-020-00431-8.
- [36] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Information Sciences*, vol. 514, pp. 118–130, 2020, doi: 10.1016/j.ins.2019.12.007.
- [37] O. R. Merad-Boudia and S. M. Senouci, "An Efficient and Secure Multidimensional Data Aggregation for Fog-Computing-Based Smart Grid," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6143–6153, 2021, doi: 10.1109/JIOT.2020.3040982.
- [38] P. Hosseinioun, M. Kheirabadi, S. R. K. Tabbakh, and R. Ghaemi, "aTask scheduling approaches in fog computing: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3792.
- [39] B. Jamil, H. Ijaz, M. Shojafar, K. Munir, and R. Buyya, "Resource Allocation and Task Scheduling in Fog Computing and Internet of Everything Environments: A Taxonomy, Review, and Future Directions," *ACM Computing Surveys*, vol. 54, no. 11s, 2022, doi: 10.1145/3513002.
- [40] P. Saraswat, "Survey on Fog Computing and Its Function in IoT," *Smart Innovation, Systems and Technologies*, vol. 273, pp. 483–488, 2022, doi: 10.1007/978-3-030-92905-3_59.
- [41] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A taxonomy, survey and future directions," *Internet of Things*, vol. 0, no. 9789811058608, pp. 103–130, 2018, doi: 10.1007/978-981-10-5861-5_5.
- [42] A. Markus and A. Kertesz, "A survey and taxonomy of simulation environments modelling fog computing," *Simulation Modelling Practice and Theory*, vol. 101, 2020, doi: 10.1016/j.simpat.2019.102042.
- [43] W. Lee, K. Nam, H.-G. Roh, and S.-H. Kim, "A gateway based fog computing architecture for wireless sensors and actuator networks," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, pp. 1–1, 2016, doi: 10.1109/icact.2016.7423331.
- [44] 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, doi: 10.1109/MC.2016.245.
- [45] S. Zahran, H. Elkadi, and W. Helmy, "Fog Computing Platform to Handle Internet of Things Data Heterogeneity," *Journal of System and Management Sciences*, vol. 12, no. 1, pp. 521–544, 2022, doi: 10.33168/JSMS.2022.0133.
- [46] M. A. Al-Shareeda and S. Manickam, "Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation," *Symmetry*, vol. 14, no. 8, 2022, doi: 10.3390/sym14081543.
- [47] S. Rani, A. Kataria, and M. Chauhan, "Fog Computing in Industry 4.0: Applications and Challenges—A Research Roadmap," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 74, pp. 173–190, 2022, doi: 10.1007/978-981-16-3448-2_9.
- [48] J. Li, J. Jin, D. Yuan, and H. Zhang, "Virtual Fog: A Virtualization Enabled Fog Computing Framework for Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 121–131, Feb. 2018, doi: 10.1109/JIOT.2017.2774286.
- [49] Y. Xu, V. Mahendran, and S. Radhakrishnan, "Towards SDN-based fog computing: MQTT broker virtualization for effective and reliable delivery," *2016 8th International Conference on Communication Systems and Networks, COMSNETS 2016*, 2016, doi: 10.1109/COMSNETS.2016.7439974.
- [50] J. S. Fu, Y. Liu, H. C. Chao, B. K. Bhargava, and Z. J. Zhang, "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018, doi: 10.1109/TII.2018.2793350.
- [51] K. Gasmı, S. Dilek, S. Tosun, and S. Ozdemir, "A survey on computation offloading and service placement in fog computing-based IoT," *Journal of Supercomputing*, vol. 78, no. 2, pp. 1983–2014, 2022, doi: 10.1007/s11227-021-03941-y.
- [52] J. A. S. Aranda, R. dos S. Costa, V. W. de Vargas, P. R. da S. Pereira, J. L. V. Barbosa, and M. P. Vianna, "Context-aware Edge Computing and Internet of Things in Smart Grids: A systematic mapping study," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107826.
- [53] M. R. Anawar, S. Wang, M. A. Zia, A. K. Jadoon, U. Akram, and S. Raza, "Fog Computing: An Overview of Big IoT Data Analytics," *Wireless Communications and Mobile Computing*, vol. 2018, 2018, doi: 10.1155/2018/7157192.
- [54] A. Varmaghani, A. M. Nazar, M. Ahmadi, A. Sharifi, S. J. Ghoushchi, and Y. Pourasad, "DMTC: Optimize Energy Consumption in Dynamic Wireless Sensor Network Based on Fog Computing and Fuzzy Multiple Attribute Decision-Making," *Wireless Communications and Mobile Computing*, vol. 2021, 2021, doi: 10.1155/2021/9953416.
- [55] M. M. Hamdi, A. S. Mustafa, H. F. Mahdi, M. S. Abood, C. Kumar, and M. A. Al-Shareeda, "Performance Analysis of QoS in MANET based on IEEE 802.11b," *2020 IEEE International Conference for Innovation in Technology, INOCON 2020*, 2020, doi: 10.1109/INOCON50539.2020.9298362.
- [56] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: A Location Difference-Based Proximity Detection Protocol for Fog Computing," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1117–1124, 2017, doi: 10.1109/JIOT.2017.2670570.
- [57] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for Fog Computing," *Future Generation Computer Systems*, vol. 78, pp. 799–806, 2018, doi: 10.1016/j.future.2017.05.035.
- [58] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018, doi: 10.1016/j.future.2016.11.009.
- [59] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 310–320, 2014, doi: 10.1109/TPDS.2013.37.
- [60] A. Narayanan and V. Shmatikov, "Myths and fallacies of 'Personally Identifiable Information'," *Communications of the ACM*, vol. 53, no. 6, pp. 24–26, Jun. 2010, doi: 10.1145/1743546.1743558.




BIOGRAPHIES OF AUTHORS

Mahmood A. Al-Shareeda    received his B.S degree in from communication Engineering in Iraq University College and M.Sc. in Information Technology from Islamic University of Lebanon (IUL) in 2018. He obtained Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He was worked as a postdoctoral fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He is currently assistant professor at Communication Engineering, Iraq University College (IUC). His current research interests include network monitoring, IoT, VANET security, and IPv6 security. He can be contacted at email: alshareeda022@gmail.com.






Abeer Abdullah Alsadhan    is currently working as Assistant Professor in Information Security and Artificial Intelligence at Imam Abdulrahman Bin Faisal University Dammam Saudi Arabia. Her research interests include machine learning, deep learning, cyber security, and IoT. She has published a number of publications in reputed journals. She can be contacted at email: Aalsadhan@iau.edu.sa.



Hamzah H. Qasim    received the B.S. degrees in Communication Engineering, In 2018, he received the M.Sc. degree in Electrical Engineering from University Tun Hussein Onn Malaysia (UTHM), Malaysian. He is currently Ph.D. student in Universiti Teknologi MARA (UiTM), Malaysian. In addition, he is currently a lecturer In Basrah University for Oil and Gas, Department of Oil and Gas Engineering. His current research interests include IoT, WSN, V2X; SUMO, OM-NET++, and mobility management for resource allocation in cellular communication. He can be contacted at email: Enghamza.iq@gmail.com, and Hamza.hadi@buog.edu.iq.



Selvakumar Manickam    is currently working as an Associate Professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, IoT, Industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.