Fog Computing and SDN in IoT Networks

This report was prepared for Professor Ahmed Karmouch in partial fulfillment of the requirements for the course ELG7187F Software Defined Networks and Cloud
Group 5
22 Dec 2022

1st Varun Narayana Naik
Department of Electrical and Computer Engineering
University of Ottawa
Ottawa, Canada
vnaik041@uottawa.ca
300270736

2st Nishad Sanjay Vyas
Department of Electrical and Computer Engineering
University of Ottawa
Ottawa, Canada
nvyas028@uottawa.ca
300267323

***Abstract*—In recent times, the Internet of Things (IoT) has seen rapid advancements and subsequently the number of applications has also increased significantly, resulting in new concepts such as smart health, smart cities, and smart homes. These IoT networks require vast amounts of processing and data storage. Generally, cloud computing is used to meet these demands. Although the cloud can provide processing and resources it still faces some challenges. The rising number of IoT devices as well as the distance between the cloud and these devices is an issue since it leads to higher latency, which is an obstacle for real-time applications. Fog computing, which is a highly virtualized paradigm can address these issues by delivering computational resources, data storage and network services closer to the end devices. However, there are issues such as heterogeneity that plague fog computing and to tackle them centralized network control in the form of Software Defined Networking (SDN) is needed. In this paper, we describe SDN-enabled fog computing and its architecture. Then, we present the unique features and advantages of SDN-enabled fog over traditional fog computing. Finally, we have discussed the challenges and solutions currently faced in this paradigm.**

***Index Terms*—Fog computing, Software Defined Networking, Fog-SDN, Internet of Things**

I. Introduction

The advent of the internet and the rise of smart devices has led to the growth of the Internet of Things (IoT) and hence the IoT revolution. IoT encompasses smart devices and objects that have electronics, software and networking capability that allow inter-device communication [1]. These devices such as smart vehicles, and smart appliances use the IoT network to exchange data. The scale of growth is estimated to reach 75 billion devices alone, this means a much larger number of connections are needed to interconnect these devices [2]. There are a lot of advances being made in computing paradigms. The most well know paradigm is that of cloud computing, providing a centralized approach to enabling computing as a utility and acting as a catalyst for internet services development. But such a centralized paradigm has inevitably led to some limitations and has opened doors for a more decentralized paradigm to computing, one that can address the challenges of latency, bandwidth and anomaly detection. As a result, new approaches have been developed such as fog computing. The decentralized nature itself presents new problems when dealing with routing data among the nodes, hence complex network management and traffic engineering are crucial to reducing the data transmission latency. The idea of Software-defined networking has proven useful in this aspect. In this paper, we refer to the combination of fog and SDN as SDN-enabled fog or fog-SDN.

A. Fog Computing

Fog computing is a decentralized approach to computing in stark contrast to the centralized nature of traditional cloud computing. A term coined by Cisco [3]; Fog computing is defined as the cloud near the network edge closer to the end devices and acts as an intermediary between the IoT and the cloud [1]. Fog aims to bring computing and data storage closer to IoT devices. Fog computing works in conjunction with the cloud and acts as a bridge between the cloud and IoT devices [4]. It does not aim to replace cloud computing but rather distributes the resources in all directions in the cloud IoT continuum. It addresses the problems associated with cloud computing such as high latency, bandwidth, location awareness and reliability since the processing power is brought closer to the IoT devices which also provides better access to data storage. This structure can be represented by three layers namely, the IoT device layer, fog layer and cloud layer. While fog handles local data, the cloud handles mainly global data. The fog network constitutes fog nodes that are low processing-power devices such as servers, devices, or virtual machines. The fog nodes communicate with the IoT devices and form a bridge to the cloud. These nodes can be placed anywhere between the cloud and the IoT devices in the cloud-IoT continuum. These nodes communicate with each other to exchange data and resources. The fog nodes process the real-time data at the edge of the network without sending large amounts of data to the cloud. However, if the processing power of the fog nodes is insufficient, the fog nodes send the data to the cloud for further processing. The presence of numerous fog nodes provides better services to IoT devices compared to cloud data centres; hence fog has more services to offer like lower latency, better bandwidth and location awareness. This has paved the way to support applications such as smart homes, smart healthcare and smart cities which require real-time analysis.

B. Software Defined Networking (SDN)

Software-defined networking is a paradigm where the data plane is separated from the control plane and a central controller governs the network behaviour [5]. The aim is to form a centralized intelligence having a global view of the network which not only allows easier network management but rather better network security. The network control logic is implemented by the controller and is separated from the forwarding process where the network devices perform packet forwarding.

Being software in nature, SDN allows new changes to be made to the network easily using a software program compared to using fixed commands in the network devices. Due to its centralized approach, SDN can make traffic forwarding decisions from a single controller and thus removes the need to individually configure each network device to change network behaviour [6]. The conventional hardware-based network architecture is error-prone and has complex network control. Any failure results in expensive and time-consuming repairs. Using a software-based architecture removes the need for highly skilled network engineers. The process of managing a network becomes easier since the control plane only deals with traffic management and network topology, hence can be used to control fog nodes and based on the configurations in the control plane, the data plane manages the flow of traffic in the fog nodes.

The separation of layers allows the network providers to distribute the resources using the application layer which also provides services like routing and monitoring. They can configure the network policies using the control plane where all the control logic resides and set up hardware routers and nodes using the data plane which is formed by the interconnected forwarding devices. The protocols used to provide communication between the controller and the forwarding devices are known as southbound Application Programming Interfaces (APIs). One such is the OpenFlow API, which defines the flow rules used by network devices. Whereas northbound APIs are used to connect the applications and the control plane. Thus Software-defined networking enables the concurrent update of network resources as per the application and data scaling.

This paper makes contributions such as: We describe what is fog computing. We give a brief description of the working of fog computing and how it compares with cloud computing as well as how it works in conjunction with cloud computing. Next, we talk about what Software-defined networking is and how it is used to handle networking when compared to traditional hardware methods. We discuss how SDN can be used for fog computing and how they can complement each other. We see the architecture of such a proposed new paradigm. Furthermore, we describe what are its characteristics and benefits for use in IoT networks. We also present a few challenges that add limitations to reaching the full potential of fog computing which are solved using SDN.

The outline of the paper is as follows. Section II defines the architecture of SDN-enabled fog computing. It provides details about each component. Section III outlines the advantages and characteristics of SDN-enabled fog that make it useful for IoT networks. Section IV briefly discusses the real-world applications of SDN-enabled fog. Section V discusses the challenges and solutions faced by the SDN-enabled fog domain. Finally, Section VI ends the paper with the conclusion.

II. Architecture of SDN-Enabled Fog

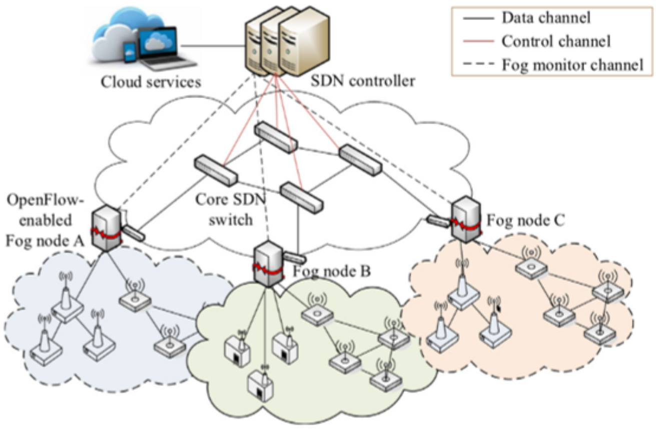

Fig. 1. SDN-Enabled Fog Model

The emergence of complex IoT paradigms needs solutions that can handle the latency and resource requirements. Fog computing is a viable solution to this issue as it develops on the existing technology of cloud computing. IoT applications in smart cities, healthcare and industry have strict requirements for latency. This is solved by fog computing by bringing the computing resources and the data storage closer to the IoT devices near the edge. Thus fog computing closes the gap between the IoT paradigm and cloud computing. With the presence of numerous networking elements in the form of fog nodes as discussed earlier, the latency with each node traversed increases, hence it is vital to configure and manage how data is transferred among the network elements to meet the latency needs [7]. This issue of managing the network flow and traffic is best handled by using Software-defined networking (SDN) as shown by Fig. 1. Moreover, it can help with the scalability and flexibility of the fog network. Hence an SDN-enabled fog is utilised for IoT applications. The Fig. 2 shows the structure of such an SDN-enabled fog. There are mainly four components such as fog nodes, SDN switches, a controller and services.

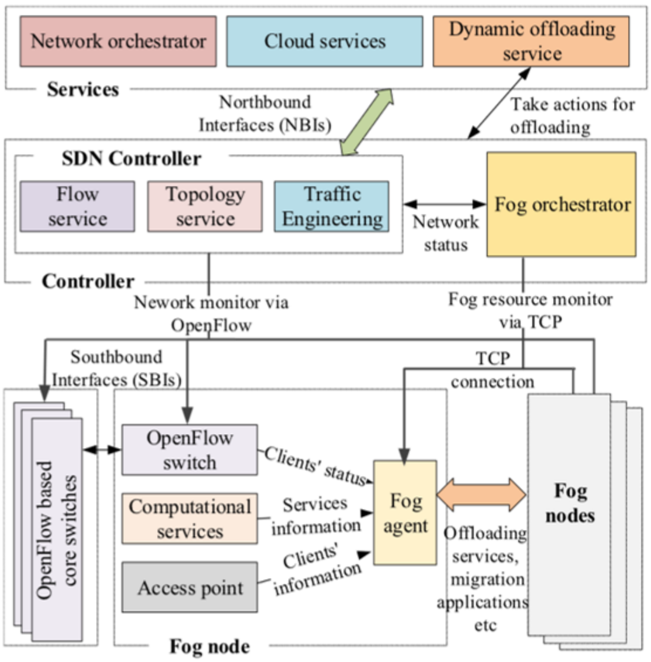

Fig. 2. Architecture of SDN-Enabled Fog

A. Fog Nodes

A fog node interacts directly with IoT end devices such as smart watches, thermostats, cameras, mobile phones and so on. It does so using a wireless interface. The fog nodes form the fog domain and it can be comprised of devices such as routers, switches, gateways, computers and set-top boxes [8]. Each node has a fog agent and several computational services [9]. The fog nodes communicate with the controller through an SDN core switches. The fog node is connected to the fog orchestrator present within the controller using the fog agent. The purpose of this fog agent is to send vital information about the fog nodes such as the availability and capacity of the computational resources, and hardware specifications which are further used by the various services.

B. SDN Switches

The SDN switches form the core SDN network. These SDN switches are controlled by an SDN controller [9]. OpenFlow is used by these switches to communicate with the controller. The controller can change the flow rules in the switches, this lets the controller dynamically control the network. The SDN controller periodically collects information about the network properties such as latency and bandwidth through the switches. The SDN network and the fog nodes are often maintained by one organization in small-scale systems. Whereas, in large-scale systems, these can be handled by multiple organizations working together.

C. Controller

The controller is known as the brain of the SDN-enabled fog [5]. It houses the SDN controller and the fog orchestrator. Some of the well-known SDN controllers are NOX [10] and OpenDaylight [11] and one of the well-known fog orchestrators is FORCH [12]. The SDN controller handles network management and traffic monitoring. It establishes the flow tables and rules as well as the policies for handling the data. The controller helps in abstracting the network complexity. The controller is connected to the services using the northbound APIs. The SDN controller uses the southbound APIs (OpenFlow) to connect with the SDN switches. The controller uses the SDN switches to ensure proper forwarding, fragmentation and reassembly take place. The fog orchestrator handles the fog node operation. The fog agent and SDN switches are used to gain information about the fog nodes and the network.

D. Services

This layer consists of applications that can provide various functionalities to the end devices. These services are developed to help the operation of the fog system. The controller uses northbound interfaces such as OpenDaylight to communicate with the topmost layer, the services. The services offered include firewall, quality of service, access control and proxy control.

III. Advantages of Fog and SDN

A. Handling Heterogeneity

The IoT network is heterogenous in nature due presence of a wide diversity of IoT devices. IoT devices often have different data formats and different protocols for communication information which is also influenced by the presence of legacy devices [13]. These devices are made up of various types of hardware configurations, protocols, communication technologies and standards. The application of SDN providing network control over the fog enables multiple protocols and devices to be interconnected. Not only does the SDN allow interoperability among various types of fog nodes, but it also enables interoperability between end devices of different types which can be physical or virtual. SDN-enabled fog can handle IoT devices using heterogeneous networks for communication such Wifi, Bluetooth and ethernet [14]. Thus SDN-enabled fog computing can provide a platform for these devices of different environments to interoperate with each other. Moreover, various service providers are often used in a large-scale system and SDN-enabled fog computing can effectively handle these different service providers.

B. Location Awareness

In SDN-enabled fog, the nodes are not centralized in one location, rather they are distributed in different locations. The SDN, having a global view of the network as well as the fog nodes enables location awareness and geographical distribution of resources [15]. The IoT devices are far away from the cloud servers and need real-time communication with the server for computing and resources, but by utilising fog nodes in close proximity and the traffic engineering of SDN, the data can be processed efficiently and closer to the

IoT devices. This in turn improves performance by drastically reducing the delays for real-time applications. The services and the applications offered by fog are distributed as well and can be easily accessed by end devices compared to cloud services. Due to the location awareness of fog-SDN, the location of the fog nodes can be determined accurately [16]. Hence the presence of fog nodes near the end devices helps determine the location of the end devices easily [17]. This is particularly useful for application in smart cities and healthcare as the location can have an impact on the Quality of Service (QoS) [18].

C. Network Security and Privacy

While fog computing has benefits such as latency, fast processing, service allocation and many more, a security issue is associated with them. These fog nodes lack efficient security algorithms, and the data stored in them might get breached by hackers or malicious users. The existing solutions are only partially suitable for IoT devices with limited computational resources. To overcome these security issues [19], fog nodes can be enabled by a centralized SDN controller in the cloud layer and multiple distributed controllers near the edge in the control layer. It works on a master-slave paradigm, wherein the central controller manages the secure communication for all the components in the network. The SDN controllers in the control layers act as a sub-master, providing secure mobility to this architecture and ensuring secure, manageable, and coordinated communication between fog nodes and the cloud. The slaves in this architecture are the devices at the edge of the network, including all the sensors and mobile components. The controller in this network helps reduce the delay time for authentication for communications between fog and cloud, which was very difficult to achieve with just the fog network.

D. Resource and Network Management

Enabling fog computing with SDN eases communication among the fog nodes to ensure good performance. Fog computing can be beneficial for real-time applications which require low latency and real-time responses, but its network diversity can become challenging to manage. Using SDN controllers in conjunction with fog nodes can provide low latency along with efficient resource and network management. For smart grids in Wireless Body Area Networks (WBANs) [20], a three-layered architecture is used for efficient resource management. The architecture's bottom layer consists of all the IoT sensors responsible for generating the data. The middle layer, or the second layer, has fog nodes which comprise intelligent meters and servers, these servers are responsible for collecting data generated by the first layer. In the third layer, there is an SDN controller that manages all the fog nodes. The SDN controller manages data forwarding by using the shortest path algorithm and three types of path recoveries in case any failure occurs during data transmission. Similarly, for the Internet of Vehicles (IoV), the same architecture can have five layers for better Central Processing Unit (CPU) utilization in case it is overloaded or under-loaded [21].

IV. Applications

Fog computing can have various applications in different domains, such as real-time traffic regulation in smart cities, garbage truck routing using sensors in garbage bins, real-time video processing for surveillance systems and many more. Although it has many applications with increases in network size and number of devices, there are some limitations to it, such as high latency and node overloading, which can be tackled by utilizing an SDN controller, which will be discussed in the next section.

Smart healthcare is one of the significant applications of fog computing, which is being improved with the help of SDN. In e-healthcare, fog-SDN ensures the Quality-of-Service parameters like bandwidth, latency, higher throughput, and less packet loss while ensuring the privacy and the security of the patient's sensitive information is secured. This is made possible by the centralized SDN controller, and the flow rules designed by these controllers and switches. Based on these flow rules, the switches decide to send the packets to the cloud or to process them at the edge; further discussion about similar implementation is presented in the next section.

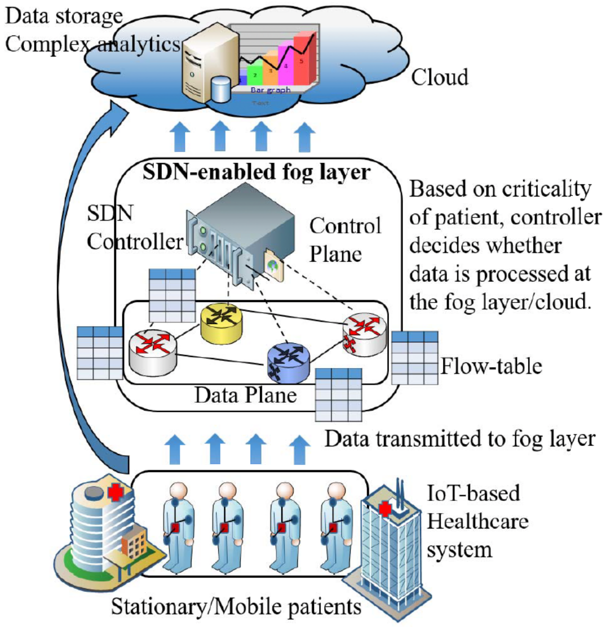
Data storage
Complex analytics
Cloud
SDN-enabled fog layer
SDN Controller
Control Plane
Based on criticality of patient, controller decides whether data is processed at the fog layer/cloud.
Flow-table
Data Plane
Data transmitted to fog layer
IoT-based Healthcare system
Stationary/Mobile patients

Fig. 3. Architecture of SDN-Enabled Fog

V. Challenges and Solutions

A. Latency

In applications concerning healthcare data, the transmission of packets is very time critical. While transmitting the data to the server, factors such as throughput, latency, and loss of packets can affect the network's performance. These issues must be addressed to process information in real time with less delay while efficiently utilizing the network's available resources. The proposed architecture [22] considers patients' health conditions and determines a Criticality Index (CI) to prioritize the tasks in the network.

In Fig. 3, the architecture is divided into three parts, a traditional wireless-based network consists of all the sensor nodes that collect the patient's information. The SDN-enabled fog layer consists of a control plane with an SDN controller and the OpenFlow switches in the data plane with their flow rules. Finally, a cloud layer comprises data centers for storing patients' information, such as Electronic Medical Images (EMI), Electronic Medical Records (EMR) and Electronic Health Records (EHR) for complex analytics. Whenever OpenFlow switches receive data packets from the WBAN, they determine their criticality index, which is divided into subranges to consider cases in which patients' conditions might be deteriorating quickly. Based on the criticality index, the OpenFlow switches decide whether to send the data to the cloud or to process it at the fog nodes. Utility values such as energy consumption and bandwidth are also considered. If no fog nodes are available, the controller will find newly updated nodes and update the flow table while recomputing the utility values. Finally, after the task completion, the fog node sends a signal to the SDN controller to update the flow table and utility values. Furthermore, to reduce latency, this number of flow rules is reduced by replacing the most used flow rule with the least used one.

B. *Task Offloading*

Even though fog computing works well in reducing the latency between the end devices and the cloud center, the fog node can get overloaded due to a surge in requests from the IoT devices. For issues such as this, an effective task-offloading technique must be implemented in the fog nodes [9]. SDN-based fog computing networks can dynamically offload the tasks to improve the bandwidth between end devices and the cloud center. Fig. 4 depicts the offloading scheme used by the fog-SDN network to efficiently manage the incoming task requests and select the optimal node for its processing. When a fog node is overloaded, it sends a request for offloading the task to the fog orchestrator, and this request contains resource requirements. Node selection is made in two steps; in the first step, the offloading service starts a search for all the available optimal nodes capable of handling the requested task. The second step ranks all these nodes based on the network condition and computational resources. Dividing this process into two steps improves the running time because the first step reduces the number of nodes which will then be input for step 2. Finally, the node accepting the offload request is selected based on the least communication cost compared to other fog nodes. Any algorithm can be used and applied in the OpenFlow switches for choosing the optimal routing path for the task offloading.

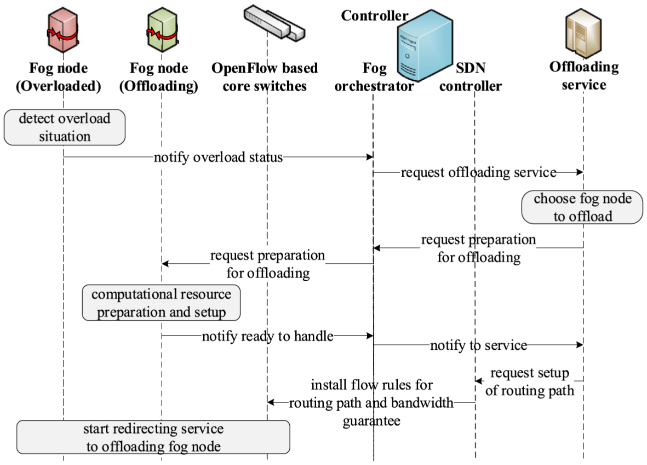
Controller
Fog node (Overloaded)
Fog node (Offloading)
OpenFlow based core switches
Fog orchestrator
SDN controller
Offloading service
detect overload situation
notify overload status
request offloading service
choose fog node to offload
request preparation for offloading
request preparation for offloading
computational resource preparation and setup
notify ready to handle
notify to service
request setup of routing path
install flow rules for routing path and bandwidth guarantee
start redirecting service to offloading fog node

Fig. 4. Sequence of Task Offloading in Fog-SDN

VI. Conclusion

Fog computing along with SDN forms a bridge between the cloud and the IoT end devices and helps support real-time applications. In this paper, we have described SDN-enabled fog which is an architecture that combines the advantages of fog computing and SDN for IoT devices. We looked at how fog computing can be beneficial for IoT applications and how the performance can be further improved by using SDN. We also described the advantages of fog-SDN such as interoperability to tackle heterogeneity, location awareness to deal with the vast size of IoT, network management to handle the resources efficiently and network security to deal with data intrusion. We have also mentioned how fog-SDN can be used for various applications such as smart cities and smart healthcare. Finally, we have identified the challenges such as the overloading of fog nodes and high latency in time-sensitive applications. We have also detailed the solutions to these challenges that can be achieved by using SDN with fog computing.

This paper covers various aspects of fog computing and SDN by providing descriptions of the advantages, applications and challenges. For future work, we would like to delve deeper into the research focusing on the advantages of fog-SDN.

References

[1] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, IOT, Edge, and Fog," IEEE Access, vol. 7, pp. 150936–150948, 2019.

[2] L. S. Vailshery, "IOT devices installed Base Worldwide 2015-2025," Statista, 27-Nov-2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed: 17-Dec-2022].

[3] "What is edge computing?," Cisco, 20-Oct-2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/computing/what-is-edge-computing.html. [Accessed: 17-Dec-2022].

[4] P. Verma and S. K. Sood, "Fog assisted-IOT enabled patient health monitoring in Smart Homes," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1789–1796, 2018.

[5] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): A survey," Security and Communication Networks, vol. 9, no. 18, pp. 5803–5833, 2016.

[6] H. Kim and N. Feamster, “Improving network management with software defined networking,” IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, 2013.

[7] J. L. Herrera, J. Galan-Jimenez, L. Foschini, P. Bellavista, J. Berrocal, and J. M. Murillo, “QoS-aware fog node placement for intensive IOT applications in SDN-fog scenarios,” IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13725–13739, 2022.

[8] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow and P. A. Polakos, ”A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges,” in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 416-464, Firstquarter 2018, doi: 10.1109/COMST.2017.2771153.

[9] L.-A. Phan, D.-T. Nguyen, M. Lee, D.-H. Park, and T. Kim, “Dynamic fog-to-fog offloading in SDN-based Fog Computing Systems,” Future Generation Computer Systems, vol. 117, pp. 486–497, 2021.

[10] F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network and openflow: From concept to implementation,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2181–2206, 2014.

[11] J. Medved, R. Varga, A. Tkacik, and K. Gray, “OpenDaylight: Towards a model-driven SDN controller architecture,” Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, 2014.

[12] G. Davoli, D. Borsatti, D. Tarchi and W. Cerroni, ”FORCH: An Orchestrator for Fog Computing service deployment,” 2020 IFIP Networking Conference (Networking), 2020, pp. 677-678.

[13] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, “A software defined networking architecture for the internet-of-things,” 2014 IEEE Network Operations and Management Symposium (NOMS), 2014.

[14] I. Bedhief, M. Kassar, and T. Aguili, “SDN-based architecture challenging the IOT heterogeneity,” 2016 3rd Smart Cloud Networks & Systems (SCNS), 2016.

[15] H. Atlam, R. Walters, and G. Wills, “Fog computing and the internet of things: A Review,” Big Data and Cognitive Computing, vol. 2, no. 2, p. 10, 2018.

[16] T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, “Fog computing in healthcare internet of things: A case study on ECG feature extraction,” 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

[17] J. Ni, K. Zhang, X. Lin, and X. Shen, “Securing fog computing for internet of things applications: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2018.

[18] A. Markus, J. D. Dombi, and A. Kertesz, “Location-aware task allocation strategies for IOT-fog-cloud environments,” 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2021.

[19] S. Kahvazadeh, V. B. Souza, X. Masip-Bruin, E. Marn-Tordera, J. Garcia, and R. Diaz, “Securing combined fog-to-cloud system through SDN approach,” Proceedings of the 4th Workshop on CrossCloud Infrastructures & Platforms - Crosscloud’17, 2017.

[20] J. Ren, J. Li, H. Liu, and T. Qin, “Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IOT,” Tsinghua Science and Technology, vol. 27, no. 4, pp. 760–776, 2022.

[21] A. Alomari, S. K. Subramaniam, N. Samian, R. Latip, and Z. Zukarnain, “Resource Management in SDN-based Cloud and SDN-based Fog Computing: Taxonomy study,” Symmetry, vol. 13, no. 5, p. 734, 2021.

[22] C. Roy, R. Saha, S. Misra, and D. Niyato, “Soft-Health: Software-defined fog architecture for IOT applications in Healthcare,” IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2455–2462, 2022.