A Critical Analysis of Healthcare Applications Over Fog Computing Infrastructures

Pedro H. Vilela[1], Joel J. P. C. Rodrigues[1,2,3], Luciano R. Vilela[1], Mukhtar M. E. Mahmoud[4], Petar Solic[5]
[1]National Institute of Telecommunications (INATEL), Santa Rita do Sapucaí - MG, Brazil
[2]Instituto de Telecomunicações, Portugal
[3]University of Fortaleza (UNIFOR), Fortaleza - CE, Brazil
[4]Faculty of Computer Science and Information Technology, University of Kassala, Kassala, Sudan
[5]University of Split, Split, Croatia
pedrov@mtel.inatel.br, joeljr@ieee.org, luciano.ctrl@hotmail.com, mukhtaredris@gmail.com, psolic@fesb.hr

***Abstract*— Over the last decade, the number of Internet of Things (IoT) smart devices has grown exponentially. In order to support the computational demand of real-time latency-sensitive applications in healthcare, a new paradigm named Fog Computing has emerged. Fog Computing is located closer to the IoT devices/sensors and is considered to be an extension of the Cloud Computing. In this paper, a hospital ward room is used as a case study, where the scenario is simulated using the *iFogSim* simulator, in order to evaluate and analyse its behaviour in terms of latency, network usage, cost of transmission, and power consumption. The results point out the possibility to enhance Quality of Service for patients and care givers by adding the Fog Computing layer to the current Cloud infrastructure.**

***Index Terms*— Cloud Computing, Fog Computing, Healthcare, eHealth, Internet of Things**

I. Introduction

In the last few years, Cloud Computing granted many opportunities to businesses by providing a wide length of services and platform independence, where no software installation was needed on the user-side. Offering a *pay-as-you-go* service model, the concept of Cloud enabled enterprises to reduce its costs and increase its collaboration through resource pooling and fast elasticity.

Recently, Fog Computing has emerged with the potential to satisfy the requirements that the Cloud-based model is not able to address [1]. Such paradigm extends the computation resources available in the Cloud to the edge of the network, focusing on Internet of Things (IoT) solutions. Thus, it enables the support for billions of connected devices to provide data processing, storage, and services to its end-users.

The Fog architecture introduces the support for real-time data analysis where computational resources are distributed among devices within a Fog environment. This approach helps to reduce significantly the amount of data sent to a Cloud infrastructure, once the necessary data processing occurs directly in the device located at the edge of the network.

With the arrival of IoT, CISCO estimates that around 50 billion devices will be connected to the Internet by 2020 [2]. This means the Cloud Computing infrastructure may require a vast amount of bandwidth to manage all these data, which, in these terms, is impractical.

The Fog Computing approach aims to attend a new scenario where the volume of data through the Cloud shall quadruple in the next years, reaching about 92% of total data centre traffic by 2020 [3].

The main objective of this paper is to critically evaluate the integration of the Fog Computing concept and compare it with the traditional Cloud Computing model. The main contributions of this work are the following:

- An overview of the benefits and characteristics of Fog Computing;
- The identification of the challenges in a healthcare scenario;
- A case study performing a comparison between Cloud and Fog Computing in healthcare.

The rest of the paper is organised as it follows. Section II presents some of the most relevant studies related to the Fog paradigm in healthcare applications. Section III describes the concepts of Cloud and Fog Computing, as well as their basic architecture models, also depicting the motivation for employing Fog Computing in healthcare solutions, defining the scenario for the case study, and the simulation tool-kit. Section IV performs the result analysis of some the most important parameters related to Fog Computing concept using the *iFogSim* simulator. The last section summarises some of the benefits brought by the integration of Cloud and Fog Computing models. It also points out new directions for healthcare applications that are not yet investigated by the research community.

II. Related work

The current most relevants researches for this study related to the Cloud and the Fog Computing paradigms in health care solutions are described in this section.

Liu *et al.* [4] report in this survey that, by offering computation and storage at the edge of the network, latency and network bandwidth can be reduced as well as security and privacy concerns can be mitigated. Through the hundreds of thousands of devices connected to the Internet, the huge volume of data generated will require real-time responses. Therefore, this amount of data causes a high bandwidth cost.

If false data are injected into these IoT devices, besides compromising the data accuracy, there may be an increase in the use of communication resources. Tackling this situation, Lu *et al.* [5] present an aggregation scheme of lightweight privacy-preserving data, which addresses the above challenges for Fog devices. The researchers performed several experiments showing that, by applying early filters at the edge of the network, communication resources are saved, avoiding false data injection.

Chen *et al.* present an architecture for autonomic security management which is able to assess risks in health care information systems applying a cost-efficient self-protecting approach with little or no human intervention at all. This framework also offers prevention mechanisms for monitoring and management solutions helping decision making actions based on security issues [6].

Huang *et al.* created a framework considering how to keep private health information safe from eavesdropping or malicious manipulation. Based on this framework, the authors developed a medical expert system to tackle low effectiveness due to manual operations and privacy breaches caused by the participation of doctors in the medical information process [7].

Gu *et al.* [8] suggest a concept of Fog Computing in medical systems able to allocate services closer to end devices in order to improve quality of service (QoS). The presented model helps to share the burden of offloading traffic from the core network by distributing tasks through base station association, where virtual machines are deployed.

Although IoT devices play an important role in services delivering more efficiently in health environments, there are still many challenges related to security and privacy. To exemplify this situation, Alrawais *et al.* [9] delineate a new scheme applying Fog Computing that addresses the distribution of digital certificates in IoT environments. The new scheme approach ensures that the revoked certificates can be immediately sent to the Fog nodes, mitigating the risk of accepting a revoked certificate.

III. System Model

This section introduces the basic idea of the Cloud Computing infrastructure and the Fog Computing concept along with their basic architectural models.

A. Cloud Computing

In the last few decades, *Cloud Computing* became one of the major research topics of the information technology (IT), providing resources such as scalability and mobility. The National Institute of Standards and Technology (NIST) defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [10]. As Griebel *et al.* mention in their paper, one of the attributes of Cloud Computing applied to healthcare is the possibility to consume resources from the Cloud whenever needed, and pay only for the used resources [11]. Another great advantage is the capability of sharing information among health professionals, caregivers, and patients in a more structured way, reducing the risks of losing documents such as exams and medical records. On the other hand, the majority of the Cloud data centres are geographically centralised and located far from its end-users. As a consequence, real-time and latency-sensitive applications suffer from high round-trip delay, network congestion, among other issues.

B. Fog Computing

Similar to Cloud Computing, Fog Computing is able to provide computation and storage services to its end-users. Due to its characteristic of being closer to devices and its dense geographical distribution, services can be placed at the edge of the network, which reduces latency and bandwidth usage. The Fog Computing concept has been first introduced by CISCO as an architecture that extends computational and storage capacity of the Cloud to the edge of network [2]. In other words, it brings the Cloud closer to its end-users. Thus, it allows data to be collected and processed locally, reducing network latency as well as bandwidth usage.

Some benefits brought by Fog Computing found in literature are the following:

1) Latency: When compared to other Cloud-based architectures, the placement of processing closer to end-users reduces network latency, since the physical distance is shorter. Thus, possible processing delays in data centres are avoided. Also, latency can be reduced by moving computation-intensive tasks from constrained resources to a more powerful Fog Computing node [12].

2) Privacy: Different from the Cloud architecture, the Fog concept enables the analysis and data processing on a local gateway, instead of sending it to the Cloud. Therefore, the privacy of user data is enhanced [13].

3) Bandwidth: The volume of data in the Fog Computing paradigm can be reduced in several ways. For instance, the data collected by smart devices can be preprocessed, analysed, and compressed when needed in Fog nodes. In this way, only a small part of the data may be sent to a remote Cloud data centre [14]. Fog nodes are also able to comply with specific requests from devices based on cached data, removing the communication with the Cloud [15].

4) Dependability: Fog Computing helps to increase the system dependability in different manners. One example is through sharing the same functionality among several nodes in order to achieve data redundancy. Another example is the lower dependency on network connection availability, since computational resources are placed closer to devices [16].

C. Basic Architecture

The reference model of the Fog Computing architecture is a promising topic in the communications research. Recently, a vast number of architectures have been proposed for Fog Computing, where the three tiers architecture is considered to be the predominant structure nowadays [17].

The basic Fog Computing architecture depicted in Figure 1 is split in the following three main layers:

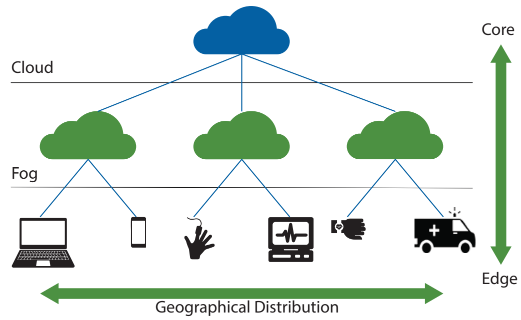

Figure 1: Illstration of the three tiers basic Fog computing architecture.

1) Device layer: The device layer is the closest layer to the end-users/devices. It is comprised of several devices such as sensors and mobile phones. These devices are widely geographically distributed and are responsible for sensing the physical object and sending the data to the upper layer for processing and storage.

2) Fog layer: The second layer is the Fog layer. Located at the edge of the network, this layer is composed by a large number of fog nodes, which commonly includes routers, gateways, access points, base stations, among others.

Fog nodes, located at the edge of the network, are responsible for performing tasks such as scheduling, storing, and managing distributed computation.

3) Cloud layer: The Cloud layer is responsible for permanent storage and performing extensive computational analysis of data. Unlike the traditional Cloud architecture, in Fog Computing, the Cloud core is accessed in a periodical and controlled manner, leading to an improved utilisation of the available resources.

D. Scenario

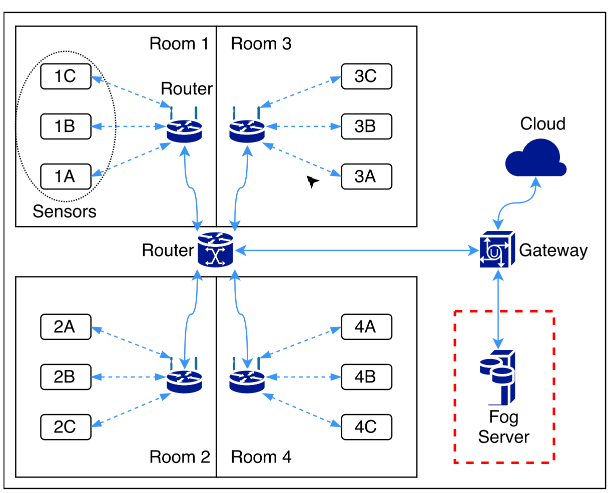

Figure 2: Illustration of the integrated Cloud-Fog hospital scenario.

In order to critically compare the current Cloud Computing infrastructure with the new paradigm named Fog Computing, both scenarios have been simulated using the *iFogSim* simulator, which is described in the next subsection. As represented in Figure 2, the healthcare system scenario is composed by four rooms with three beds each one. Each bed has one specific device application, such as an electroencephalogram (EEG), a temperature sensor, a heart rate sensor, or a glucose sensor.

In the Cloud-based scheme, each device submit its sensed data to a border router, which is located at the room. Then, another router is placed to aggregate data from other routers and then send it to a gateway. The gateway in this scenario is responsible for data forwarding to the Cloud.

When employing a Fog environment on top of the Cloud infrastructure (shown in Figure 2 in a red-dashed rectangle), a Fog server, as called in this work, is able to offer computational data processing to a particular healthcare application. In a real scenario, many Fog servers/nodes can be placed to enhance QoS of an application. To exemplify its benefits, only one Fog server has been employed in this study.

Applying this strategy, the gateway will be in charge of selecting where data shall be processed. If there are enough resources in the Fog to process the incoming data, these data are sent to the Fog; otherwise, it is sent to the Cloud. To accomplish the objective of this study, the parameters shown in Table I have been used in the study (performed by simulation).

Table I: Main simulation parameters.

Parameters	**Values**
Simulation time	400 seconds
Cloud latency	100 ms
Fog latency	50 ms
device latency	2 ms
Cost of network	0.001 - 0.05 $/MB
Cloud energy usage	150 - 400 W
Fog energy usage	70 - 130 W
Data sensing interval	5 ms

E. Simulation tools

An evaluation environment for real-time applications employing Fog Computing is necessary to enhance innovation and development of new technologies. As testbeds in real world can be very expensive, simulators prove to be efficient tools to address these problems. Proposed by Gupta *et al.*, *iFogSim* is a tool-kit for modelling and simulation of resource management written in JAVA. Programmable objective include minimising latency, energy consumption, bandwidth usage, or operational costs [18]. The simulator has been implemented on top of *CloudSim* and, apart of being the first simulator to allow IoT objects simulations, it enables simulating a Cloud environment, including its most pertinent elements such as data centres and Cloudlets [19].

IV. RESULTS ANALYSIS

In a remote Cloud infrastructure, all healthcare applications share the same link leading to a higher network traffic congestion. Such congestion impacts directly in the increase of network latency. Since the available bandwidth is divided among the service requests, each one of the later is able to transmit at a rate that is lower than the one the maximum bandwidth allows, therefore, increasing transmission delays. The effect of dividing the bandwidth among service requests as the number of running applications increases, can be observed in Figure 3. Conversely, in a Fog environment, Fog nodes/servers are placed closer to end-devices, and because of that proximity, network delay can be drastically reduced.

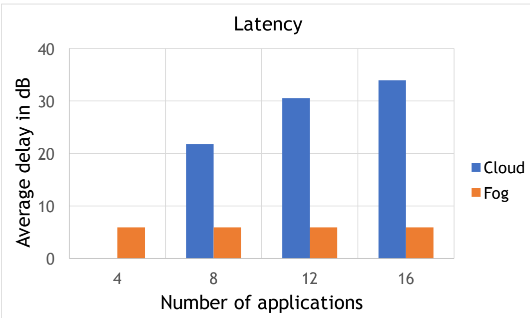

Figure 3: Average network delay (in dB) according to the number of healthcare applications.

In a Cloud model infrastructure, all the applications must submit their data to be processed in a remote Virtual Machine (VM). Usually, a single VM is allocated to handle all the services, while in a Fog scenario, multiple VMs hosted in Fog nodes may be assigned to execute a particular task at the same time. Nonetheless, as virtual machines in Fog nodes are less powerful in terms of processing capacity, the overall energy consumption is smaller than in the Cloud model. Another important advantage in Fog scenarios is the possibility of placing multiple Fog nodes to meet an application demand, which improves the system performance, since a specific service may be executed in more than one node. Figure 4 outlines this scenario.

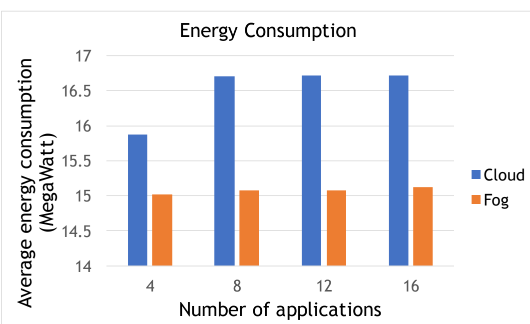

Figure 4: Average energy usage (in megaWatt) according to the number of healthcare applications.

A particular application service fragment running in Fog requires much less resources for data processing than the whole application. If such a resource is well provisioned according to its application needs, the total cost of the service may be drastically decreased since just the right amount of resources will be charged. In the Cloud scheme, that kind of plan is difficult to achieve as the configuration of virtual machines are predefined. Figure 5 shows the cost of network per megabyte.

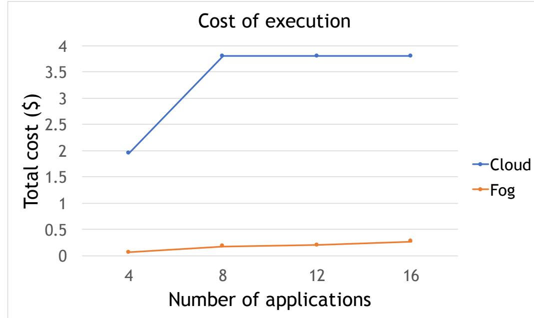

Figure 5: Overall execution network cost per megabyte according to the number of healthcare applications.

Figure 6 delineates the network congestion according to the number of application services. In a Cloud approach, as the number of sensors increase, the network traffic also increases. This rise of data sent to the Cloud for processing may lead the network to congestion due to the amount of used bandwidth. In a Fog infrastructure, all data locally generated can be preprocessed and analysed at the edge of network. In this manner, only a small part of the information may be sent to the Cloud for permanent storage. Therefore, the use of network bandwidth is much lower than the Cloud system.

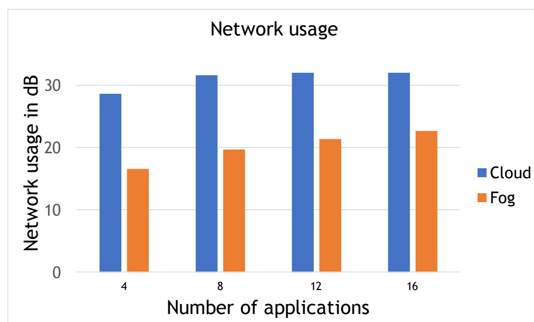

Figure 6: Total network usage (in bD) according to the number of healthcare applications.

V. Conclusion and Future Directions

In this paper, an evaluation between Cloud and Fog Computing has been performed through simulation through the *iFogSim* simulation tool that enabled the measurement of the most critical parameters regarding the use of IoT devices in healthcare applications.

The Fog paradigm plays an important role in IoT by addressing the issues related to security, confidentiality, and system reliability. This approach promises to help networks that require faster processing capacity with less delay. From the obtained results, it is easy to notice that Fog paradigm provides a significant enhancement in terms of QoS.

To the best of the authors' knowledge, the main benefit provided by the concept of Fog Computing is that it can reduce the burden in centralised systems, such as data centres employed in Cloud Computing, by enabling applications to be deployed at the edge of the network. Consequently, it avoids the need of bandwidth expenditures by offloading network traffic data from the core of the network.

In summary, Fog Computing demonstrates better performance than Cloud Computing in terms of meeting the demands of the emerging paradigms. But for certain, it cannot totally replace Cloud Computing. Nevertheless, Fog and Cloud models will complement each other while considering their own advantages and disadvantages.

Some of potential open issues regarding the integration of Cloud and Fog computing are the following:

1) Security & Trust: Relationship in a Fog environment tends to be more complex due to the large number of interconnected IoT devices. In addition, association among Fog nodes happens, mainly, dynamically. Besides all security and privacy concerns related to patients' health records, a trust management system among these devices is a critical issue.

2) Power management within the Fog: Fog nodes will have to interconnect a large number of IoT devices as well as sensors and actuators that may generate service requests at the same time. One possible solution is to deploy Fog nodes according to the demand. However, by applying this approach with Fog nodes, the total power consumption of the system may be affected by the increase of computation tasks. For that reason, proper power management within Fog nodes is very important. Further studies should consider resource and task allocation among Fog devices in an effective way in order to achieve the best use of energy in the Fog environment.

3) Multi-tenant support in Fog resources: Multi-tenancy approach is an application which is able to attend multiple clients. In a Fog environment, multi-tenancy means that available resources may be virtualised and allocated to multiple users. For this purpose, resource placement and tasks scheduling have not been fully investigated in terms of QoS requirements.

4) Pricing and Billing: Fog Computing can provide utility services like Cloud Computing. In Cloud Computing, typically, users are charged according to the horizontal scale of usage. Unlike Cloud Computing, in the Fog, vertical arrangement of resources contributes to the expenses of both users and providers to a great extent. Therefore, the pricing and billing policies in the Fog generally differ significantly from the Cloud oriented policies. Besides, due to the lack of proper pricing and billing policies of Fog-based services, users often face difficulty in identifying suitable providers for a Service Level Agreement (SLA). In such circumstances, a proper pricing and billing policy of Fog-based services will surely be considered a potential contribution in the field of Fog Computing.

Acknowledgements

This work was supported by the National Funding from the FCT - Fundação para a Ciência e a Tecnologia through the UID/EEA/50008/2013 Project; by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Centro de Referência em Radiocomunicações - CRR project of the Instituto Nacional de Telecomunicações (Inatel), Brazil; and by the Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017-5.

References

[1] M. Khalid, M. M. Yousaf, Y. Iftikhar, and N. Fatima, "Establishing the state of the art knowledge domain of cloud computing," in *Advanced Computer and Communication Engineering Technology*. Springer, 2016, pp. 1001–1014.

[2] F. Computing, "the internet of things: Extend the cloud to where the things are," 2016.

[3] C. V. Networking, "Cisco global cloud index: Forecast and methodology, 2015-2020," *White paper*, 2016.

[4] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy, and Y. Zhang, "Mobile edge cloud system: Architectures, challenges, and approaches," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–14, 2017.

[5] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[6] D. S. Linthicum, "Connecting fog and cloud computing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 18–20, March 2017.

[7] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2017.

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

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

[10] P. Mell, T. Grance *et al.*, "The nist definition of cloud computing," *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg*, 2011.

[11] L. Griebel, H. Prokosch, F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, "A scoping review of cloud computing in healthcare," *BMC Medical Informatics and Decision Making*, vol. 15, no. 1, p. 17, 2015.

[12] R. Deng, R. Lu, C. Lai, and T. H. Luan, "Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 3909–3914.

[13] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014. [Online]. Available: http://doi.acm.org/10.1145/2677046.2677052

[14] Y. Cao, S. , P. Hou, and D. Brown, "Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation." in *NAS*. IEEE Computer Society, 2015, pp. 2–11.

[15] 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," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Oct 2015, pp. 356–363.

[16] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero, and M. Nemirovsky, "Key ingredients in an iot recipe: Fog computing, cloud computing, and more fog computing," in *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Dec 2014, pp. 325–329.

[17] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*. IEEE, 2014, pp. 1–8.

[18] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "ifogsim: A toolkit for modeling and simulation of resource management techniques in internet of things, edge and fog computing environments," *arXiv preprint arXiv:1606.02007*, 2016.

[19] A. Kapsalis, P. Kasnesis, I. S. Venieris, D. I. Kaklamani, and C. Z. Patrikakis, "A cooperative fog approach for effective workload balancing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 36–45, 2017.