Journal of
Sensor and Actuator Networks

MDPI

Article

Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain

Ammar Muthanna [1,2,*], Abdelhamied A. Ateya [1,3], Abdukodir Khakimov [1], Irina Gudkova [2,4], Abdelrahman Abuarqoub [5], Konstantin Samouylov [2,4] and Andrey Koucheryavy [1]

[1] Telecommunication Networks and Data Transmission, St. Petersburg State University of Telecommunication, 193232 St. Petersburg, Russia; a_ashraf@zu.edu.eg (A.A.A.); abdukadir94@gmail.com (A.K.); akouch@mail.ru (A.K.)
[2] Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia; gudkova_ia@pfur.ru (I.G.); ksam@sci.pfu.edu.ru (K.S.)
[3] Electronics and Communications Engineering, Zagazig University, 44519 Sharqia, Egypt
[4] Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 119333 Moscow, Russia
[5] Faculty of Information Technology Middle East University Amman, 383 Amman 11831, Jordan; Aabuarqoub@meu.edu.jo
* Correspondence: ammarexpress@gmail.com; Tel.: +7-952-210-4486

Received: 27 December 2018; Accepted: 9 February 2019; Published: 18 February 2019

Abstract: Designing Internet of Things (IoT) applications faces many challenges including security, massive traffic, high availability, high reliability and energy constraints. Recent distributed computing paradigms, such as Fog and multi-access edge computing (MEC), software-defined networking (SDN), network virtualization and blockchain can be exploited in IoT networks, either combined or individually, to overcome the aforementioned challenges while maintaining system performance. In this paper, we present a framework for IoT that employs an edge computing layer of Fog nodes controlled and managed by an SDN network to achieve high reliability and availability for latency-sensitive IoT applications. The SDN network is equipped with distributed controllers and distributed resource constrained OpenFlow switches. Blockchain is used to ensure decentralization in a trustful manner. Additionally, a data offloading algorithm is developed to allocate various processing and computing tasks to the OpenFlow switches based on their current workload. Moreover, a traffic model is proposed to model and analyze the traffic indifferent parts of the network. The proposed algorithm is evaluated in simulation and in a testbed. Experimental results show that the proposed framework achieves higher efficiency in terms of latency and resource utilization.

Keywords: internet of things; fog computing; traffic; latency; SDN; OpenFlow

1. Introduction

The Internet of Thing (IoT) is an adaptive self-configuring network that enables the communication and interaction between physical objects; transforming these objects from being blind to being smart [1,2]. Recently, IoT gained significance because of the great impact it has had on all aspects of our life [3]. IoT is expected to completely change our life by introducing a wide range of applications in various fields [4]. These applications include smart home, smart cities, healthcare, smart vehicles and remote monitoring [5,6]. IoT has a high market potential as it comes with big opportunities for various sectors, such as hardware manufacturers, service providers and software developers [7].

IoT represents the third generation of the Internet that is expected to connect billions of heterogeneous devices in a smart way [8]. This large number of connected devices puts high constraints on the system structure and design in terms of [9–11]:

- Network coverage,
- High system reliability,
- Security and privacy,
- Integration with other existing communication networks,
- Traffic load, and
- Latency constraints for some applications.

To overcome these challenges and achieve higher system efficiency, capable of connecting this huge number of devices, new technologies and communication paradigms can be deployed to support IoT networks. These paradigms include distributed edge computing (e.g., Fog computing), software-defined networking (SDN), network virtualization and blockchain [12].

Edge computing is a new paradigm that aims to provide cloud services and computing capabilities, e.g., storage and processing, at the edge of the access network; one or two hops away from the end user [13]. This introduces a way of moving from huge centralized data centres to the distributed cloud units with limited capabilities [14]. Deploying edge computing for IoT networks achieves various benefits such as reducing the communication latency, providing a path for data offloading, increasing the spectral efficiency and the introduction of new services [15,16].

Fog computing is a form of edge computing that is suitable for IoT networks [17]. It acts as an extension to the cloud computing paradigm to provide processing, computing and storage capabilities. It also introduces other cloud services to the communication nodes in the vicinity of the distributed Fog nodes. Fog computing supports various types of heterogeneous devices that can connect and communicate with the distributed Fog nodes, these devices include sensors, actuators and wireless gateways [18]. Fog nodes refer to a computing unit powered by limited computational and storage resources that are deployed to serve connected devices. Fog computing IoT-enabled networks share various and significant advantages that include the improved system privacy and security, the reduction of end-to-end communication latency, higher system reliability and the reduction of traffic overhead and congestion [19,20].

The introduction of Fog computing to IoT presents new challenges. Managing and controlling Fog distributed nodes and synchronizing their operation with an IoT network that is located remotely is a challenge [21]. However, deploying an orchestrator or a controller represents an efficient solution; this is the concept behind SDN. SDN physically separates the forwarding plane and the control plane to provide a dynamic network structure [22]. The data plane represents the network part that is responsible for forwarding traffic, while the control plane is the part that makes the decision of the traffic. SDN networks generally consist of a centralized or distributed controller and distributed forwarding devices or switches. The controller connects and communicates with the network devices via an open standard interface protocol such as the OpenFlow (OF) protocol [23]. SDN is known for its ability to achieve higher system flexibility and scalability.

Blockchain is another main paradigm that was recently deployed for the IoT networks to manage the distributed edge cloud units and work against heterogeneous cybersecurity attacks [24]. Deploying the blockchain paradigm for IoT networks enables decentralization in a trustful manner. The introduction of blockchain technology to the IoT networks achieves various vital benefits that include the management of decentralized computing resources, increasing the overall flexibility of the system, achieving higher system security by preventing various cybersecurity threats and attacks, and reducing the cost of the system operation [25,26]. Blockchain technology can be described as a peer-to-peer distributed ledger that is used to record all approved events and transactions. Recently, the blockchain paradigm was used to support applications and communication networks (e.g., IoT) beside the crypto-currency systems [27].

In this work, we provide a framework for an IoT-Fog system that integrates SDN and blockchain. This system introduces a distributed edge computing layer of Fog nodes that is deployed between the distributed heterogeneous IoT nodes and the IoT centralized cloud in order to make use of various benefits of the Fog computing. The network employs a distributed SDN controller scheme with the ability to introduce blockchain technology. The SDN network consists of distributed OF switches that are deployed with some limited computing capabilities and an SDN controller that can perform resource provisioning and orchestration in synchronization with Fog orchestration. The SDN network achieves higher system performance in terms of network management, flexibility and latency performances. Moreover, a data offloading algorithm is introduced to organize and manage the offloading scheme. The proposed algorithm makes use of the available resources of the OF switches and, thus, balances the load among the core network switches. Furthermore, a traffic model for modelling and managing IoT traffic among different network parts is introduced.

The main aim of the work is to provide IoT networks with high resource utilization efficiency, high flexibility and the reduction of end-to-end latency. The system is simulated and tested over a testbed to evaluate its performance. In Section 2, the related works are introduced. Section 3 provides the proposed IoT framework details and the data offloading algorithm and traffic model. In Section 4, the simulation and testing are presented and the experimental results are provided and analyzed.

2. Background and Related Works

There is no doubt that cloud computing and edge computing represent the main base of the fifth-generation cellular network (5G), IoT networks and future smart systems [28,29]. There are many studies dedicated to the development and deployment of the edge computing units in communication networks, especially for cellular and IoT networks. Many researchers use the term cloudlet to refer to any secondary, small and limited-capability cloud units [30]. There are many other forms of the edge cloud units that include Fog nodes and the micro-cloud units and other forms [15,31].

Fog computing is considered to be the most suitable edge computing platform for IoT networks and applications. Since it was first announced by Cisco as a form of edge computing and an extension of the cellular edge computing [32], researches and studies have been developed to analyse, define, improve and integrate Fog computing. Many works that consider Fog computing for IoT have been conducted; either without the deployment of SDN technology or with SDN. Most of these works are literature reviews; in the following section(s), we consider some of these efforts.

In Reference [33], the authors developed a framework for an IoT network with Fog computing deployment. This work was mainly developed for considering IoT applications from a Fog computing point of view. The authors introduced a distributed data flow mechanism, referred to as DDF, which is programmable. The dataflow programming model was used for building different IoT applications and services. The data algorithm was validated over the open-source flow-based run time and visual programming tool, Node-RED. The testing was introduced just to validate that the architecture and algorithm are suitable. However, no performance metrics were considered.

In Reference [34], the authors developed a hierarchical computing structure for medical applications over IoT networks. The hierarchical structure consists of a centralized cloud and distributed Fog units. The proposed paradigm was introduced to partition and accommodate the machine learning methods used for health care applications over IoT networks. The computation tasks and medical data have been distributed among two computing levels in a partitioning way that increases the system availability. Furthermore, a closed loop management technique was developed that is mainly dependent on the user's condition (e.g., medical parameters). The system was validated in terms of response time and availability. Our proposed work shares the similarity of using Fog paradigm with this work, while this work mainly considers medical applications over the IoT networks and also only considers availability as a performance metric.

In Reference [35], the authors proposed an internet of vehicles (IoV) Fog-based architecture, with SDN deployed. The work is the first study that considers such a structure and combines IoV with the

Fog computing and SDN paradigms. The work mainly considers a specific problem, which is the SDN controller placement. The SDN network consists of two levels of controllers; the primary controller and secondary controller. The primary controller is a centralized one that takes the control and management task of the overall system. The secondary controller is a distributed controller dedicated to different regions of the covered area. The two controllers are physically connected. An optimization problem was solved to optimize the geographic placement of the distributed controllers. The work shares the similarity of deploying Fog computing and SDN with an IoT network with our proposed framework, while it considers only the IoV, which is a high mobility application. One main issue of this algorithm is that it has not been evaluated and that the performance was not checked. The authors only introduced a system structure.

In Reference [36], the authors developed a secure IoT system that deploys Fog computing, SDN and blockchain to enhance the security of IoT networks. The system uses SDN and blockchain to secure and control the distributed Fog architecture. Fog services have been allowed at the edge of the access network by the distributed Fog nodes. The system achieves higher latency and security efficiency since bringing computing resources at the edge of the IoT network could secure the core network traffic and minimize the end-to-end latency between IoT devices and the computing unit. The system introduces a novel security method that allows the system to adapt to the threat landscape automatically. This allows system administrators to run as many recommendations at the network edge as needed. The system was evaluated for different security scenarios and attacks. The main focus of this work is security issues, while our proposed framework is mainly concerned with the end-to-end latency performance and resources utilization. Furthermore, our developed SDN network completely differs from the SDN network used in this work since we use a distributed SDN controller with distributed resource powered OF switches. Feeding OF switches with ultra-small computing capabilities achieves various benefits to IoT networks in terms of latency and reliability. Moreover, we consider network traffic management by introducing a traffic model to control the data traffic among the network, which is also novel.

In Reference [37], the performance of the IoT networks with the Fog computing deployment is studied. A testbed of 50 IoT nodes, distributed Fog nodes and a controller was described. This testbed is used to validate the benefits of Fog computing. This work can be considered as an extension to this study, while in this work, we use powered OF switches with more capabilities and responsibilities. Furthermore, we introduce a structure of the system with the deployment of blockchain. Additionally, we introduce a data flow algorithm to manage the traffic among the proposed network.

3. IoT System Structure with Distributed Fog Computing and SDN

In this section, we introduce the proposed IoT system that comprises the distributed Fog computing with the SDN and blockchain paradigms. At first, the IoT system structure is introduced and the comprised paradigms and system components are defined. Then, a data offloading algorithm is described for the proposed structure. Finally, a traffic model for analyzing traffic among the proposed structure is introduced.

3.1. System Structure

The proposed system deploys Fog computing with blockchain and SDN to support IoT networks and applications. The system can be viewed as a three-layer system as illustrated in Figure 1. The first layer represents the device layer, which contains all IoT devices and sensor devices. These devices are used to measure and capture physical and environmental data. All devices deployed in this layer always have data to be transferred through the network. IoT devices are heterogeneous in terms of computing capabilities, i.e., storage and processing, and energy resources. These devices are battery operated and should be managed in an energy efficient way.

The second layer represents the Fog layer, which deploys Fog nodes to provide an offloading path for the captured data and enable other Fog computing benefits to the IoT network. This moves from the centralized computing scheme to the distributed computing scheme. Fog nodes are deployed at the edge of the access network and each Fog node can serve for a group of IoT devices associated with certain services and a dedicated location. The Fog node handles data forwarded from the dedicated IoT devices. Thus, the Fog layer enables data analyzing, classification and monitoring at the edge of the network. Computing results are forwarded to the higher cloud layer and a response is sent to the IoT devices in cases that required such response.

Adding distributed Fog to an IoT network provides an offloading path for the collected data and thus, reduces the data traffic at the core network. Additionally, Fog nodes provide the computing capabilities near to IoT devices and thus, reduce the end-to-end latency. Furthermore, the introduction of Fog computing increases the overall network flexibility and availability.

The top layer is the cloud layer that is represented by the remote cloud unit. The IoT cloud supports different IoT services and protocols. A service provider can integrate and connect the IoT cloud with other networks. Using the cloud layer, network clients are empowered to use, search and manage the computing resources and data. The cloud layer offers network users the ability to control and monitor the application.

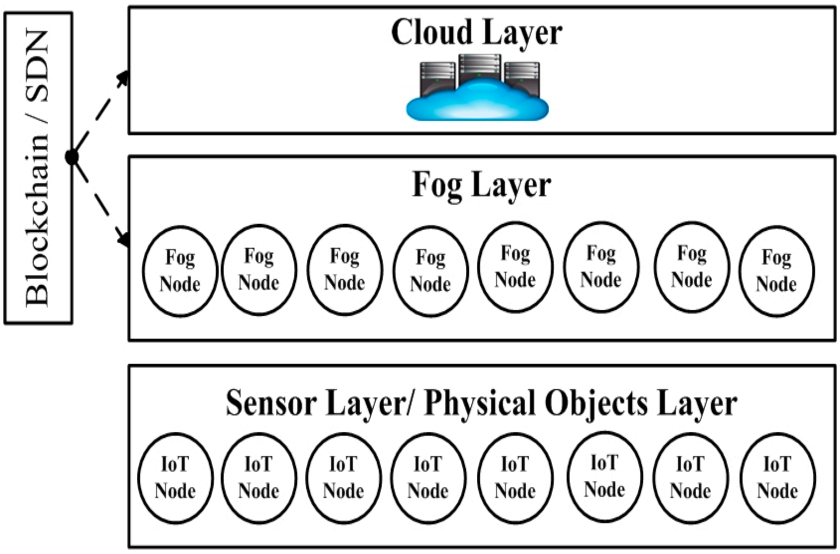

Figure 1. The main layers of the proposed Internet of Things (IoT)-Fog system.

The network also deploys two main communication paradigms, side by side with the three introduced levels. These paradigms are the SDN technology and the blockchain that are deployed to assist the system and provide control, management and security issues to the introduced system. The end-to-end system structure of the proposed IoT system is presented in Figure 2.

3.1.1. SDN Operation and Integration

The system deploys a single centralized physical SDN controller that controls and manages distributed Fog nodes and, hence, IoT devices. Figure 3 illustrates the three main layers of the deployed SDN model. The data plane of the SDN network contains all sensor nodes that could have additional recourses from the Fog nodes, while the control plane scheme is represented by the deployed SDN controller.

The SDN network also employs distributed OF switches that are powered by limited computing capabilities. These switches can provide some limited services in addition to the switching functions. The SDN controller is able to configure and manage all deployed OF switches via a proper interface, i.e., any supported version of OF protocol [38]. The SDN controller employs a clustering algorithm introduced in Reference [39] so that each Fog node or a group of Fog nodes are associated with a distributed SDN controller. Distributed SDN controllers deploy packet migration function to provide security over the databases and work against saturation attacks [36]. A distributed SDN network allows the network operator to program and manage Fog nodes and IoT devices via application programming interfaces (APIs). All distributed SDN controllers are connected by the blockchain to provide a high-security level to the proposed IoT network.

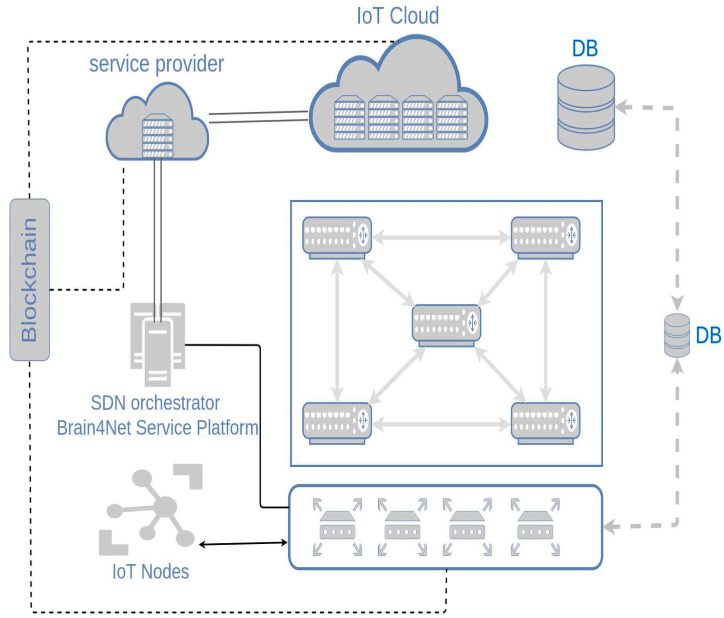

Figure 2. The system structure of the proposed IoT-Fog system with Software Designed Networking (SDN)/blockchain.

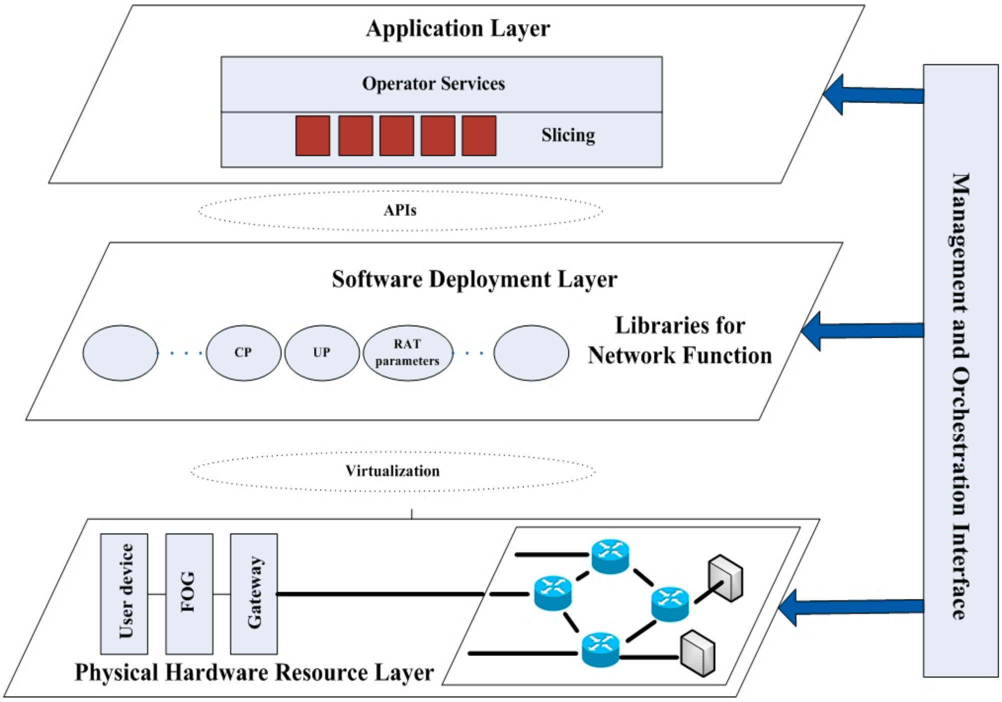
Application Layer
Operator Services
Slicing
APIs
Software Deployment Layer
CP
UP
RAT parameters
Libraries for Network Function
Virtualization
User device
FOG
Gateway
Physical Hardware Resource Layer
Management and Orchestration Interface

Figure 3. The layers of an SDN network.

3.1.2. Blockchain Operation

Distributed Fog based SDN nodes are connected and managed via the blockchain technology that is used for updating flow table in a secure manner. Furthermore, the cloud layer is split into distributed clouds through the blockchain.

Introducing peer-to-peer paradigm (i.e., blockchain) to the distributed computing achieves various benefits to IoT network such as working against heterogeneous attacks and, thus, increases the overall system security, leading to increasing the flexibility of the system, achieving the required scalability of the IoT networks, and increasing the overall system availability.

In this paper, studying blockchain is limited to its functions as a structural component; other aspects will be studied in future publications. This is because the main objective of this work is the end-to-end latency, not the analysis of security issues.

3.2. Data Offloading Algorithm

The proposed system works based on the data flow algorithm illustrated in Figure 4. The network operation goes through various steps. The first step is authentication, as the IoT node should be authorized. The IoT node communicates directly with the IoT cloud to be authorized. Then, the IoT cloud performs the authentication process and identifies the device to be authorized.

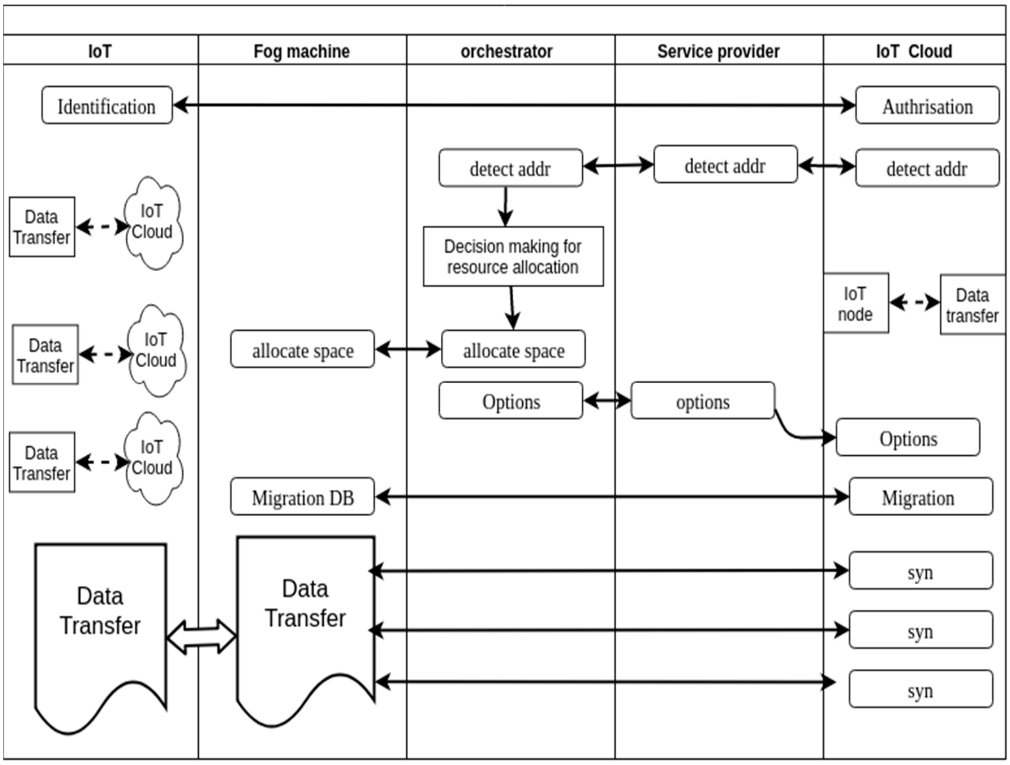

Figure 4. The data flow algorithm.

The next step is address detection, in which the cloud calls the service provider to determine the location of the IoT. For this purpose, the service provider refers to the SDN orchestrator, which makes an investment to locate the IoT device. Moreover, the SDN orchestrator populates the routing table with different routing paths between the IoT node and the cloud and locates all OF switches that are dedicated to this communication.

- As the system mainly considers resource utilization, it makes use of all the available resources. Consequently, the SDN controller allows the OF switches to handle some processing and computing tasks for the IoT forwarded data after the Fog level. The SDN controller estimates the OF switches with the available resources upon checking certain parameters. These parameters are the following:
- IoT traffic,
- Transit traffic,

- Traffic access type,
- Time delay constraints,
- Processing power for servicing the IoT data, and
- The current state of the OF switches in terms of traffic and resources.

The SDN controller decides the possibility of enabling the IoT data, passed to the core network through the Fog layer, to be a part of the available resources of the OF switches by optimizing the previous parameters and, thus, informs the selected switches. The orchestrator creates a virtual machine on the selected OF switches that are used for data processing. The next step is database migration. The IoT Cloud, through the service provider, migrates the database for servicing the IoT group over certain OF switches. The network continues working and OF switches aggregate and synchronize the IoT data with the cloud.

Handling computing tasks to OF switches achieves various benefits to our proposed IoT system structure, these benefits include the following:

- Reduction of communication latency,
- Channel load reduction,
- Useful for anti-persistence traffic in the core network, and
- Efficient resource utilization.

3.3. Traffic Model

It is clear that reducing a part of the subscriber traffic in the local cloud reduces the total traffic, and, thus, increases the quality of service (QoS) of the traffic served by the network. Introducing Fog nodes with SDN to IoT networks has a great impact on the network traffic performance and efficiency. To enhance this performance, a Fog computing-based traffic model is introduced. This traffic model reflects the impact of introducing Fog computing on the traffic services over the network.

In order to estimate the efficiency of introducing Fog nodes (i.e., Fog computing) on the traffic performance and efficiency, the delivery time of the data offloaded is considered as the main metric, which reflects the impact of the Fog computing on the traffic service in the network.

The proposed traffic model considers the operation of the access network, the core network and the application server as queuing processes. The traffic model assumes a G/G/1 queuing system and also assumes that the main characteristic of the access network, core network and an application server is the delivery time T [40]. Figure 5 illustrates the proposed traffic model based on the G/G/1 queuing model.

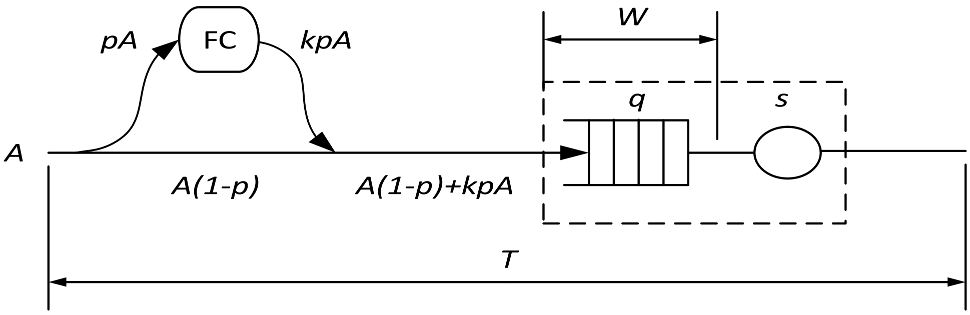

Figure 5. The traffic service model.

The total traffic originated by a group of users (e.g., IoT nodes) in a cell or a base station has the intensity *A*. The user traffic may be forwarded to a nearby Fog node; the probability that this event happens is assumed to be *P*. This reduces the amount of traffic handled to the access network. Thus, the traffic served by the access network is equal to x, where x is calculated as follows:

$$x = A\ (1 - P) \quad (1)$$

The intensity of the traffic handled by the Fog node is x', where x' can be calculated as follows:

$$x' = AP \tag{2}$$

As a result, the traffic service of the Fog computing node originates the traffic that is forwarded to the core network with intensity x'', where x'' is calculated as follows:

$$x'' = APK, \qquad 0 < K \leq 1 \tag{3}$$

where, K is the probability constant with a value between zero and one. For K with any value below one, the amount of traffic forwarded to the core network is reduced and, thus, the Fog unit achieves traffic reduction and reduces the network congestion. The zero value of the constant K corresponds to the removal of the Fog computing layer.

The total delivery time T can be calculated as follows [41]:

$$T = W + s = \ \rho s/(2\ (1-\rho)\ )\ \varepsilon + s, \quad \rho = as \tag{4}$$

$$a = x + x'' = A(1-P) + APK \tag{5}$$

where, s is the service time and ε is the form factor [41]. The efficiency of introducing Fog computing nodes on the traffic is E and can be calculated as the percentage decrease in the queuing delay of the ordinary IoT network (i.e., without the introduction of Fog computing nodes) and due to the existence of the Fog computing layer.

$$E = 1 - E_F/E_O = 1 - (1-\rho)/(1-\rho(1-P))(1-P) \tag{6}$$

where, E_F is the efficiency in the existence of Fog computing layer and E_o is the efficiency of the ordinary IoT system with no Fog layer. The maximum value of E corresponds to the maximal efficiency of using Fog computing nodes. Figure 6 shows the impact of the change of the probability of traffic forwarding to the Fog cloud layer on the efficiency E, for different values of ρ. As the probability increases, the Fog nodes can handle a higher amount of traffic and, thus, the efficiency increases. Furthermore, the dependence shows that the efficiency grows rapidly in the case of a high traffic value and grows slowly in the case of a small traffic value. Additionally, the efficiency varies from 0, when no traffic is directed to the Fog cloud, to 1, when all traffic is directed to the Fog cloud.

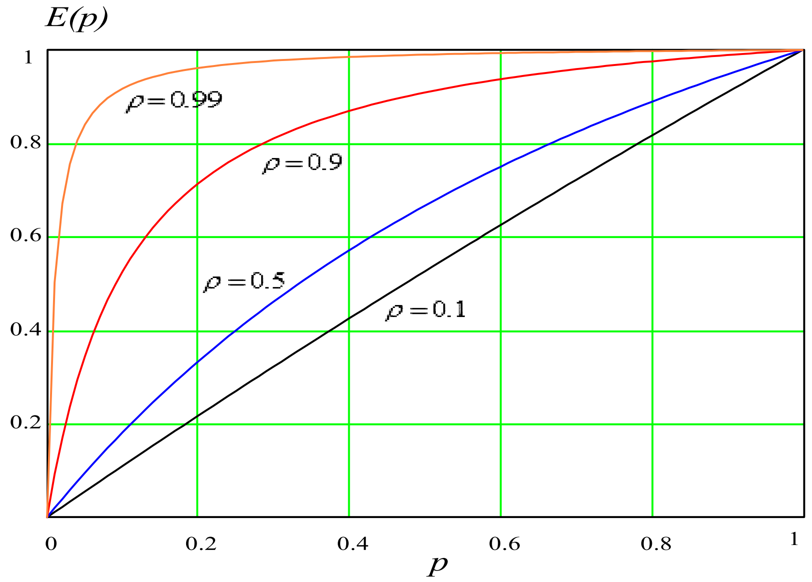

Figure 6. The traffic efficiency for the IoT based Fog system.

4. Performance Evaluation

In this section, the performance of the proposed IoT framework and all associated algorithms are evaluated. The proposed IoT-Fog system is experimentally tested in a testbed. Various parameters are considered as performance metrics. Moreover, the proposed offloading and traffic algorithms are simulated and the obtained results are analyzed.

4.1. Experiment Setup

In order to evaluate the performance of the proposed system structure and the data offloading algorithm, the following experiment is conducted. We construct the system shown in Figure 2, while the considered network components are presented in Table 1, with the introduction of the specifications of each component. Since the blockchain was considered as only a structural component in this work, it is not considered in the simulation part and the developed testbed doesn't deploy such technology. The x86 architecture is deployed to act as an OF switch, which is able to support processing and computing tasks [42]. We employ 48 Raspberry nodes; each of them represents an IoT node. The 48 Raspberry nodes act as traffic generators that generate data traffic with an average of 6 per each node. The application layer supports the MQTT and CoAP protocols [43].

Table 1. The experimental parameters and device specifications.

Device	Specifications	
IoT-Cloud	Vendor	Fujitsu
	CPU	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz
	Core	32
	RAM	48 GB
Service provider	Vendor	lanner
	CPU	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
	Core	12
	RAM	32 GB
Orchestrator/controller	Brain4Net Service Platform	
OF Switch	Vendor	lanner
	CPU	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
	Core	12
	RAM	40 GB
IoT-Node	Raspberry pi 3	

The system is also simulated over the iFogSim simulator, which is a reliable Java-based simulation environment for simulating IoT networks with a distributed Fog computing structure [44]. The iFogSim is built over the CloudSim environment and for the simulation process of the proposed system; CloudSim SDN is also involved in the SDN network [45]. CloudSim SDN is also a reliable Java-based environment; built over the CloudSim [46].

The system is simulated over a machine with an Intel Core i5 processor, with a speed of 3.07 GHz and a memory of 16 GB. The considered simulation parameters are introduced in Table 2.

For the performance evaluation of the proposed system, the following performance metrics are considered for both the simulation and experimental works; resources utilization (e.g., storage, processing and energy) and the end-to-end latency.

Table 2. The simulation parameters.

Parameter	Description	Value
Fog Node		
Upstream bandwidth	BW_{UP}	500 Mbps
Downstream bandwidth	BW_{Down}	10,000 Mbps
Storage capabilities	RAM	6144 MB
Processing capabilities	CPU	30,000 MIPS
Communication latency to the ISP gateway	$d_{Fog\text{-}Gateway}$	4 ms
Communication latency to IoT device	$d_{Fog\text{-}Node}$	1ms
Cloud		
Upstream bandwidth	BW_{UP}	10,000 Mbps
Downstream bandwidth	BW_{Down}	10,000 Mbps
Storage capabilities	RAM	40,960 MB
Processing capabilities	CPU	30,000 MIPS
Communication latency to the ISP gateway	$d_{Cloud\text{-}Gateway}$	100 ms
ISP Gateway		
Upstream bandwidth	BWUP	10,000 Mbps
Downstream bandwidth	BWDown	10,000 Mbps
Storage capabilities	RAM	8192 MB
Processing capabilities	CPU	5000 MIPS
IoT Node		
Upstream bandwidth	BW_{UP}	200 Mbps
Downstream bandwidth	BW_{Down}	250 Mbps
Storage capabilities	RAM	2048 MB
Processing capabilities	CPU	1500 MIPS

4.2. Experimental Results

In order to evaluate the performance of deploying the distributed Fog computing and SDN paradigm, the system is simulated for the three considered cases. In the first case, the system is simulated without the deployment of the distributed Fog computing and an SDN network. In this case, distributed IoT devices had to communicate with the remote cloud and no nearby computing capabilities are provided. The second case represents the system with the distributed Fog computing layer and without the deployment of an SDN network. In this case, distributed IoT devices can use the nearby Fog computing capabilities. The final case represents the proposed IoT network with the deployment of distributed Fog computing controlled by an SDN network. Table 3 summarizes the considered case specifications.

Table 3. The considered simulation cases.

Case	Deployed Communication Technology
Case (1)	- Centralized Cloud computing
Case (2)	- Centralized Cloud computing, and - Distributed Fog computing
Case (3)	- Cloud Computing, - Distributed Fog computing, and - SDN

Figures 7–9 illustrate the simulation results in terms of resources utilization. Figure 7 illustrates the amount of storage used by the system in the three considered cases. As the results indicate, the deployment of Fog computing achieves higher utilization performance of storage resources than the IoT system with only centralized cloud computing. Moreover, the proposed IoT system with distributed Fog computing and an SDN network achieves higher performance than the previously considered cases in terms of storage resources utilization.

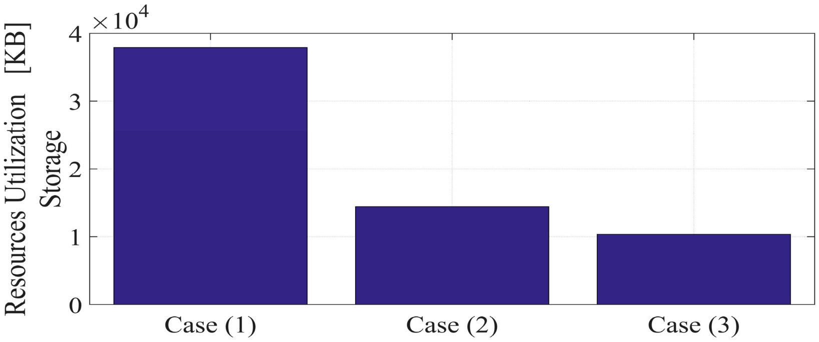

Figure 7. The average resources utilization in terms of storage for the considered simulation cases.

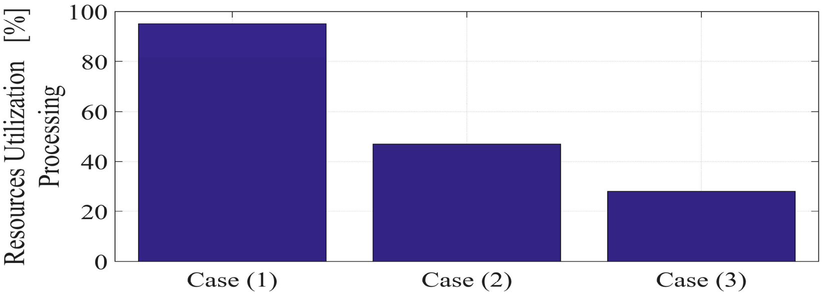

Figure 8. The average resources utilization in terms of processing for the considered simulation cases.

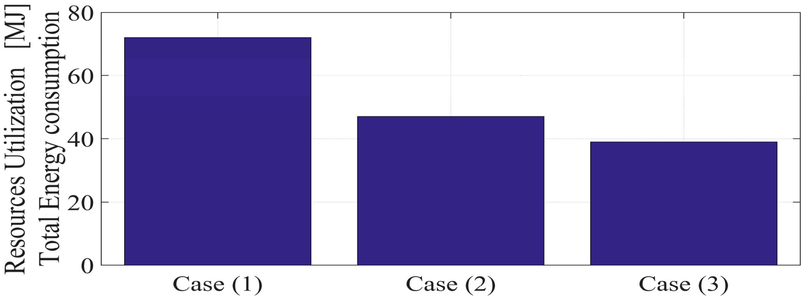

Figure 9. The average resources utilization in terms of energy for the considered simulation cases.

Figure 8 illustrates the utilization performances of the processing resources for each considered case. The proposed system utilizes the processing resources in an efficient way with higher performance than other considered systems. Figure 9 provides the total energy consumed for computing tasks by all network elements in each considered case based on the energy model introduced in Reference [47]. The deployment of SDN with distributed Fog computing achieves a higher energy efficiency of the IoT network and thus, utilize the energy resources more efficiently.

Figure 10 provides the end-to-end system latency for each considered case. The results indicate that the proposed system achieves a higher latency efficiency. Thus, the proposed IoT system achieves higher efficiency in terms of computing resources utilization (e.g., processing, storage and energy) and latency. This is because of the deployment of the distributed edge computing paradigm brings the computing resources near IoT devices. Additionally, deploying an SDN for controlling and managing the IoT-Fog network is the key solution for performance enhancement. This is because of the previously mentioned benefits of SDN based networks.

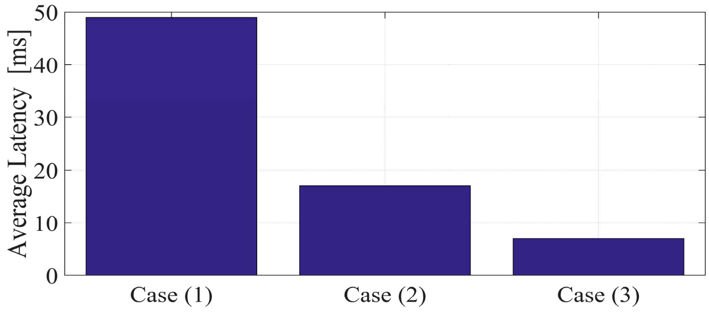

Figure 10. The average end-to-end latency for the considered simulation cases.

4.3. Experimental Results

Figure 11 illustrates the percentage of the average CPU load of the OF switches in two considered cases. In the first case, the network is operated without the Fog layer, this puts a great load on the OF switches. In the second case, the Fog nodes are deployed. The results indicate the high performance achieved in the case of Fog deployment.

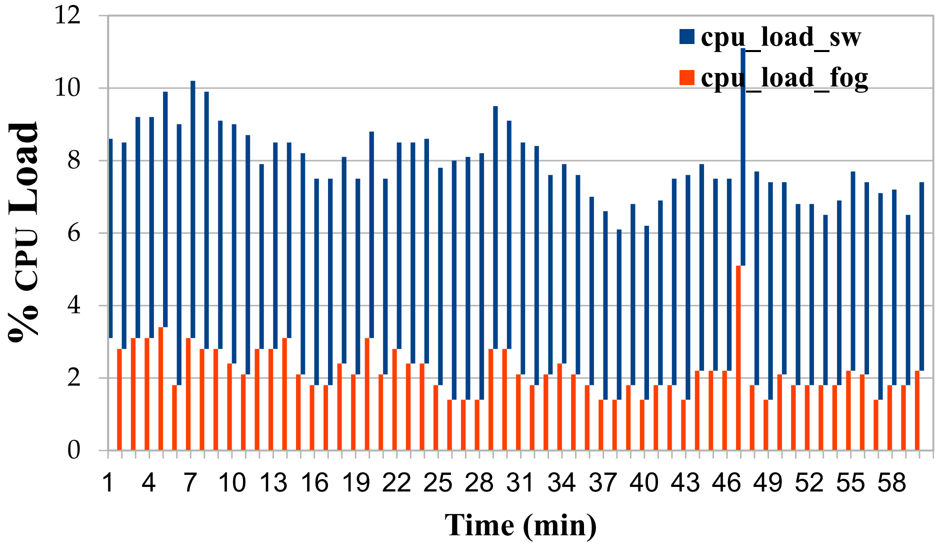

Figure 11. The percentage CPU-load for the IoT traffic and processing for the Open Flow switches.

Figure 12 illustrates the total latency of IoT traffic in the case of the network being operated without the Fog and SDN. In this case, the IoT nodes directly communicate with the IoT cloud. Figure 13 illustrates the latency for the proposed system where Fog nodes and an SDN network are deployed. By comparing the two figures, we can see vast variations in the latencies in both cases. Employing Fog nodes and an SDN network with the enabled processing capabilities of OF switches achieves a high reduction in the communication latency of IoT data and the better utilization of the computing resources, which can be considered the main benefit of the proposed system structure.

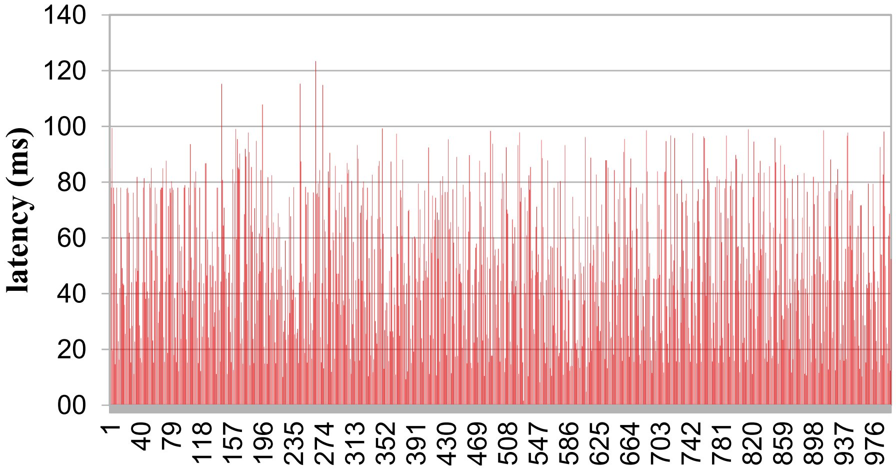

Figure 12. The communication latency in case of direct access to the IoT cloud.

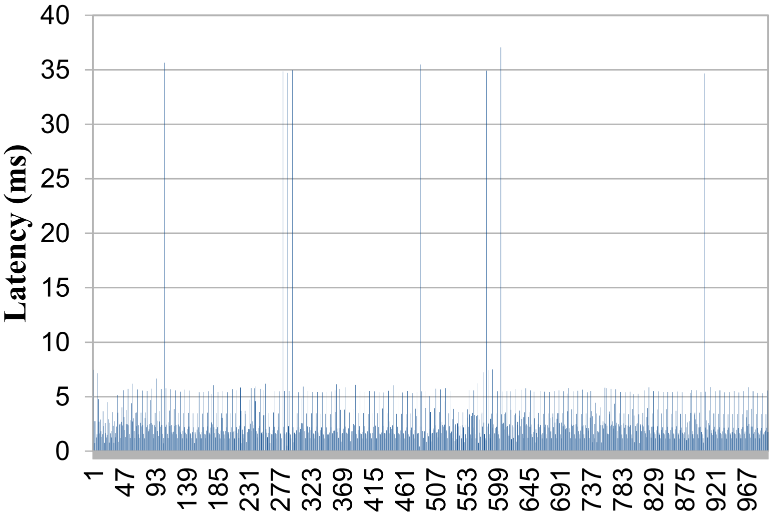

Figure 13. The communication latency for the IoT-Fog system.

5. Conclusions

Employing distributed Fog computing for IoT networks achieves various benefits since it brings the cloud computing capabilities (e.g., computing, storage and processing) near IoT nodes. This work has introduced a framework of the IoT system that deploys distributed Fog computing with the SDN and blockchain paradigms. The SDN employs a physical centralized/logical distributed controller with distributed OF switches to manage and control distributed Fog computing. The distributed OF switches have been empowered with limited resources that can be used for assisting forwarded traffic. The introduction of an SDN achieves higher flexibility and higher performance in utilizing computing resources. The work provides a novel offloading mechanism that handles certain processing and computing tasks to OF switches to reduce the data latency and achieve other benefits. The data offloading algorithm for controlling and managing data offloading over the proposed system was developed with the traffic model. The proposed system was simulated over a reliable environment and also experimentally evaluated via a developed testbed. Simulation and experimental results validate the system and ensure the efficiency claims.

Author Contributions: Conceptualization, A.A.A., A.M. and A.K. (Andrey Koucheryavy); methodology, A.K. (Andrey Koucheryavy) and K.S.; software, A.K. (Abdukodir Khakimov) and I.G.; validation, A.A.A., A.M. and A.A.; formal analysis, A.K. (Abdukodir Khakimov), A.M. and A.A.A.; investigation, I.G.; resources, A.A. and K.S.; data curation, A.K. (Abdukodir Khakimov); Writing—Original Draft preparation, A.A.A.; Writing—Review and Editing, A.A.A, A.M. and A.K. (Andrey Koucheryavy); visualization, A.A.; supervision, A.K. (Andrey Koucheryavy) and K.S.; project administration, A.M.; funding acquisition, I.G.

Funding: The publication was supported by the Ministry of Education and Science of the Russian Federation (project No. 2.882.2017/4.6).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Iannacci, J. Internet of things (IoT); internet of everything (IoE); tactile internet; 5G–A (not so evanescent) unifying vision empowered by EH-MEMS (energy harvesting MEMS) and RF-MEMS (radio frequency MEMS). *Sens. Actuators A Phys.* **2018**, *272*, 187–197. [CrossRef]
2. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
3. Abuarqoub, A.; Abusaimeh, H.; Hammoudeh, M.; Uliyan, D.; Abu-Hashem, M.A.; Murad, S.; Al-Jarrah, M.; Al-Fayez, F. A survey on internet of things enabled smart campus applications. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017.
4. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [CrossRef]
5. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
6. Farhan, L.; Kharel, R.; Kaiwartya, O.; Hammoudeh, M.; Adebisi, B. Towards green computing for Internet of things: Energy oriented path and message scheduling approach. *Sustain. Cities Soc.* **2018**, *38*, 195–204. [CrossRef]
7. Lund, D.; MacGillivray, C.; Turner, V.; Morales, M. *Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand*; International Data Corporation: Framingham, MA, USA, 2014.
8. Li, S.; Xu, L.; Zhao, S. 5G internet of things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [CrossRef]
9. Mihovska, A.; Sarkar, M. Smart Connectivity for Internet of Things (IoT) Applications. In *Proceedings of the New Advances in the Internet of Things*; Springer: Cham, Switzerland, 2018; pp. 105–118.
10. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
11. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319. [CrossRef]
12. Muhizi, S.; Shamshin, G.; Muthanna, A.; Kirichek, R.; Vladyko, A.; Koucheryavy, A. Analysis and performance evaluation of SDN queue model. In *Proceedings of the International Conference on Wired/Wireless Internet Communication*; Springer International Publishing: Cham, Switzerland, 2017; pp. 26–37.
13. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
14. Satyanarayanan, M. The Emergence of Edge Computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
15. Ateya, A.A.; Vybornova, A.; Kirichek, R.; Koucheryavy, A. Multilevel cloud based Tactile Internet system. In Proceedings of the IEEE 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 105–110.
16. Ansari, N.; Sun, X. Mobile edge computing empowers Internet of Things. *IEICE Trans. Commun.* **2018**, *101*, 604–619. [CrossRef]
17. Negash, B.; Rahmani, A.M.; Liljeberg, P.; Jantsch, A. Fog Computing Fundamentals in the Internet-of-Things. In *Fog Computing in the Internet of Things*; Springer International Publishing: Cham, Switzerland, 2018; pp. 3–13.
18. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
19. Naranjo, P.G.; Pooranian, Z.; Shamshirband, S.; Abawajy, J.H.; Conti, M. Fog over Virtualized IoT: New Opportunity for Context-Aware Networked Applications and a Case Study. *Appl. Sci.* **2017**, *7*, 1325. [CrossRef]

20. Byers, C.C. Architectural imperatives for Fog computing: Use cases, requirements, and architectural techniques for FOG-enabled IoT networks. *IEEE Commun. Mag.* **2017**, *55*, 14–20. [CrossRef]
21. Hosseinian-Far, A.; Ramachandran, M.; Slack, C.L. Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living. In *Technology for Smart Futures*; Springer International Publishing: Cham, Switzerland, 2018; pp. 29–40.
22. Cui, L.; Yu, F.R.; Yan, Q. When big data meets software-defined networking: SDN for big data and big data for SDN. *IEEE Netw.* **2016**, *30*, 58–65. [CrossRef]
23. Ateya, A.A.; Muthanna, A.; Gudkova, I.; Abuarqoub, A.; Vybornova, A.; Koucheryavy, A. Development of Intelligent Core Network for Tactile Internet and Future Smart Systems. *J. Sens. Actuator Netw.* **2018**, *7*, 1. [CrossRef]
24. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
25. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
26. Banafa, A. IoT and Blockchain Convergence: Benefits and Challenges. In *IEEE Internet of Things*; IEEE: Piscataway, NJ, USA, 2017.
27. Peter, H.; Moser, A. Blockchain-Applications in Banking & Payment Transactions: Results of a Survey. *Eur. Financ. Syst.* **2017**, *2017*, 141.
28. Uddin, M.; Mukherjee, S.; Chang, H.; Lakshman, T.V. SDN-based Multi-Protocol Edge Switching for IoT Service Automation. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 2775–2786. [CrossRef]
29. Alliance, N.G.M.N. *5G White Paper*; Next Generation Mobile Networks: Frankfurt, Germany, 2017.
30. Ateya, A.A.; Muthanna, A.; Koucheryavy, A. 5G framework based on multi-level edge computing with D2D enabled communication. In Proceedings of the 2018 IEEE 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea, 11–14 February 2018; pp. 507–512.
31. Wang, S.; Tu, G.H.; Ganti, R.; He, T.; Leung, K.; Tripp, H.; Warr, K.; Zafer, M. Mobile micro-cloud: Application classification, mapping, and deployment. In *Proceedings of the Annual Fall Meeting of ITA (AMITA)*; Imperial College London: London, UK, 2013.
32. Computing, F. *The Internet of Things: Extend the Cloud to Where the Things Are*; CISCO: San Jose, CA, USA, 2015.
33. Giang, N.K.; Blackstock, M.; Lea, R.; Leung, V.C. Developing IoT applications in the Fog: A distributed dataflow approach. In Proceedings of the 2015 IEEE 5th International Conference on the Internet of Things (IOT), Seoul, Korea, 26–28 October 2015; pp. 155–162.
34. Azimi, I.; Anzanpour, A.; Rahmani, A.M.; Pahikkala, T.; Levorato, M.; Liljeberg, P.; Dutt, N. HiCH: Hierarchical Fog-assisted computing architecture for healthcare IoT. *ACM Trans. Embed. Comput. Syst.* **2017**, *16*, 174. [CrossRef]
35. Borcoci, E.; Ambarus, T.; Vochin, M. Distributed Control Plane Optimization in SDN-Fog VANET. *ICN* **2017**, *2017*, 135.
36. Sharma, P.K.; Chen, M.Y.; Park, J.H. A software defined Fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2018**, *6*, 115–124. [CrossRef]
37. Khakimov, A.; Muthanna, A.; Muthanna, M.S.A. Study of Fog computing structure. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 29 January–1 February 2018; pp. 51–54.
38. Rofie, S.A.; Ramli, I.; Redzwan, K.N.; Hassan, S.M.; Ibrahim, M.S. OpenFlow Based Load Balancing for Software-Defined Network Applications. *Adv. Sci. Lett.* **2018**, *24*, 1210–1213. [CrossRef]
39. Kirichek, R.; Vladyko, A.; Zakharov, M.; Koucheryavy, A. Model networks for internet of things and SDN. In Proceedings of the 2016 IEEE 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31 January–3 February 2016; pp. 76–79.
40. Kleinrock, L. *Queueing Systems, Volume 2: Computer Applications*; Wiley: New York, NJ, USA, 1976.
41. Iversen, V.B. *Teletraffic Engineering Handbook*; International Telecommunication Union: Geneva, Switzerland, 2005; p. 16.
42. Vogl, S.; Eckert, C. Using hardware performance events for instruction-level monitoring on the x86 architecture. In Proceedings of the 2012 European Workshop on System Security EuroSec, Bern, Switzerland, 10 April 2012.

43. Karagiannis, V.; Chatzimisios, P.; Vazquez-Gallego, F.; Alonso-Zarate, J. A survey on application layer protocols for the internet of things. *Trans. IoT Cloud Comput.* **2015**, *3*, 11–17.
44. Gupta, H.; Vahid Dastjerdi, A.; Ghosh, S.K.; Buyya, R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Softw. Pract. Exp.* **2017**, *47*, 1275–1296. [CrossRef]
45. Kumar, R.; Sahoo, G. Cloud computing simulation using CloudSim. *arXiv*, 2014; arXiv:1403.3253.
46. CloudSimSDN Project. Available online: https://github.com/jayjmin/cloudsimsdn (accessed on 10 September 2018).
47. Taneja, M.; Davy, A. Resource aware placement of IoT application modules in Fog-Cloud Computing Paradigm. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 1222–1228.