Article

Secure IoT network structure based on distributed Fog computing, with SDN/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; akhaimov@hs-mittweida.de; akouch@mail.ru

[2] Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia; gudkova_ia@pfur.ru; ksam@sci.pfu.edu.ru

[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, 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

Abstract: IoT is a new communication paradigm that gains a very high importance in the past few years. This communication paradigm supports various heterogeneous applications in many fields and with the dramatic increase of the number of sensor devices, it becomes a demand. Designing IoT networks faces many challenges that include security, massive traffic, high availability, high reliability and energy constraints. Thus, new communication technologies and paradigms should be deployed for IoT networks to overcome these challenges and achieve high system performance. Distributed computing techniques (e.g. fog and MEC), software defined networking (SDN), network virtualization and blockchain are common recent paradigms that should be deployed for IoT networks, either combined or individually, to achieve the main requirements of the IoT networks at a high system performance. Fog computing is a form of edge computing that has been developed to provide the computing capabilities (e.g. storage and processing) at the edge of the access network. Employing Fog computing in IoT networks, as an intermediate layer between IoT devices and the remote cloud, becomes a demand to make use of the edge computing benefits. In this work, we provide a framework for the IoT system structure that employs an edge computing layer of Fog nodes controlled and managed by SDN network with the blockchain technology to achieve a high level of security for latency sensitive IoT applications. The proposed system employs SDN network with distributed controllers and distributed OpenFlow switches; these switches are enabled with limited computing and processing capabilities. Furthermore, a data offloading algorithm is developed to allocate different processing and computing tasks to the distributed OpenFlow switches with available resources. Moreover, a traffic model is proposed to model and analyze the traffic among different parts of the network. The proposed work achieves various benefits to the IoT network, such as the latency reduction, security improvement and high efficiency of resources utilization. The proposed algorithm is simulated and also the proposed system is experimentally tested over a developed testbed to validate the proposed structure. Experimental results show that the proposed system achieves higher efficiency in terms of latency, security and resource utilization.

Keywords: Internet of Things; Fog computing; Security; Blockchain; Traffic; latency; SDN; OpenFlow

1. Introduction

With the dramatic increase of the number of physical objects (e.g. sensors) connected to the Internet, Internet of Thing (IoT) become a high demand [1]. IoT is an adaptive self configuring network that enables the communication and interaction between physical objects; this transforms these objects from being blind to be smart [2]. Recently, IoT gains a very high significance because of the great impact of all life fields [3]. IoT is expected to completely change our life by introducing wide range of applications in various fields [4]. These applications include smart home, smart cities, health care, smart vehicle and remote monitoring [5, 6]. The IoT technology has a high market impact as it comes with big market opportunities for various sectors such as hardware manufacturers, service providers and software developers [7].

The IoT technology is always defined by the three-layer reference model as illustrated in figure 1. The IoT architecture may be viewed as a Perception layer, Network layer, and Application layer [8]. Two more layers may be deployed around the application layer; Middleware layer and Business layer [9]. The perception layer represents the bottom layer that contains the IoT nodes deployed for perceiving data from the surrounding environment. Thus, this layer is mainly responsible for data sensing and data collection. The network layer is the middle layer that connects the perception layer and the application layer. This layer contains all network components and protocols that are deployed for forwarding data perceived to the application layer. The top layer is application layer that provides the overall management of the data perceived. This layer is responsible for presenting data in a form of an application [10].

IoT represents the third generation of the Internet that is expected to connect billions of heterogeneous devices in a smart way [11]. This large number of connected devices puts high constraints on the system structure and design [12]. These challenges include the following [13, 14]:

1- Network coverage,
2- Support of heterogeneous devices and different communication standards,
3- High system reliability,
4- Security and privacy,
5- Integration with other existing communication networks,
6- Traffic load, and
7- Latency constraints for some applications.

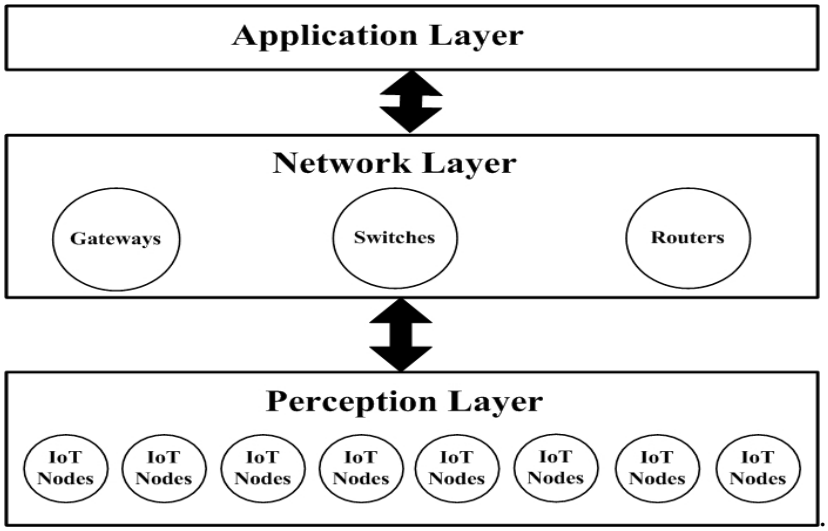

Figure 1. IoT reference model.

To overcome these challenges and achieve higher system efficiency, capable of connecting this huge number of devices, new technologies and communication paradigms should be deployed to serve for the IoT networks. These paradigms include the distributed edge computing (e.g. Fog computing), software defined networking (SDN), network virtualization and blockchain [15].

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 [16]. This introduces a way of moving from the centralized huge data centers to the distributed cloud units with limited capabilities [17]. Deploying the edge computing for the IoT networks achieves various benefits that include the following [18, 19]:

1- Higher system bandwidth,
2- Reduced communication latency,
3- Providing a path for data offloading, and
4- Introduction of new services.

Fog computing is a form of edge computing that is suitable for IoT networks [20]. It introduces a new computing paradigm that acts as an extension to the cloud computing paradigm able to provide processing, computing and storage capabilities. It also introduces other cloud services to the communication nodes in vicinity to the distributed Fog nodes. Fog computing supports various types of heterogeneous devices that can connect and communicate with Fog nodes, these devices include sensors, actuators and wireless gateways [21]. Fog node is a computing unit powered by limited computational and storage resources that are deployed to serve for connected devices. Fog computing IoT- based networks share various and significant advantages that include the following [22, 23]:

1- Improving system privacy,
2- High system security,
3- High system reliability,
4- Achieving higher latency efficiency,
5- System lightness, and
6- Reduction of traffic overhead and congestion.

However, fog computing paradigm achieves various benefits to IoT networks; it introduces a much complex scheme to be managed. Managing and controlling Fog distributed nodes, and synchronizing their operation with the IoT cloud that is located remotely is a challenge [24]. Deploying an orchestrator or a controller represents an efficient solution. This is the concept behind SDN.

SDN is a new paradigm that physically separates the forwarding plane and the control plane to provide a dynamic network structure [25]. 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 scheme and distributed forwarding devices or switches. The controller connects and communicates with the network devices via an open standard interface protocol such as OpenFlow protocol [26]. SDN achieves higher system flexibility and scalability, which makes it considered as a part of all recently developed communication systems.

Blockchain is another main paradigm that is recently deployed for the IoT networks to manage the distributed edge cloud units and work against the heterogeneous cyber security attacks [27]. Deploying blockchain paradigm for IoT networks enables the decentralization in a trustful manner. The introduction of blockchain technology to the IoT networks achieves various vital benefits that include the following [28, 29]:

1- Management of decentralized computing resources,
2- Increasing the overall flexibility of the system,
3- Achieving higher system security, by preventing various cyber security threats and attacks, and
4- Reducing the cost of the system operation.

The blockchain technology can be defined as the peer-to-peer distributed ledger that is used to record approved events and transactions. It can be represented by a distributed database or data servers that contains all approved and shared data among all participants [30]. Participants in turn must approve the new added entities; thus, blockchain guarantee approved transactions and no

interruption of the stored data without verifications. Recently, blockchain paradigm turned to support applications and communication networks (e.g. IoT) beside the crypto-currency systems [31].

In this work, we provide a framework for an IoT-Fog based system with the enabling of SDN/Blockchain paradigms. The system introduces a distributed edge computing layer of Fog nodes deployed between the distributed heterogeneous IoT nodes and the IoT centralized cloud to make use of various benefits of the fog computing. The network employs a distributed SDN controller scheme with the blockchain technology. The SDN network consists of distributed OpenFlow switches (OF) that are deployed with some limited computing capabilities and SDN controller that can perform resource provisioning and orchestration in synchronization with Fog orchestration. The SDN/blockchain network achieves higher system performance in terms of network management and security. 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, balance the load among core network switches. Furthermore, a traffic model for modeling and managing IoT traffic among different network parts is introduced.

The main vision of the work is to provide an IoT network with high resource utilization efficiency, high security and reduction of end-to-end latency. The system is simulated and tested over a developed testbed to validate the work and check the system performance. In (Sec. 2) related works to the proposed system are introduced. Sec.3 provides the proposed IoT system with the deployment of distributed Fog computing, SDN and blockchain technologies. Also, the data offloading algorithm and traffic model are presented in this section. In (Sec.4) the simulation and testing is introduced and the experimental results are provided and analyzed.

2. Background and related works

There are many features associated with the IoT networks that put high constraints on the designing of a secure IoT network. These features related to the topology and the nature of the IoT networks and can be summarized in the following [32, 33]:

1- Scalability:
With the dramatic massive increase of wireless devices, the scalability of next generation networks should be considered while designing these systems. By 2020, it is expected that higher than 50 billion devices will be connected [34]. IoT networks will suffer from this dramatic increase of network nodes and traffic. Thus, designing a secure IoT network should consider the network scalability. Decentralized solutions represent a vital solution.

2- Heterogeneous technologies:
IoT networks comprise many heterogeneous communication technologies that have different security requirements [35]. Thus, secure reliable IoT network should consider the heterogeneity of these technologies and therefore, provide the security for all comprised technologies.

3- Latency:
A part of IoT applications are latency sensitive applications that required a low end-to-end latency. All introduced solutions and algorithms for such applications shouldn't add extra delays.

4- Availability:
IoT applications required a high system availability to support the massive traffic demand. Developed algorithms and methods for IoT networks should support the availability requirements for various IoT applications.

5- Mobility:
Mobility can be defined as the way of providing seamless service experience to users, while they are moving. Various mobility demands may be required for various IoT applications; some applications may require a very high mobility demands such as high speed systems (e.g. IoT devices deployed in trains) [36]. Other applications may be associated with

stationary devices or low speed and thus require a low mobility. Different mobility levels put constraints on different solutions developed for IoT networks.

6- Battery operated nodes:
Energy conservation represents an important issue in designing IoT networks, this is because heterogeneous IoT devices are battery operated and recharging may be hard in many applications. Thus, conserving energy of IoT devices and prolong the life time of distributed nodes become critical in many applications. Therefore, the comprised solutions developed for IoT networks should be energy efficient.

7- Service discovery:
Service discovery is the process hold by the IoT network user to discover resources and get much information about the endpoints of the application server. IoT networks should deploy self configuring, reliable and scalable mechanisms to provide service discovery [59].

8- Application level protection:
IoT is expected to support various applications in various fields. Thus, secure IoT ensures a proper application level protection so that all heterogeneous applications are saved from different cyber security attacks.

Cyber security attacks and threats put high constraints and demands on the design of the IoT networks, as IoT networks should be able to work against these attacks [37]. This can be achieved by introducing new communication paradigms to the IoT networks. SDN is one of the main paradigms that are used to achieve higher security of the IoT networks beside many other benefits to the overall network performance. Another main paradigm is the distributed computing techniques (e.g. Fog computing and mobile edge computing (MEC)) [38].

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 [39]. There many studies dedicated with development and deployment of edge computing units in communication networks, especially for cellular networks and IoT. A part of researchers uses the term cloudlet to refer to any secondary, small and limited capabilities cloud units [40]. There are many other forms of the edge cloud units include Fog nodes and the micro-cloud units and other forms [18], [41].

Fog computing is considered to be the most suitable edge computing platform for the IoT networks and applications. The Fog computing paradigm was first announced by Cisco as a form of edge computing and an extension of the cellular edge computing [42]. Then, researches and studies have been developed to analysis, define, improve and integrate this new computing paradigm. Many literatures that consider the 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 this part, we consider the related works to our proposed work.

In [43], authors have developed a framework for IoT network with the fog computing deployment. The work has mainly developed for considering IoT applications from the Fog computing point of view. Authors have introduced a distributed data flow mechanism referred to as DDF that is programmable. The dataflow programming model is used for building different IoT applications and services. The data algorithm is validated over, the open-source flow based run time and visual programming tool, Node-RED. The testing has been introduced just to validate that the architecture and algorithm are suitable, however no performance metrics were considered. The work mainly considered as a programming platform, however our work is validated over a developed testbed. Furthermore, we consider more technologies (i.e. SDN and Blockchain) to enhance the performance of Fog units and the overall system performance.

In [44], authors have developed a hierarchical computing structure for medical applications over IoT networks. The hierarchical structure consists of the centralized cloud and distributed Fog units. The proposed paradigm has mainly introduced to partition and accommodate the machine learning methods used for health care applications over the IoT networks. The computation tasks and medical data are distributed among two computing levels in a partitioning way that increases the system availability. Furthermore, a closed loop management technique is developed that is mainly dependent on the user's condition (e.g. medical parameters). The system has been 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 it considers the availability only as the performance metric.

In [45], authors proposed an internet of vehicles (IoV) Fog based architecture, with SDN deployed. The work is the first that considers such structure and gather 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; 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 with different regions of covered area. The two controllers are physically connected. An optimization problem has been solved to optimize the geographic placement of distributed controllers. The work shares the similarity of deploying Fog computing and SDN with an IoT network with our proposed system, while it considers only the IoV which is a high mobility application. One main issue of this algorithm is that it hasn't been validated and no performance has been checked. Authors have introduced a system structure only.

In [46], authors have developed a secure IoT system that deploys Fog computing, SDN and blockchain paradigms. The main objective of the work is to enhance the security of the IoT networks through the deployment of these technologies (i.e. Fog computing, SDN and blockchain). The system uses the SDN and blockchain technologies 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 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 much as needed of recommendations at the network edge. The system has been evaluated for different security scenarios and attacks. This system shares a similarity with our proposed system, which is focused in the deployment of distributed Fog computing besides the SDN and blockchain technologies. However, the main concern of this work is the security issues, while our proposed structure mainly concerned with the end-to-end latency performance and the resources utilization. Furthermore, our developed SDN network completely differs from the SDN network used in this work, since we use a distributed controller scheme with distributed resource powered OF switches. Feeding OF switches with ultra small computing capabilities achieves various benefits to the IoT networks in terms of latency and reliability. Moreover, we consider the network traffic management by introducing a traffic model to control the data traffic among network, which is also novel.

In [47], we study the performance of IoT networks with the Fog computing deployment. We have constructed a testbed of 50 IoT nodes, distributed Fog nodes and a controller. The 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. Also, 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 part, 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 well defined. Then, a data offloading algorithm is introduced 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 the concept of Fog computing with the blockchain and SDN paradigms to serve for IoT networks and applications. The system can be viewed as a three layer

system as illustrated in figure 2. 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 energy efficiently managed.

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 a certain services and a dedicated location. The Fog node handles the data forwarded from the dedicated IoT devices. Thus, 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.

Distributed fog nodes add various benefits to the proposed IoT network that include the following:

1- Provide an offloading path for the collected data,
2- Provide computing capabilities near to IoT devices,
3- Increase the system security by detecting and blocking heterogeneous attacks,
4- Reduce the data traffic at the core network, and
5- Increase 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 the network users an overall controlling and monitoring of the application.

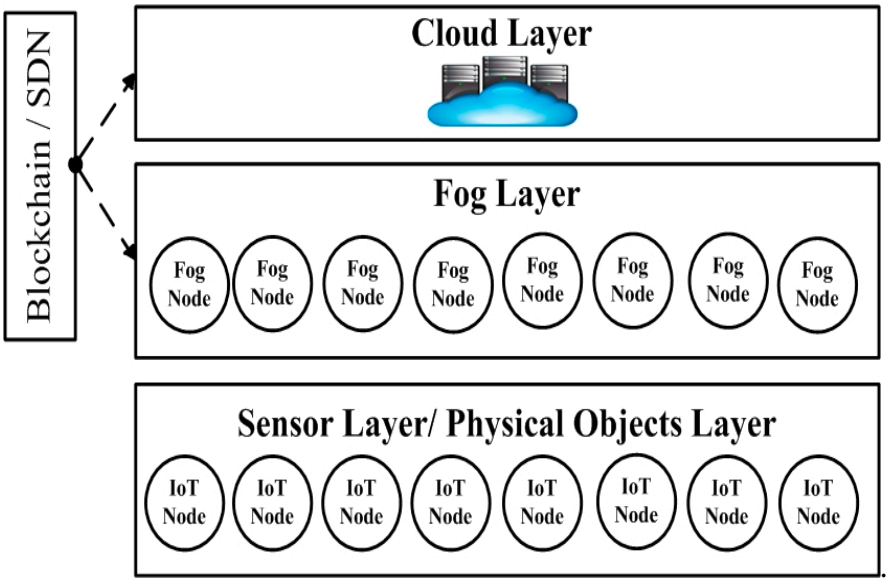

Figure 2. The main layers of the proposed IoT-Fog system.

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 3.

a- SDN paradigm

The system deploys a single centralized physical SDN controller that controls and manages distributed fog nodes and hence IoT devices. Figure 4 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 OpenFlow protocol) [48]. The SDN controller employs a clustering algorithm introduced in [49], 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 the security over the databases and work against saturation attacks [50]. 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 paradigm to provide a high security level to the proposed IoT network.

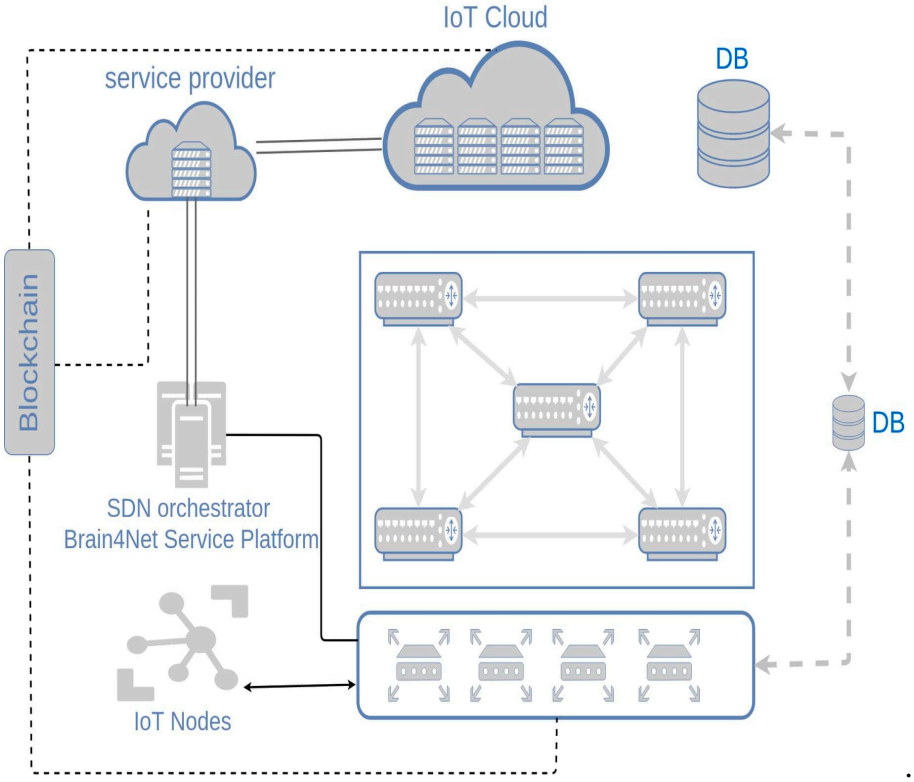

Figure 3. System structure of the proposed IoT-Fog system with SDN/blockchain.

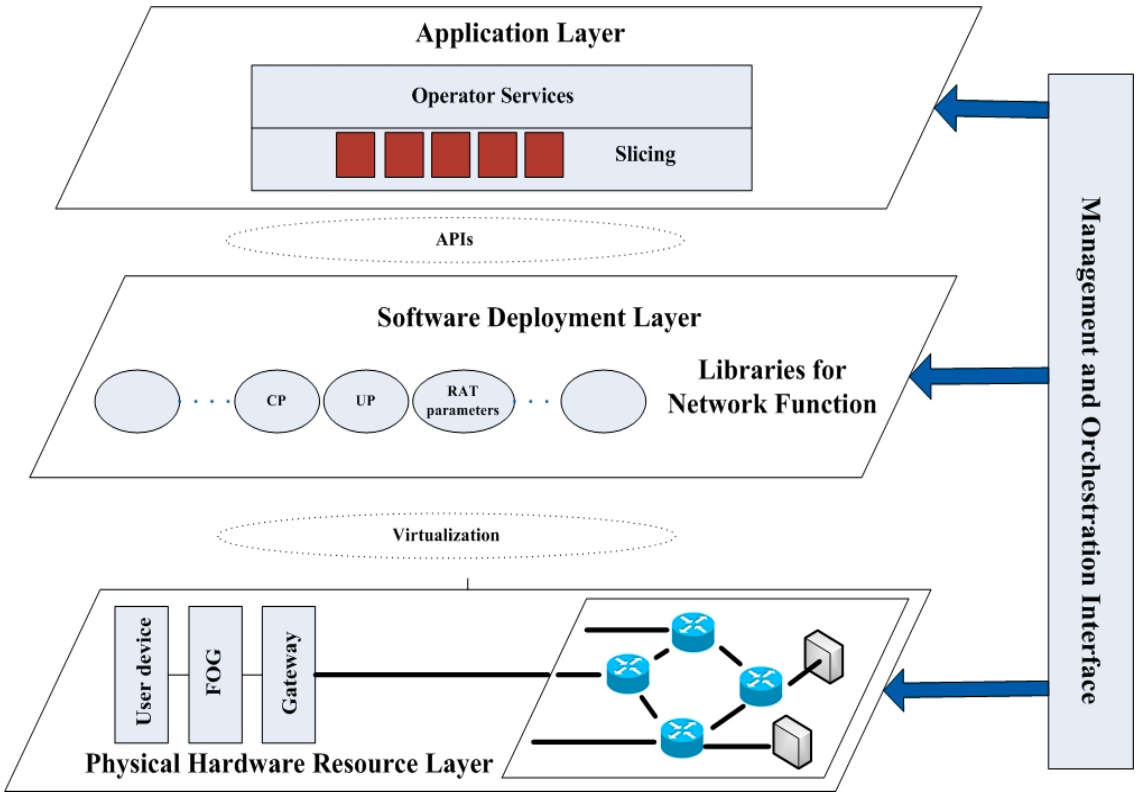

Figure 4. Layers of SDN network.

b- Blockchain paradigm

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 the IoT network, these benefits includes the following:

1- Work against network heterogeneous attacks and thus, increases the overall system security;
2- Increases the flexibility of the system;
3- Achieves the required scalability of the IoT networks; and
4- Increases the system availability.

In this work, the block chain is considered as a structural component, while further analysis of the blockchain to the proposed structure need to be conducted in single work. 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 5. The network operation goes through various steps; the first step is the authentication, as the IoT node should be authorized. IoT node communicates directly with the IoT cloud to be authorized. Then, IoT cloud performs the authentication process and mentioned the device to be authorized.

The next step is the 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.

Moreover, the SDN orchestrator estimates the routing table with different routing paths between the IoT node and the cloud and locates all OF switches dedicated with this communication.

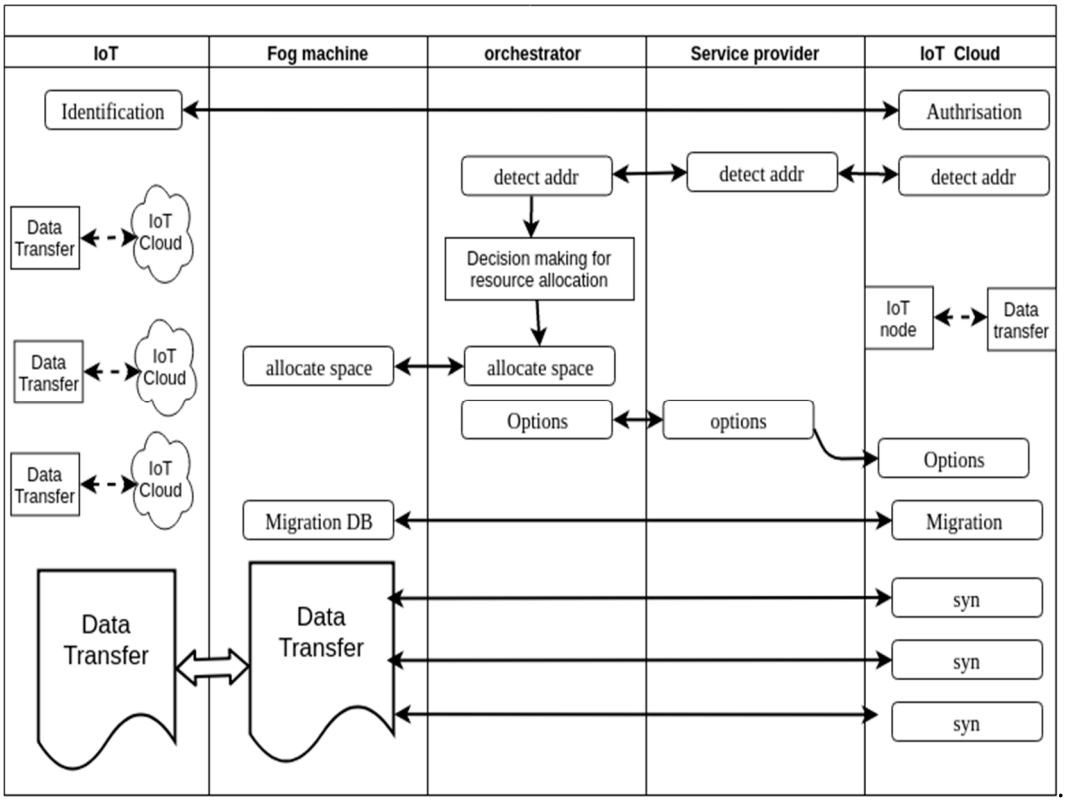

Figure 5. Data flow algorithm.

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

1- IoT traffic,
2- Transit traffic,
3- Traffic access type,
4- Time delay constraints,
5- Processing power for servicing the IoT data, and
6- Current state of the OF switches in terms of traffic and resources.

SDN controller decides the possibility of enabling the IoT data, passed to the core network through the Fog layer, a part of 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 is used for data processing. The next step is the database migration, as the IoT Cloud through the service provider migrates the database for servicing 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:

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

3.3-. Traffic model:

It is clear that, reducing a part of subscriber traffic in the local cloud reduces the total traffic value, and thus, increases the quality of service (QoS) of the traffic served by the network.

Introducing Fog nodes (i.e. Fog computing) with the SDN paradigm to the 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 data offloaded is considered as the main metric, which reflects 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 [51]. Figure 6 illustrates the proposed traffic model based on the G/G/1 queuing 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 following:

$$x = A\,(1 - P) \tag{1}$$

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

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

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

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

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 is corresponding to the removal of the Fog computing layer.

The total delivery time T can be calculated as following [52]:

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

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

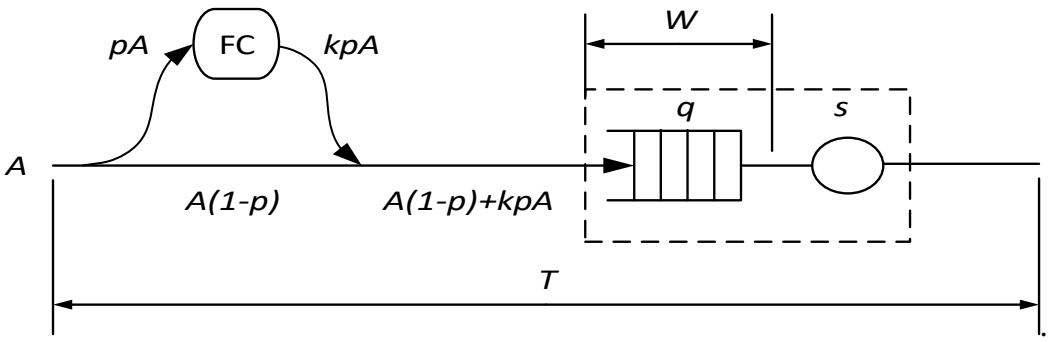

Figure 6. Traffic service model.

Where, s is the service time and ε is the form factor [52].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.

$$E = 1 - E_F/E_O = 1 - (1-\rho)/(1-\rho(1-P))\ (1-P) \quad (6)$$

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 is corresponding to the maximal efficiency of using Fog computing nodes. Figure 7 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 much traffic and thus, the efficiency increases. Furthermore, the dependence shows that the efficiency grows rapidly in case of high traffic value and grows slowly in case of small traffic value. Also, efficiency varies from 0, when no traffic is directed to fog cloud, to 1 when all traffic is directed to fog cloud.

Performance evaluation

In this part, the performance of the proposed IoT system and all comprised algorithms is evaluated. The proposed IoT-Fog system is experimentally tested over our proposed 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 3, while the considered network components are presented in Table 1, with the introduction of the specifications of each component. The x86 architecture is deployed to act as an OF switch, which is able to support processing and computing tasks [53]. 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 average of 6 per each node. The application layer supports MQTT and CoAP protocols [54].

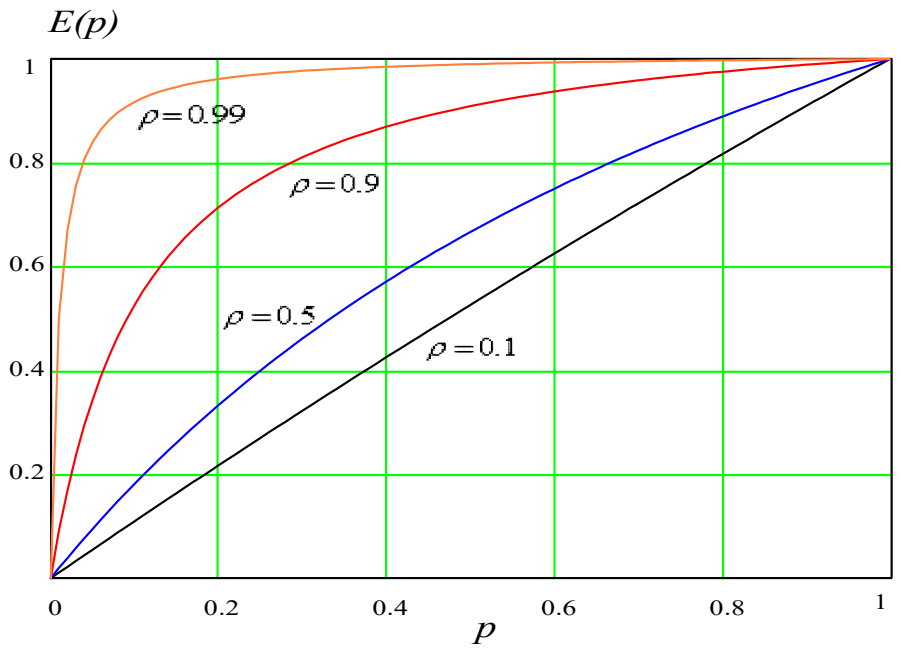

Figure 7. Traffic efficiency for IoT based Fog system.

Table 1. 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 iFogSim simulator, which is a reliable java based simulation environment for simulating IoT networks with distributed Fog computing structure [55]. The iFogSim is built over the CloudSim environment and for simulation process of our proposed system; CloudSim SDN is also involved for the SDN network [56]. CloudSim SDN is also a reliable java based environment; built over the CloudSim [57].

The system is simulated over a machine with an Intel core i5 processor, with a speed of 3.07 GHz and 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 simulation and experimental works; resources utilization (e.g. storage, processing and energy) and the end-to-end latency.

4.2. Experimental results:

In order to evaluate the performance of deploying distributed fog computing and SDN paradigm, the system is simulated for three considered cases. In the first case, the system is simulated without the deployment of distributed Fog computing and 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 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 SDN network. Table 3 summarized the considered cases specifications.

Figures 8, 9 and 10 illustrate the simulation results in terms of resources utilization. Figure 8 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 SDN network achieves higher performance in terms of storage resources utilization than the previous considered cases.

Table 2. Simulation parameters.

Parameter	Description	Value
Fog node		
Upstream bandwidth	BW_{UP}	500 Mbps
Downstream bandwidth	BW_{Down}	10000 Mbps
Storage capabilities	RAM	6144 MB
Processing capabilities	CPU	30000 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}	10000 Mbps
Downstream bandwidth	BW_{Down}	10000 Mbps
Storage capabilities	RAM	40960 MB
Processing capabilities	CPU	30000 MIPS
Communication latency to the ISP gateway	$d_{Cloud\text{-}Gateway}$	100 ms
ISP Gateway		
Upstream bandwidth	BWUP	10000 Mbps
Downstream bandwidth	BWDown	10000 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

Table 3. 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

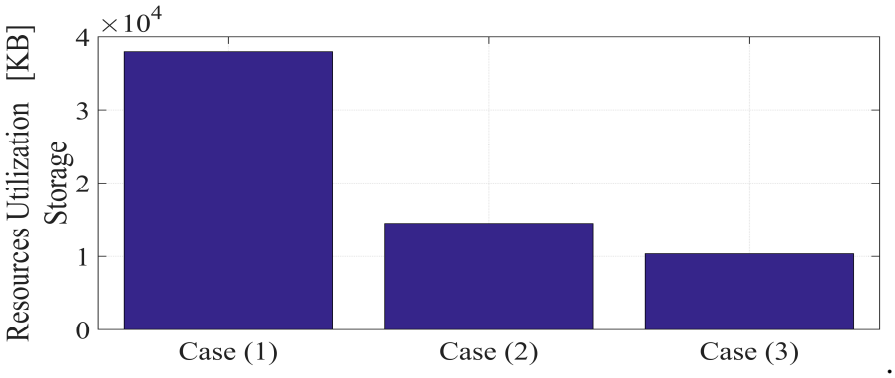

Figure 8. Average resources utilization in terms of storage, for the considered simulation cases.

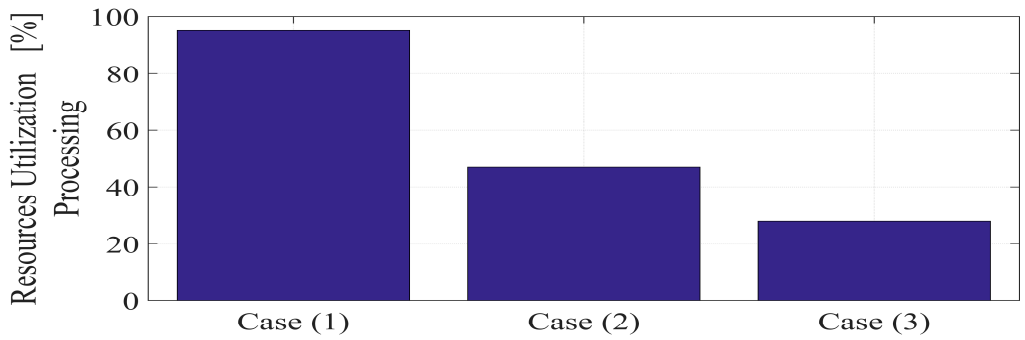

Figure 9. Average resources utilization in terms of processing, for the considered simulation cases.

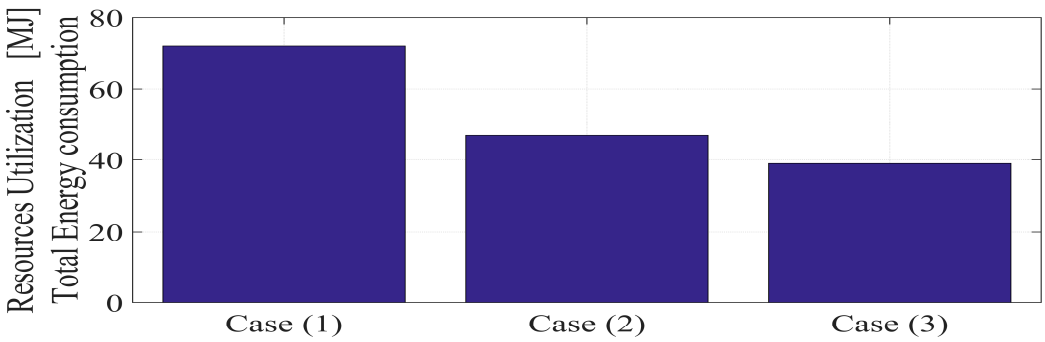

Figure 10. Average resources utilization in terms of energy, for the considered simulation cases.

Figure 9 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 10 provides the total energy consumed for computing tasks by all network elements in each considered case, based on the energy model introduced in [58]. The deployment of SDN with distributed Fog computing achieves higher energy efficiency of the IoT network and thus, utilize the energy resources more efficiently.

Figure 11 provides the end-to-end system latency for each considered case. Results indicate that the proposed system achieves 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 distributed edge computing paradigm that brings the computing resources near to IoT devices. Also, deploying SDN for controlling and managing IoT -Fog network is the key solution for the performance enhancement, this is because of the previous mentioned benefits of SDN based networks.

4.3. Experimental results:

Figure 12 illustrates the percentage of the average CPU load of the OF switchs in two considered cases. In the first case, the network is operated without the Fog layer, this puts great load on OF switches. In the second case, the Fog nodes are deployed. Results indicate the high performance achieved in case of Fog deployment.

Figure 13 illustrates the total latency of IoT traffic, in case of the network is operated without the Fog and SDN. In this case, the IoT nodes directly communicate with the IoT cloud. Figure 14 illustrates the latency for the proposed system where Fog nodes and SDN network are deployed. Comparing the two figures, we can get the vast variations in the latency in both cases. Employing Fog nodes and the SDN network with the enabled processing capabilities OF switches achieves a

high reduction in communication latency of IoT data and also better utilization of computing resources, which can be considered as the main benefit of the proposed system structure.

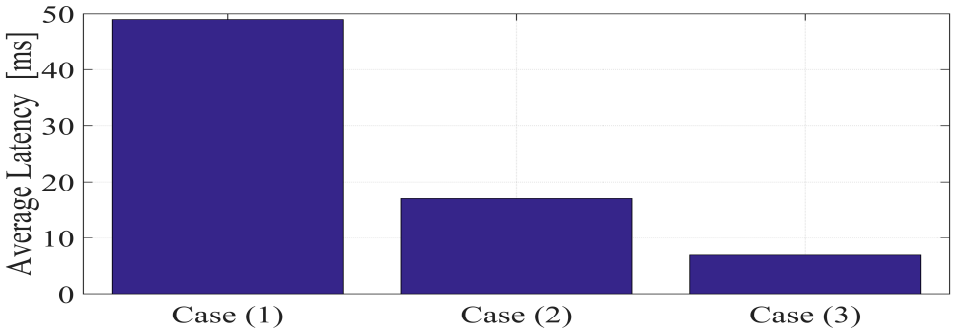

Figure 11. Average end-to-end Latency, for the considered simulation cases.

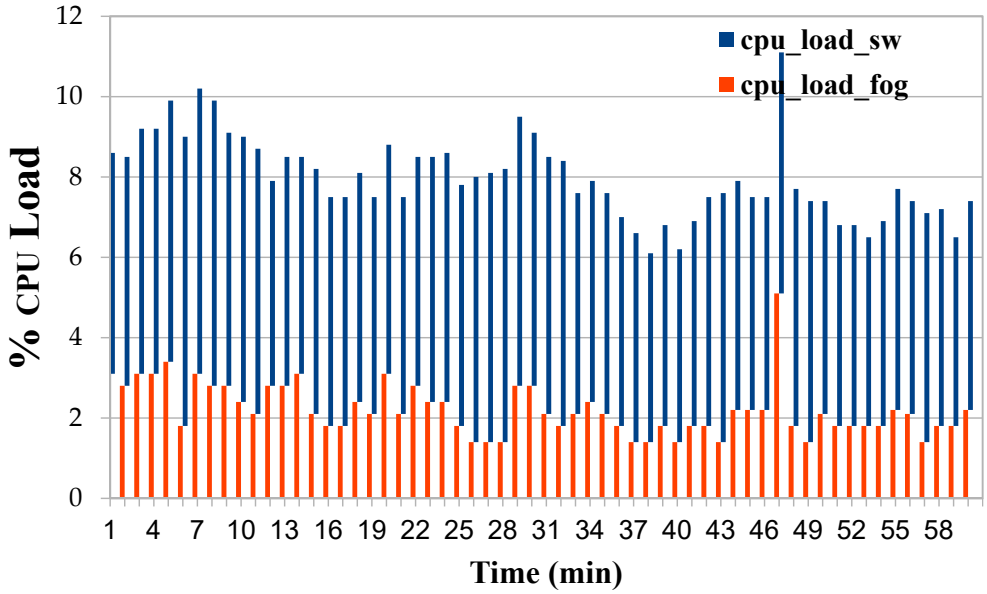

Figure 12. Percentage CPU-load for IoT traffic and processing for OF switches.

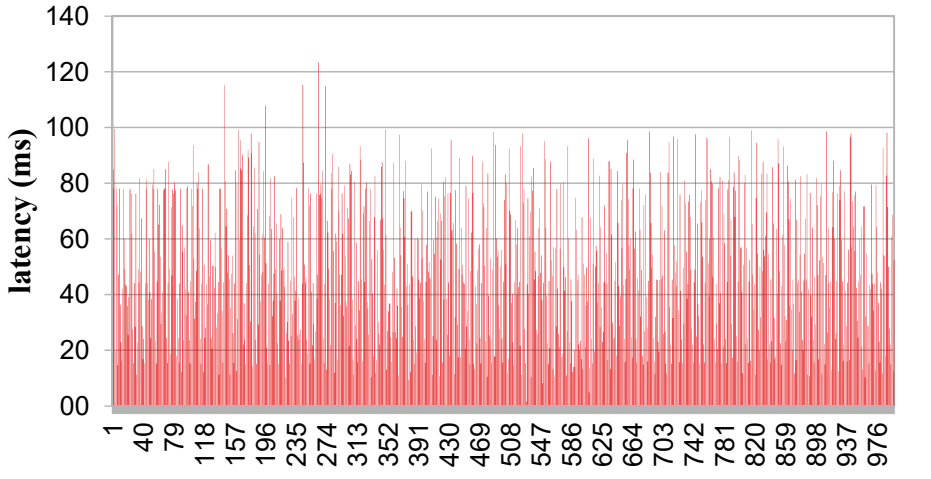

Figure 13. Communication latency in case of direct access to the IoT cloud.

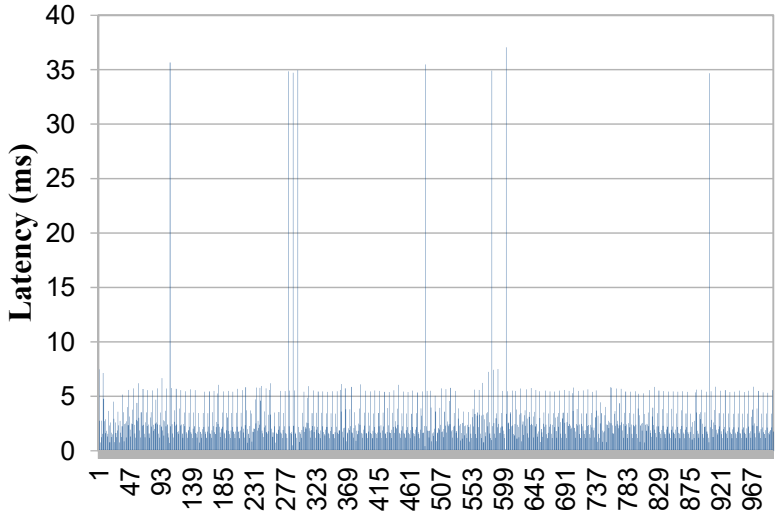

Figure 14. Communication latency for the IoT-Fog system.

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 to 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 a distributed OF switches to manage and control the distributed Fog computing. The distributed OF switches have been empowered with limited resources that can be used for assist forwarded traffic. The introduction of 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 is developed, with the traffic model. The proposed system has been 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.

Acknowledgments: 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). *Sensors and Actuators A: Physical*, 2018.
2. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 2017, 140, pp.1454-1464.
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. *Journal of Electrical and Computer Engineering*, 2017.
5. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 2015, 17(4), pp.2347-2376.

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. *Sustainable Cities and Society*, 2018, 38, pp.195-204.
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 (IDC)*, Tech. Rep, 1, 2014.
8. Manogaran, G.; Varatharajan, R.; Lopez, D.; Kumar, P.M.; Sundarasekar, R.; Thota, C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems*, 2018, 82, pp.375-387.
9. Aazam, M.; Huh, E.N. Fog computing and smart gateway based communication for cloud of things. In Proceedings of the 2014 IEEE International Conference on Future Internet of Things and Cloud (FiCloud), Aug. 2014, pp. 464-470.
10. Muruganandam, M.K.; Balamurugan, B.; Khara, S. Design Of Wireless Sensor Networks For IOT Application: A Challenges and survey. *International Journal of Engineering and Computer Science*, 2018, 7(03), pp.23790-23795.
11. Li, S.; Da Xu, L.; Zhao, S. 5G internet of things: A survey. *Journal of Industrial Information Integration*, 2018.
12. Mihovska, A.; Sarkar, M. Smart Connectivity for Internet of Things (IoT) Applications. In Proceedings of the New Advances in the Internet of Things, Springer International Publishing: Cham, 2018, pp. 105-118.
13. 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 of Things Journal*, 2017, 4(5), pp.1125-1142.
14. Ray, P.P. A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 2018, 30(3), pp.291-319.
15. 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, June 2017, pp. 26-37.
16. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 2018, 78, pp.680-698.
17. Satyanarayanan, M. The Emergence of Edge Computing. *Computer*, 2017, 50(1), pp.30-39.
18. 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), Feb. 2017, pp. 105-110.
19. Ansari, N.; Sun, X. Mobile edge computing empowers Internet of Things. *IEICE Transactions on Communications*, 2018, 101(3), pp.604-619.
20. 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, 2018, pp. 3-13.
21. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 2016, 56, pp.684-700.
22. 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. *Applied Sciences*, 2017, 7(12), p.1325.
23. Byers, C.C. Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for FOG-enabled IoT networks. *IEEE Communications Magazine*, 2017, 55(8), pp.14-20.
24. 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, 2018, pp. 29-40.
25. Cui, L.; Yu, F.R.; Yan, Q. When big data meets software-defined networking: SDN for big data and big data for SDN. *IEEE network*, 2016, 30(1), pp.58-65.
26. 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. *Journal of Sensor and Actuator Networks*, 2018, 7(1), p.1.
27. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors*, 2018, 18(8), p.2575.

28. 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), March 2017, pp. 618-623.
29. Banafa, A. IoT and Blockchain Convergence: Benefits and Challenges. *IEEE Internet of Things*, 2017.
30. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the IEEE 2017 19th International Conference on Advanced Communication Technology (ICACT), Feb. 2017, pp. 464-467.
31. Peter, H.; Moser, A. Blockchain-Applications in Banking & Payment Transactions: Results of a Survey. *European Financial Systems 2017*, p.141, 2017.
32. Dabbagh, M.; Rayes, A. Internet of things security and privacy. *In Internet of Things From Hype to Reality*, Springer International Publishing: Cham, 2019, pp. 211-238.
33. Atwady, Y.; Hammoudeh, M. A survey on authentication techniques for the internet of things. In Proceedings of the ACM International Conference on Future Networks and Distributed Systems, July 2017, p. 8.
34. ATEYA, A.; AL-BAHRI, M.; MUTHANNA, A.; KOUCHERYAVY, A. End-to-end system structure for latency sensitive applications of 5G. *Электросвязь*, 2018, (6), pp.56-61.
35. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), August 2016, pp. 145-149.
36. 3GPP TR 38.913, "Study on Scenarios and Requirements for Next Generation Access Technologies," Ver. 14.3.0, June. 2017.
37. Choo, K.K.R.; Bishop, M.; Glisson, W.; Nance, K. Internet-and cloud-of-things cybersecurity research challenges and advances, 2018.
38. Uddin, M.; Mukherjee, S.; Chang, H.; Lakshman, T.V. SDN-based Multi-Protocol Edge Switching for IoT Service Automation. *IEEE Journal on Selected Areas in Communications*, 2018.
39. Alliance, N.G.M.N. 5G white paper. Next generation mobile networks, *white paper*, 2017.
40. 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), Feb. 2018, pp. 507-512.
41. 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), Oct 2013.
42. Computing, F. the Internet of Things: Extend the Cloud to Where the Things Are. *White paper*. CISCO, 2015.
43. 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),* Oct. 2015, pp. 155-162.
44. 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 Transactions on Embedded Computing Systems (TECS)*, 2017, 16(5s), p.174.
45. Borcoci, E.; Ambarus, T.; Vochin, M. Distributed Control Plane Optimization in SDN-Fog VANET. *ICN 2017*, p.135.
46. 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, pp.115-124.
47. 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), Jan. 2018, pp. 51-54.
48. Rofie, S.A.; Ramli, I.; Redzwan, K.N.; Hassan, S.M.; Ibrahim, M.S. OpenFlow Based Load Balancing for Software-Defined Network Applications. *Advanced Science Letters*, 2018, 24(2), pp.1210-1213.
49. 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), Jan. 2016, pp. 76-79.
50. 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, pp.115-124.
51. Kleinrock, L. Queueing systems, *volume 2: Computer applications*, 1976, (Vol. 66). New York: wiley.

52. Iversen, V.B. Teletraffic engineering handbook. *ITU-D SG*, 2005, 2, p.16.
53. 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, April 2012, Vol. 12.
54. Karagiannis, V.; Chatzimisios, P.; Vazquez-Gallego, F.; Alonso-Zarate, J. A survey on application layer protocols for the internet of things. *Transaction on IoT and Cloud Computing*, 2015, 3(1), pp.11-17.
55. 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. *Software: Practice and Experience*, 2017, 47(9), pp.1275-1296.
56. Kumar, R.; Sahoo, G. Cloud computing simulation using CloudSim. *arXiv*, 2014.
57. CloudSimSDN Project. Available online: https://github.com/jayjmin/cloudsimsdn (accessed on 10 September 2018).
58. 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), May 2017, pp. 1222-1228.
59. Cirani, S.; Davoli, L.; Ferrari, G.; Léone, R.; Medagliani, P.; Picone, M.; Veltri, L. A scalable and self-configuring architecture for service discovery in the internet of things. *IEEE Internet of Things Journal*, 2014, 1(5), pp.508-521.