IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 24, 2019, accepted October 20, 2019, date of publication November 8, 2019,
date of current version December 5, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2952472*

# DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things

**RAHEEL AHMED MEMON[1,2], JIAN PING LI[1], MUHAMMAD IRSHAD NAZEER[2], AHMAD NEYAZ KHAN[1], AND JUNAID AHMED[3]**

[1]School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Department of Computer Science, Sukkur IBA University, Sindh 65200, Pakistan
[3]Department of Electrical Engineering, Sukkur IBA University, Sindh 65200, Pakistan

Corresponding authors: Raheel Ahmed Memon (raheelmemon@iba-suk.edu.pk) and Jian Ping Li (jpli2222@uestc.edu.cn)

This work was supported by the National Natural Science Foundation of China Grant 61370073, National High Technology Research and Development Program of China Grant 2007AA01Z423, Project of Science and Technology Department of Sichuan Province; and Chengdu Civil-Military Integration Project Management Co., Ltd.

**ABSTRACT** Integration of blockchain and Internet of Things (IoT) to build a secure, trusted and robust communication technology is currently of great interest for research communities and industries. But challenge is to identify the appropriate position of blockchain in current settings of IoT with minimal consequences. In this article we propose a blockchain-based DualFog-IoT architecture with three configuration filter of incoming requests at access level, namely: Real Time, Non-Real Time, and Delay Tolerant Blockchain applications. The DualFog-IoT segregate the Fog layer into two: Fog Cloud Cluster and Fog Mining Cluster. Fog Cloud Cluster and the main cloud datacenter work in a tandem similar to existing IoT architecture for real-time and non-real-time application requests, while the additional Fog Mining Cluster is dedicated to deal with only Delay Tolerant Blockchain application requests. The proposed DualFog-IoT is compared with existing centralized datacenter based IoT architecture. Along with the inherited features of blockchain, the proposed model decreases system drop rate, and further offload the cloud datacenter with minimal upgradation in existing IoT ecosystem. The reduced computing load from cloud datacenter doesn't only help in saving the capital and operational expenses, but it is also a huge contribution for saving energy resources and minimizing carbon emission in environment. Furthermore, the proposed DualFog-IoT is also being analyzed for optimization of computing resources at cloud level, the results presented shows the feasibility of proposed architecture under various ratios of incoming RT and NRT requests. However, the integration of blockchain has its footprints in terms of latent response for delay tolerant blockchain applications, but real-time and non-real-time requests are gracefully satisfying the service level agreement.

**INDEX TERMS** Blockchain, Internet of Things, fog layer, DualFog-IoT, quality of service (QoS).

## I. INTRODUCTION

Internet of things (IoT) is the most fascinating technological revolution to empower things by connecting and taking autonomous decisions in a smart environment. The miniaturization of electronic devices and communication technologies have contributed to achieve surprisingly a rapid evolution in its growth. Currently there are more than five billion devices connecting to Internet on account of IoT. The number of connected devices is even predicted to get doubled every year in 2017, and in 2020 it is expected to reach 29 billion [1]. However, it is a bitter fact that after achieving innovative hardware and software technologies, IoT is running beyond its prediction made during past decade by enterprises and researchers [2]–[8]. Involvement of third-party to keep the data in a Centralized Datacenter (CDC) introduced several critical issues in recent years, and those issues might be playing as a barrier to achieve its future vision. The discussion of issues and challenges of IoT is beyond the scope of this paper, but plenty of literature is available on the details of issues, which can be found as: security [9]–[11], privacy [12]–[14], losses and risks [15], [16] scalability [17], latency [18], [19],

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

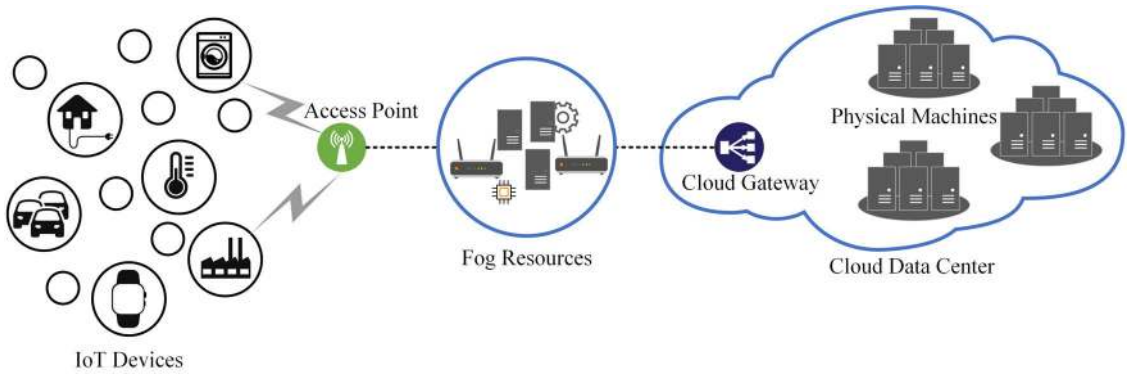


**FIGURE 1.** Existing centralized datacenter based Internet of Things (CDC-IoT) architecture.

energy consumption [20], [21] and cost [22]. Survey presented in [23] provides good insight when it comes to issues of IoT.

To address challenges of scalability, latency, cost and energy consumption involved in IoT architecture, in 2006 Cisco announced Fog computing to bring processing resources at the edge of device [24]. Fog layer at the access level of network is there to offload burden from main datacenters and also response to request with minimal latency [18], [25]–[27]. Currently, IoT is a three Tier architecture as shown in Figure 1, Layer one, includes sensors, actuators and the smart devices, Layer two, is Fog layer provides instant response to real time applications, it is composed of devices such as smart gateways, routers and dedicated fog computing devices, the fog devices are connected to gateway of cloud to get access to the main datacenter at Layer three [28]. The integration of fog layer in traditional cloud architecture, have reduced latency but still the issues related security and lack of trust are persistent in IoT today [1], [22], [29]–[31].

Recently blockchain has received tremendous popularity and attention from researchers and industries. Blockchain which raised as underlying technology of Bitcoin (digital cryptocurrency) in year 2008 [32], has started to influence many different fields other than economics, such as e-healthcare, e-finance, real estate, e-voting, supply chain, smart homes and Internet of things [31], [33]–[35]. Blockchain is a decentralized and distributed architecture forming a peer-to-peer network, where cryptographically signed transactions of digital currency take place. The exciting feature of Blockchain is distributed ledger technology (DLT), where the metadata about transactions are accumulated in blocks, which are then verified by the consensus of all peers in network. Each time after verification, a new block is added to the main Blockchain. The Blockchain is like a linked list type of data structure which is replicated across the distributed network. Once a block is added on blockchain it cannot be tampered due to multiple available copies in overall the network [32].

The significant properties of blockchain are; it is tamper-proof, secure, preserve privacy and build a reliable network with no downtime. While the same properties of currently available IoT infrastructure are of prime concern. Thus the integration of these two technologies is a potential candidate to best fit the needs of ever-growing IoT ecosystem. A detailed survey on integration of blockchain in IoT, existing and expected issues of both technologies, and future research directions are well presented by Memon et al. [23]. There have been several startups from enterprises to strengthen IoT by integrating blockchain technology [36]–[38], also a list of well-known companies created A Trusted IoT Alliance for establishing a fearless IoT ecosystem using blockchain [39], [40]. Some startups like Slock.it, Filament, Chronicled, Ambisafe and many others are also contributing in same cause [36]–[38]. A number of platforms such as Ethereum, Hyperledger Fabric, multichain, litecoin, Lisk, Quorum and HDAC are also trying to decrease the complexity of blockchain for easy integration with resource constrained devices in IoT settings [41]–[44]. Cisco startup of OpenFog Consortium also a missioned for decentralized computing of IoT by enhancing capabilities of Fog layer [26].

The research efforts in recent years tends to integrate blockchain with IoT can be broadly divided into two categories, the first is an entire shift of IoT over blockchain, where all the devices in IoT communicates directly with each other without involvement of any trusted third party, such as EthEmbedded, Ethraspbian, Raspnode, and Bitmain [45]–[48] are the examples of available devices in market. But the entire shift of IoT over blockchain is not practical in long run, because the mining operation in blockchain is a special task requires heavy computation capabilities, which is currently being performed using Application Specific Integrated Circuit (ASIC) chips, thus it is useless to try that on resource constrained devices in IoT environment [49]. While the second category tries to improve one of the three layers of existing IoT architecture or introducing an additional layer dedicated to operate blockchain protocols [50]–[54], which is significantly a good direction to get explored. On the evidence

of a large number of available proposals about Blockchain and IoT we can say that:

1) The integration of Blockchain with IoT may bring some compromises in terms of latent response time and reduced throughput
2) But Blockchain and IoT Integration is the missing part of the same puzzle, both have capabilities to address the identified issues in each other.
3) A well-organized, and optimum solution is needed for the integration of blockchain with IoT, which requires minimum upgradation in existing settings of IoT.

In this article we present a Fog level integration of IoT with blockchain and named it as DualFog-IoT, where the fog level computing resources are virtually divided into two: Fog Cloud Cluster (FCC) and Fog Mining Cluster (FMC). FCC communicates with cloud as in available IoT architecture, while the FMC of trusted fog devices is dedicated to perform the mining operation for blockchain-based applications. The proposed DualFog-IoT model is simulated and compared with existing Fog/Cloud based IoT (FC-IoT) architecture using Queuing theory in Java Modeling Tool (JMT) for performance evaluation [55]. The critical Quality of Services (QoS) parameters such as: (1) System drop rate, (2) Utilization of fog computing resources (3) Utilization of Cloud Data Center (CDC) resources (4) Number of requests available in system at any instance of time, (5) System response time, and (6) System throughput are obtained during simulation. It is found that the proposed DualFog-IoT reduces the drop rate and VOLUME XX, 2017 3 offload the fog and cloud layers by releasing a number of hardware resources, which doesn't only reduce the CAPEX and OPEX involved in establishing and maintaining the CDCs, but also reduces the energy consumption of giant CDC. Furthermore, the analysis of DualFog-IoT is presented by optimizing the resources and varying RT and NRT request ratios. The obtained results are satisfactory with a number of cases in both simulations. However, due to inherited latency issue in blockchain, system response time, and throughput are affected, but still the proposed DualFog-IoT satisfies the Service Level Agreement (SLA).

The proposed DualFog-IoT works on the three configurations, where the configuration describes the type of incoming request namely, Real-Time (RT), Non-Real-Time (NRT), and Delay-Tolerant Blockchain (DTB) applications. The three configurations of proposed architecture could also be an icebreaker to the pending debate about service level policies for the type applications needed to be performed on blockchain. The main contributions of this article can be summarized as:

A. *Proposed DualFog-IoT with Blockchain integration:* A fog level integration of blockchain in existing settings of IoT without troubling the available layout of existing IoT architecture.
B. *Simulation Model:* Simulation of DualFog in JMT simulator (A queuing theory simulator) is also novel in itself which provide a base model for simulation of blockchain with IoT.
C. *An Icebreaker:* The proposed three configurations of DualFog are opening a debate for research community of IoT on service level policies for blockchain-based application.
D. *Outcome:* Besides achieving security and privacy for critical applications by using blockchain, the proposed model also offloads fog and cloud layers by releasing hardware resources. Furthermore, the lower drop ratio can also be observed in proposed DualFog method. However, as expected a few compromises in terms of System response time and throughput exists there.

The rest of this article is organized as follows, section 2 provide an adequate background of related work, section 3 describe the working of proposed DualFog-IoT. Section 4 presents the simulation setup, Section 5 about the obtained results, and discusses the outperformer and underperformer architecture. Section 6 presents the analysis of proposed architecture for optimization of resources, and finally, section 7 concludes.

## II. RELATED WORK

### A. FOG COMPUTING IN INTERNET OF THINGS

With the huge storage capacity, enormous computing power and other advanced hardware and software technologies, CDCs are being used to serve the resource constrained devices of IoT [18]. The initial cloud layout (High level) was composed of three layers, first layer comprises of user end devices also known as IoT device tier like sensors, actuators and other IoT devices. Second layer named as networking layer which works as communication medium in between layer one and layer three. Third layer was cloud layer also known as datacenter or cloud computing layer, this layer comprises of huge computation and storage capacity resource. All the traffic generated from layer one forwarded to layer three to take the action. In several real time applications, the Round-Trip Time (RTT) of a request and response were high. In 2006, Cisco coined the concept of Fog to offload the cloud by injecting smart device over network layer to provide limited computation facilities at the edge of device layer [56], the fog layer is also known as Edge layer because it is consists of smart gateways, routers and dedicated computing devices. The smart devices at edge are sometimes are also being considered as devices at Edge Layer while Fog layer is treated separately [57]. This new addition of fog layer has reduced network latency, and workload from CDCs [58]. As shown in FIGURE 1, currently the Cloud architecture layout is three-layer architecture. layer one is IoT device layer, layer two is Fog and layer three is CDC layer in rest of the paper we will be referring this current architecture as CDC-IoT.

There are a number of opinions and proposals with different implementations and schemes for fog in three tier CDC-IoT architecture. Bonomi proposed that with distributed networking capabilities fog platform can provide virtualized services of cloud at the edge of network [59], [60]. As proposed by Cisco, fog is implemented using Cisco edge

router in [56]. While depending on the definitions of fog nodes in three layer architecture of IoT; a fog node can be routers at the core network, switches in WAN, Wireless Access Points at the access level, or even Smart phones at user level [57]. Aazam, M. et al. proposed fog nodes as smart gateways [61], and as micro datacenter in [62], Abdullahi et al. proposed services of fog as caching in information centric network [63]. Working of fog as a distributed mini cloud are also proposed in [64], [65].

In fog to cloud communication, each request is first directed to fog node instead of directly submitting to main cloud, then fog layer filters incoming requests on the basis of application or required processing and storage capacity, that it should be performed at fog or at the main cloud. The location of fog nodes is also a key characteristic discussed in previous years. Azam *et al.* [61], [62] suggested location of fog nodes in highly efficient devices such as smart routers and smart gateways. In [59], [60] authors proposed fog node as an individual computing node serve as intermediary in between device and cloud communication. Also in smart city environment Tang et al. [64] proposed fog as a computing layer for big data analysis. In all of the proposed settings of fog nodes in three layered architecture of IoT, it is very clear that fog significantly reduces the latency as compared to cloud. However, all of the above discussed theories are mainly concerned to further reduce latency by deploying different devices as fog node.

### B. BLOCKCHAIN

In 2008 a pseudo name Satoshi Nakamoto introduced a cryptocurrency Bitcoin [32]. Along with open source Bitcoin software, the underlying technology Blockchain was also released later in 2009. Blockchain is a public ledger to record all the transactions over peer-to-peer network, the transactions are waiting for a specified time in memory pool, which is a shared memory space of all the nodes in network to get bundled as a block. Once the block is generated it gets signed by cryptographic signature also known as hash, blockchain in bitcoin uses SHA256 (Secure Hash Algorithm) a cryptographic hash function to secure the transactions [51]. After block generation it is forwarded to the network, all of the nodes of blockchain network can participate in competition of mining the block to discover the correct hash key by iterating through different nonce each time. The miner who successfully find out the correct nonce, broadcasts the nonce and block to the network as their Proof-of-Work (PoW), where the other nodes in network verifies the block by applying the received nonce, if the block is correct it is added to the main blockchain, and if not then it is discarded, this verification process is known as Consensus [66]. The miners whose block is added to blockchain receives a reward in terms of freshly released bitcoins for his efforts [67]. The addition of new block in blockchain works as a data structure, where every new block is referenced to its previous block.

Once the block is added to blockchain it is probabilistically impossible to edit or delete that block [32]. In bitcoin, every 10 minutes a new block is added to the blockchain, thus tampering with existing block requires incredible computation power to mine all the succeeding blocks before addition of another new block. Mining operation is an expensive operation, in bitcoin, the complexity of mathematical puzzle of generated hash is adjusted after every 2 weeks [68]. The addition of latest hardware technologies to speed up mining process has increased difficulty level of mathematical puzzle, so that a normal computer would take more than year to solve it, this is the reason why ASIC machines have come in to play [69]. There are 144 blocks added every day in blockchain, average number of transactions per block depends on the number of transactions can fit in 2 MB of memory. A single transaction roughly require 570 bytes, which means the number of transaction is approximately 3500 per block [70].

Comparing to traditional payment systems such as, Visa, PayPal and so on; bitcoin is very much time-consuming [71]. But as blockchain works in a decentralized and distributed peer-to-peer network, it has no third-party involvement to control over the assets of customers, and the powerful computers involved in mining process are contributing in securing the blockchain bit by bit, the blockchain-based systems are considered as safe, secure and reliable. Furthermore, it also provides a tamperproof ledger of technologies by replicating same copy of blockchain in overall network. However, this security and elimination of third-party involvement has to pay in terms of delayed transactions for may be long period, currently there are thousands of transactions are pending in memory pool [72]. To overcome the latency issues still preserving the security and discouraging third-party involvement, several platforms has come into play. Most of those platforms are using blockchain technology by relaxing its time consuming and processing hungry PoW algorithm [67].

### C. INTEGRATION OF BLOCKCHAIN WITH IoT

The Internet of things, lacks in security, reliability and trust because of involvement of third-party and centralized communication architecture. While blockchain provides security, reliability and a trustworthy network, and eliminating third-party involvement by using distributed network architecture (P2P). However, blockchain suffers from long latency and delayed transactions due to time consuming mining operation, on the other hand IoT has remarkably reduced latency in recent years by adding fog layer in three tier architecture. This is obvious that these two technologies are made for each other, and are the missing parts of puzzle to create a smart and viable communication platform for future. But in current state, the time-consuming mining operation of blockchain will result in increased latency and reduce throughput. There have been lots of work done in past few years to combine these two technologies.

There is a long list of available platforms integrating IoT with blockchain, but the popular ones are Ethereum, Hyperledger, Rootstock, Multichain, Lisk, Quorum, Steem and HDAC [49]. Ethereum is the first IoT platform to introduce

the smart contracts over the blockchain, smart contracts are the piece of code, that is used to record the rules and policies of transactions between unknown parties in a trustless way [73]. Ethereum is running a blockchain-based cryptocurrency known as ether and besides that it also provides a global Ethereum Virtual Machine (EVM) [74]. The smart contracts are currently used in development of several IoT applications. Ethereum is also pioneering of providing a platform to develop distributed applications (DApps) for blockchain network [75]. Hyperledger is another open-source IoT platform for developing blockchain and IoT related projects. Hyperledger-Fabric, IBM's blockchain platform, and IBM's Bluemix are the examples of Hyperledger projects. Hyperledger also provides support for development of distributed apps [76], [77]. Rootstock is another open platform for blockchain-based IoT, similar to Ethereum in terms of creating smart contract; the only functional difference is that it is using bitcoin ecosystem. Rootstock exist as sidechain of bitcoin's blockchain and also compatible with Ethereum's EVM, which means Ethereum contracts can also be executed over this platform. Not only this, but it is even more versatile platform that is able to merge-mine Ethereum with bitcoin [78], [79].

The multichain platform is an open source platform for blockchain development, it is a fork of bitcoin core that extends the functionality of blockchain by providing additional features such as: management of portfolio, assets, transactions and permissions [80]. Lisk is another blockchain platform specially for JavaScript developers. Sidechain or sub-blockchain can also be defined with Lisk, it also offers the use of cryptocurrencies (such as bitcoin, Ethereum etc) [81]. Quorum is specifically for financial applications, developed over Ethereum platform. It provides option to use multiple type of consensus algorithms [43]. Chronicled an enterprise supply chain management system used Quorum to interact with physical objects [82]. HDAC is project of Hyundai, it provides a platform for contract IoT and machine to machine communication [44].

### D. LOCATION OF BLOCKCHAIN in IoT

As the location of fog layer in IoT has different interpretations, similarly the integration of blockchain in IoT has also different interpretations. There are two main approaches for locating blockchain in IoT settings, the first one is entire shift from CDC-IoT architecture to a decentralized blockchain-based architecture, this approach is known as offline approach, while the second one is to modify one of the three layers of CDC-IoT architecture known as online approach. The offline approach has a number of proposals, for the integration of blockchain on device level, such as in [83] and [84]. Ethereum and its implementations, slock.it, chronicled, streamr are the popular example of device level integration [36], [82], [85]. Several embedded circuit boards has been introduce to create a blockchain-based smart devices such as; EtheEmbeded, Ethraspbian, Raspnode and Bitmain [45]–[48]. Samaniego M, et al. presented its implementation for Edison Arduino board to present deployment of blockchain on device level [86]. In such approaches, the routine requests work without interacting with Blockchain, and only a part of IoT data is stored on Blockchain, which is shared among all the devices in network. The approach is good if we have powerful computing and enough storage capacity at device level, because with time the size of blockchain also grows. Thus, limited storage capacity on end devices will soon become an issue. In IoT environment we have resource constrained devices, hence this approach seems unserviceable in long run.

The second one is online approach, where the integration of blockchain is proposed over the main cloud. Mingxin et al. have addressed security and privacy issues by using blockchain in Cloud environment [87]. Aymen Boudguiga et al. proposed integration of blockchain in cloud to address issues of availability in existing IoT ecosystem [88]. These approaches are aimed to obtain extended security, privacy, reliability and trustworthy solution over the cloud layer. It is fact that cloud is equipped with immense computational power and storage capacity, but this approach is still not suitable for mainly two reasons. 1) The idea of decentralizing IoT is totally overlooked, also 2) the energy consumption is already an issue with cloud datacenters [89], [90], furthermore increasing another layer of heavy processing is not a good idea.

In this online approach, integration of blockchain over fog layer has also been considered by researchers. In [52] authors have proposed use of blockchain with fog computing to overcome various data security issues, Tanweer A. proposed IoT-Fog as a middleware architecture using Blockchain technology [53], Pardeep Kumar et al. fog layer as controller nodes, working in distributed manner for orchestration in concatenation with software defined network (SDN) [91]. In the proposed models, blockchain operates at the fog level, where all the incoming requests are recorded over blockchain. In software defined approaches, this scheme works as orchestration. Such type of integration at fog layer might be fair approach for IoT devices, where they don't need to perform mining operation. But as fog is introduced to reduce latency and speed up response time for real time applications, in such scenarios, the real time applications have to suffer with long latency due to involvement of blockchain over the fog layer. Thus, such approaches would not be suitable for an environment where IoT devices belongs to different priorities and generates multiple type of requests. Such as medical emergency, accident avoidance, etc. are the mission critical applications and suppose to receive instant response.

Another proposed scheme is using fog computing blockchain-based distributed key management architecture (BDKMA) to enable multiblockchains operable in the cloud for achieving cross-domain access [87]. Carbone et al. also proposed blockchain at Cloud and Fog both layers in supply chain management settings of IoT [92]. Such approaches enhance the CDC-IoT security solution by implementing blockchain over both fog and cloud layers of IoT. Similar

to previous approaches, the issue of latency for real time applications and energy consumption of CDCs is again a great challenge to deal by adopting these setups.

Ali Dori et al. proposed smart home using blockchain and overlay networks [93]. The smart home devices and fog nodes are combined to create peer-to-peer blockchain network, where fog nodes act as mining nodes which reduces processing efforts of end devices, and the end devices acts as the client nodes with no mining capabilities. This approach and similar other proposals have a potential solution for future Internet technology, but on the large scale, for overall IoT setup, where a number of RT requests are also part of IoT ecosystem is a matter of great concern. Furthermore, the industrial or scientific application, which requires a huge amount of processing and storage capacity for historical data analysis is troublesome approach for overall blockchain network.

### E. EXPECTATIONS FROM BLOCKCHAIN INTEGRATION in IoT

In sharp contrast to related work, it is clear that integration of blockchain in IoT should be considered for issues related to latency, security, privacy, power consumption, processing, storage capacity, response to real time applications, industrial data analytics, and reliable communication. However, the existing proposals mainly focus on entire shift of working paradigm of IoT, which may not be a suitable option for resource constrained devices, and furthermore they also require a big change in hardware technologies. There exist several other proposals that suggests dealing with security, privacy, processing, storage capacity and reliable communication issues, by deploying blockchain at fog and/or cloud layer and leaving behind issues like: industrial data analytics, quick response to real time applications, and energy consumption. An optimum solution for blockchain integration in IoT is needed, which inherits the features of blockchain with minimum upgradation of existing IoT ecosystem, and also prevent the shortcomings of CDC-IoT.

On the basis of discussed characteristics of blockchain and IoT in earlier part of this section, we can summarize the expectations from blockchain integration in IoT as following:

1) Blockchain and IoT are the missing parts of same puzzle and are made for each other. As blockchain provides security, anonymity, tamperproof ledger, distributed network, no central control and a reliable communication mechanism. On the other hand, CDC-IoT provides, huge processing, storage capacity and well-developed software and hardware technologies.
2) With current states of Blockchain, the integration will result in reduced response time and throughput. As blockchain mining operation is time consuming and currently adding an Ethereum block requires 12 to 15 seconds. Where the average number of transactions in a block varies in between 200 to 300 transactions. Thus, it is natural that in current state of blockchain, the integration will result in increased latency and reduced throughput.
3) It is challenging, but we need to come up with an optimum solution for future IoT with minimal upgradation in existing CDC-IoT architecture.

In response to that, we propose a DualFog-IoT architecture which integrates the blockchain in existing architecture and provide a viable solution for future Internet technologies with minimal changes in CDC-IoT architecture. The proposed DualFog-IoT architecture and its three configurations are discussed with details later in Section III.

### F. SIMULATION TECHNIQUE AND TOOLS

The selection of simulation tool is critical, because the proposed model in this article concatenate two different systems, the blockchain and CDC-IoT architecture. Several simulators have been used for performance analysis of CDC-IoT architecture, specially the cloud-based systems are commonly evaluated using CloudSim, GreenCloud, CloudAnalyst, iCanCloud, GridSim, MDCSim, NetworkCloudSim, and EMUSIM. However, those tools lacks in the capabilities for observing the dynamic behavior of CDC-IoT [94]. Furthermore, these tools are not feasible for simulation of blockchain-based systems. On the other side, blockchain-based systems can be simulated using Ethereum Test Net, which is used to measure the behavior of smart contracts before deploying on publicly available blockchain [95]. Similar type of option for simulation of bitcoin blockchain is available as Bitcoin Test Net [96], another Simulator named as SimBlock has also been proposed in [97] which simulates the neighbor node discovery and block propagation time. But the suitable option for observing behaviors related to IoT which involves fog and cloud layers are not available in any of blockchain simulator.

In [28], [98] authors have proposed architectural modeling for performance analysis of IoT ecosystem using queuing theory simulation and extract a number of useful performance metrics for in depth analysis of routine tasks by varying the arrival rate. The proposed models are simulated using queuing theory simulator Java Modeling Tool (JMT) which is an open source discrete event simulator for evaluating the performance of computer and communication systems [55].

Quan-Li et al. proposed mathematical modeling using queuing theory for simulation of blockchain [99]. In [92] authors have proposed simulation of the blockchain using single $M/M/c$ queue in JMT for QoS related parameters. Memon et al. proposed model based on two *M/M/1* and $M/M/n$ queues (one for memory pool another for mining pool) with fork/join stations, the simulation is also performed in JMT. The article presents detailed analysis for a variety of performance metrics useful for observing behavior of blockchain-based applications before deploying them over blockchain network [68].

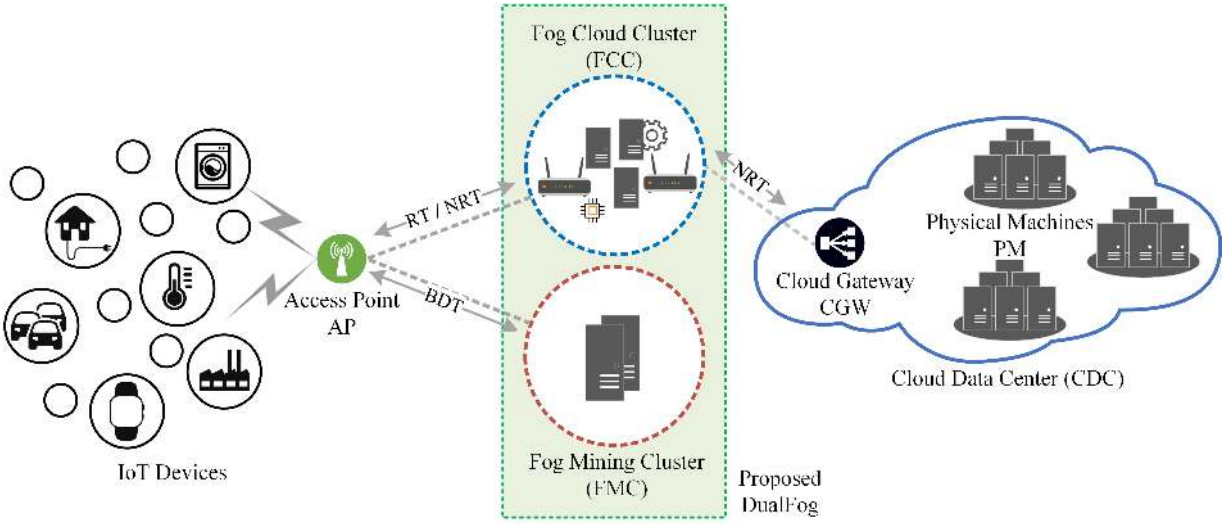


**FIGURE 2.** Proposed DualFog-IoT architecture.

## III. PROPOSED DualFog FOR IoT

In this article we propose a model to cope up all the issues in existing IoT by inheriting the benefits of blockchain with minimal changes in the CDC-IoT ecosystem. We propose DualFog to segregate the fog layer into two; Fog Cloud Clusters (FCC) and Fog Mining Cluster (FMC). In this section, we present the construction of its architecture, and will summarize the details related to each layer. As name suggests, the Fog level is updated in proposed architecture by adding or segregating the existing Fog computing devices. The Architecture is still a three-layer architecture as shown in Figure 2 with an additional neighboring layer at fog level.

### A. CONSTRUCTION OF ARCHITECTURE

This section describes the composition of proposed DualFog architecture and presents the working of each layer in that. The proposed architecture is composed of three layers, Device Layer, DualFog Layer, and the Main Cloud Data Center (CDC) Layer. There are four main components of proposed architecture need to be described: Devices at device layer, Access Point (AP), DualFog (Including: FCC and FMC), and CDC.

#### 1) DEVICE LAYER

All the data generated from IoT devices doesn't belong to blockchain or go for assembling in blocks, in our proposed model, blockchain devices and their generated data is considered to tolerate latent responses. The devices employed over fire alarm, traffic collision avoidance, or medical data belongs to the RT requests because these are mission critical applications and require instant responses. Annual business reports, scientific data compilation, weather updates are kind of NRT requests because these types of applications need long time with powerful processing and higher storage capacity, running such application over blockchain will consequently overwhelm the network with lots of junk. While the data communication with smart electric meters, smart parking lot, smart home appliances, etc. are the type of DTB applications.

The IoT devices which belongs to DTB applications are the part of blockchain network and runs the lightweight blockchain for communication with transient storage along with its dedicated functions. The existing devices in IoT are compromised in terms of resources, so the proposed model implements only the lightweight blockchain over them. Each node possess a public key and a private key, in blockchain the public key is used for communication purpose and visible to all the nodes in network, and Rivest–Shamir–Adleman (RSA) cryptosystem can be used to manage the visibly available public key identity of the devices in blockchain network [100]. While the private key is a secrete key of device used for encryption of generated data/transactions, this key resides inside the local memory of a device. Rootstock or Ethereum are one of the good options for creating blockchain enabled devices, however, as discussed earlier EtheEmbeded, Ethraspbian, Raspnode and Bitmain are the embedded devices with built-in services are also alike to run lightweight blockchain client application [45]–[48].

#### 2) ACCESS POINT (AP)

The access point is the communication device exist near to the end devices or at the edge of devices, it is a controller-based AP. All the incoming and outgoing requests acquire the services of AP as passage for generated data. The AP works as the forwarding device of all incoming requests and serves as the main memory pool of blockchain where the transactions (incoming requests) wait for being selected by the miners of FMC Cluster. The AP implements rules for forwarding specific application requests to one of the two fog clusters on the basis of pre-defined configurations, in this article we enlist a

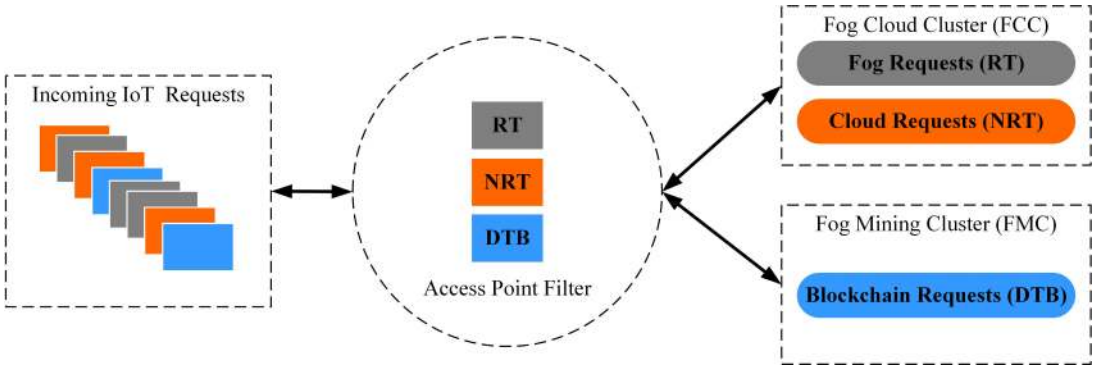


**FIGURE 3.** Publish subscribe model for proposed DualFog-IoT.

few most common applications belongs to each configuration (RT, NRT and DTB). The RT application requires instant response such as; e-health care, traffic management, vehicle-to-vehicle communication, accident avoidance and rescue, city surveillance, fire alarm, industrial sensors, machinery alerts, and tools control etc. The NRT applications could be the applications lenient to the latency and requires huge hardware resources; such as industrial data analytics, large cloud storage, weather updates, and other large storage and processing related tasks. While, a list of applications tolerant to long delays for preserving security, privacy, tamperproofness, reliability and trust to conduct fearless communication, are the DTB applications, the examples of such applications are: cryptocurrencies, renting, sharing, selling, real estate, supply chain, insurance, smart metering, smart grid, smart farming, smart home appliances, smart shopping, parking lots, etc. The AP forwards the RT and NRT applications to FCC and accumulates requests for blockchain to the FMC in its transient memory. All the nodes in blockchain network have their own local memory pool for holding the latest transactions of network. But the AP in proposed architecture works as both communication device and main memory pool of the blockchain network.

As shown in Figure 3, the proposed DualFog-IoT implements publish subscribe model. The publish/subscribe model is typically consists of three components, publisher, broker and subscriber. The Publisher in system is any data generator, it sends the generated data to network, it can be an end user, a server, a sensor or any other device. While the broker is deployed over the AP, it works as the filter of application type. The data coming from underlying heterogenous IoT devices, blockchain miners or cloud and fog servers is filtered over here. A variety of application requests/responses are categorized and forwarded to its corresponding subscribed system. Subscriber is the beneficiary or receiving end of generated data. In our proposed model there are three subscribers for outgoing requests, which are FCC, CDC and FMC. While for incoming responses the corresponding receiving nodes are subscribed to receive the updates related to RT, NRT and DTB.

### 3) DUALFOG LAYER

The proposed DualFog layer is different than Fog layer in CDC-IoT layout, as this layer is virtually separated into two sister/adjacent layers Fog Cloud Cluster (FCC) and Fog Mining Cluster (FMC), The DualFog layer comprises of multiple type of hardware resources such as smart gateways, core network routers, switches in WAN, wireless access points, and more importantly fog computing devices. Figure 4 shows the schematic diagram of DualFog, it is the middle layer of proposed architecture which includes FCC and FMC with computation, storage and forwarding resources. Given below is the working of FCC and FMC.

#### *a: FOG CLOUD CLUSTER (FCC)*

This layer working is similar to existing fog layer in CDC-IoT architecture, the FCC receives RT and NRT requests from AP and provide instant response to the mission critical applications, while the applications with requirements of high processing, storage, and large amount of incoming data in batches are the NRT requests, and are forwarded to the main cloud over Layer 3.

#### *b: FOG MINING CLUSTER (FMC)*

The nodes in this cluster are the part of blockchain node network, FMC is dedicated to perform the mining operations and responsible to maintains the distributed ledger. The main benefit of FM cluster is that it offers services to the underlying end devices. FMC computing node executes mining algorithm(s) as solo miner blockchain nodes while the client nodes (end devices) run the partial node software of blockchain as light wallet (lightweight node software). Solo miner's functions include: storage, mining and routing of the incoming requests whereas the lightweight is the type of node which only deal with routing and wallet functionalities in blockchain [49]. It should be noted that wallet in IoT scenario is the incoming raw data from environment. The FMC network can be represented as a set of individual miners ($FM_1$, $FM_2$, $FM_3$,... $FM_N$).

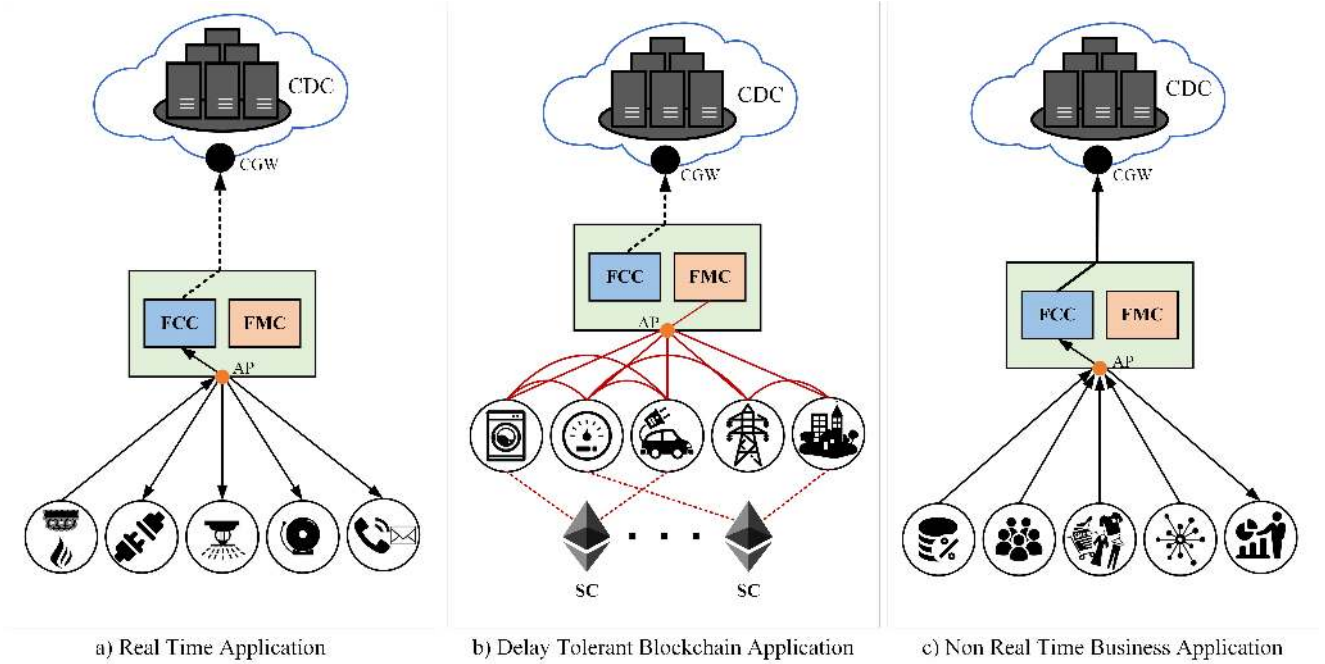


**FIGURE 4.** Three configurations of proposed DualFog-IoT architecture showing use cases.

When it reaches the specified size of a block at AP's memory pool, the least used nodes in FMC receives the new block $B_n$. Once the block is received over FMC, it starts to find the correct target number by incrementing and iterating through the nonce. Discovering the correct nonce can be represented as:

$$BlockHash\,(BlockHeader \cup nonce) \leq D \tag{1}$$

where, *BlockHash* represents the cryptographic function such as SHA256, *BlockHeader* contains the metadata of block, such as hash of previous and current block, timestamp and the contracts included in new block. Once the nonce is found and the block is generated successfully, the correct nonce and *BlockHash* is forwarded to the blockchain network as a proof for achieving consensus to get verification and updating of local copy of blockchain at every node.

We consider Ethereum in this paper for blockchain implementation, thus the block generation time is in between 12 to 15 seconds. But as block generation time is impulsive, the count of blocks $B_c$ can be calculated by $T/B_t$. Where $T$ is the total time, and $B_t$ is the average time taken to mine a block.

Similarly, as in blockchain, the difficulty level is required here too, because at any time the addition of new miners in FMC layer can speed up the mining process and the security of blockchain could be easily compromised. To maintain time in between the mined blocks, the difficulty level can be adjusted periodically.

$$Tg_{new} = Tg_{old}\frac{t}{B_c \times t_{mine}} \tag{2}$$

where $Tg_{new}$ is new difficulty of target, $Tg_{old}$ is existing difficulty, $t$ is total time taken by a certain number of blocks and $t_{mine}$ is the average time for mining a block, that is 12 to 15 seconds in case of Ethereum.

In case, the frequency of block generation exceeds the set limit, the difficulty increases, and if the number of miners has reduced, and the frequency of block generation is lower than the target number, then difficulty is lessened.

#### 4) MAIN CLOUD

The main cloud is also working similarly as in existing CDC-IoT architecture. With the plenty of hardware and software resources CDC is involved in heavy processing and analytics tasks from IoT devices.

### B. WORKING CONFIGURATIONS OF DualFog IoT

The proposed DualFog-IoT implements three configurations, this section describes the working of each configuration. Figure 4 (3), (b) and (c) illustrates each configuration with corresponding example; configuration 1 is about RT requests, configuration 2 for DTB request, and configuration 3 is NRT request.

#### 1) CONFIGURATION 1

As shown in figure 4 (a) the configuration 1 is depiction for a Real-Time (RT) system. The real-time systems are to response quickly to any incoming requests in nearly no time. However, there is latency involved for decision and communi-

cation, but focus for such applications is to quickly response for certain actions.

*a: Use case of RT Requests*

As shown in figure 4 (a), there is a smoke detection system installed in a building for a set of instant rescue actions if the fire is detected, the system takes four actions in emergency condition: 1) It disconnects the electricity for whole building except smoke detection system, 2) It starts all sprinkler in nearby proximity, 3) Sends Emergency alert to the residentials in apartments and management department 4) It inform for help to fire rescue station by sending message and/or call. The system is a real time system, everything should be done as quickly as possible with minimum latency. The sensors in IoT ecosystem sends data to the Access point (AP), if incoming request is from smoke sensor then AP immediately forward the incoming request to the FCC, which take action 2, 3, 4 and 5 simultaneously.

### 2) CONFIGURATION 2

Figure 4 (b) shows the example of DTB application. The delay tolerant blockchain-based applications are those application which can be delayed for some time, this configuration mainly focus on applications which needs blockchain for preserving tamperproof contracts, such as supply chain, smart grid, smart farming etc.

*a: Use case for DTB requests*

As shown in Figure 4 (b), there are 5 nodes shown in the network for example purpose. However, there could be a large number of nodes involved in such a scenario. It depicts a greedy scenario for power hungry electric objects. The nodes included in Figure 4 (b) are: a smart EV charging station, smart home appliances, a smart electric meter, and the smart grid. The objects establish a contract with smart meter that, if the electricity unit price is lower than certain set threshold (load limit is underutilization) then don't have a limit on the usage, but keep control on usage during peak hours. Meeting the required amount of electricity to keep the cost lower can be calculated using following equation 3.

$$\sum A_{req} \leq L_C - L_R \tag{3}$$

where the amount of electricity requested by the node(s) is $A_{req}$, $L_C$ is the community load limit in kW, $L_R$ is the regular load limit in kW.

The smart contract is executed on FMC with a given time slot as shown in Algorithm 1. By the end of time slot, the greedy algorithm for solving Knapsack problem is executed, which sorts the contracts in descending order with respect to arrival of requests $A_{req}$. It is Finally each object will be assigned with certain electricity for a given time slot. The Knapsack problem is a combinatorial problem of optimization for obtaining maximum gain when the resources are limited. The aim of knapsack is to find an optimum object

**Algorithm 1:** Example Pseudo Code for Smart Contract of Electricity Usage and Allocation

```
SmartContract CommunityElectricityUsage
    function community Capacity (Lc, Lr)
        // charging capacity
        Maxcapacity ← Lc − Lr
    Struct ChargningUnits (Areq, priority,
    schedule)
    Struct SmartHomeAppliances (Areq,
    priority, schedule)

    // Charging stations list of addresses
    ChargningUnits List []
    // Smart home appliances list of
    addresses
    SmartHomeAppliances List []

    function ChargingReqReceived (Areq,
    publicKey)
        if (Authorization && publicKey)
            Set Lr ← LR
            Set priority
            Set timeSlot
        End

    function KnapSack()
        // sor CUs decending order
        Quicksort (CUsList.length−1)
        // sort SHA decending order
        Quicksort (SHome.length−1)
```

from a set of objects, where each object is associated with a certain weight and value. The objective of knapsack problem is to select maximum valued objects with minimum weight. In smart grid management systems, this greedy algorithm is used to calculate optimum price and user need or waiting time [101].

For the complexity of the Algorithm 1 suppose that, if there are $g$ number of incoming requests from Charging Units and $h$ number of incoming requests from Smart Home appliances. Then the cardinality of structure *CUsList* is $g$ and the cardinality of structure *SHome* is $h$. The algorithmic complexity of using Knapsack approach with parameters *CUsList* and *SHome* is $O(g \times h)$. Further, the algorithmic complexity of quicksort would be $O(g\ log(g))$ and $O(h\ log(h))$. Thus the overall complexity of the Algorithm 1 can be represented as maximum of all complexities i.e. $\max\{O(gh), O(g\ log(g)), O(h\ log(h))\}$.

### 3) CONFIGURATION 3

Finally, the Figure 4 (c) shows configuration for NRT applications, these applications are also a type of delay-tolerant applications, but the main focus of such applications is to execute power and computation hungry applications over remotely located servers without worrying about the underlying infrastructure (server, network, storage, and hardware). The example of such applications is business data analysis for yearly targets, intelligent user recommendation systems etc.

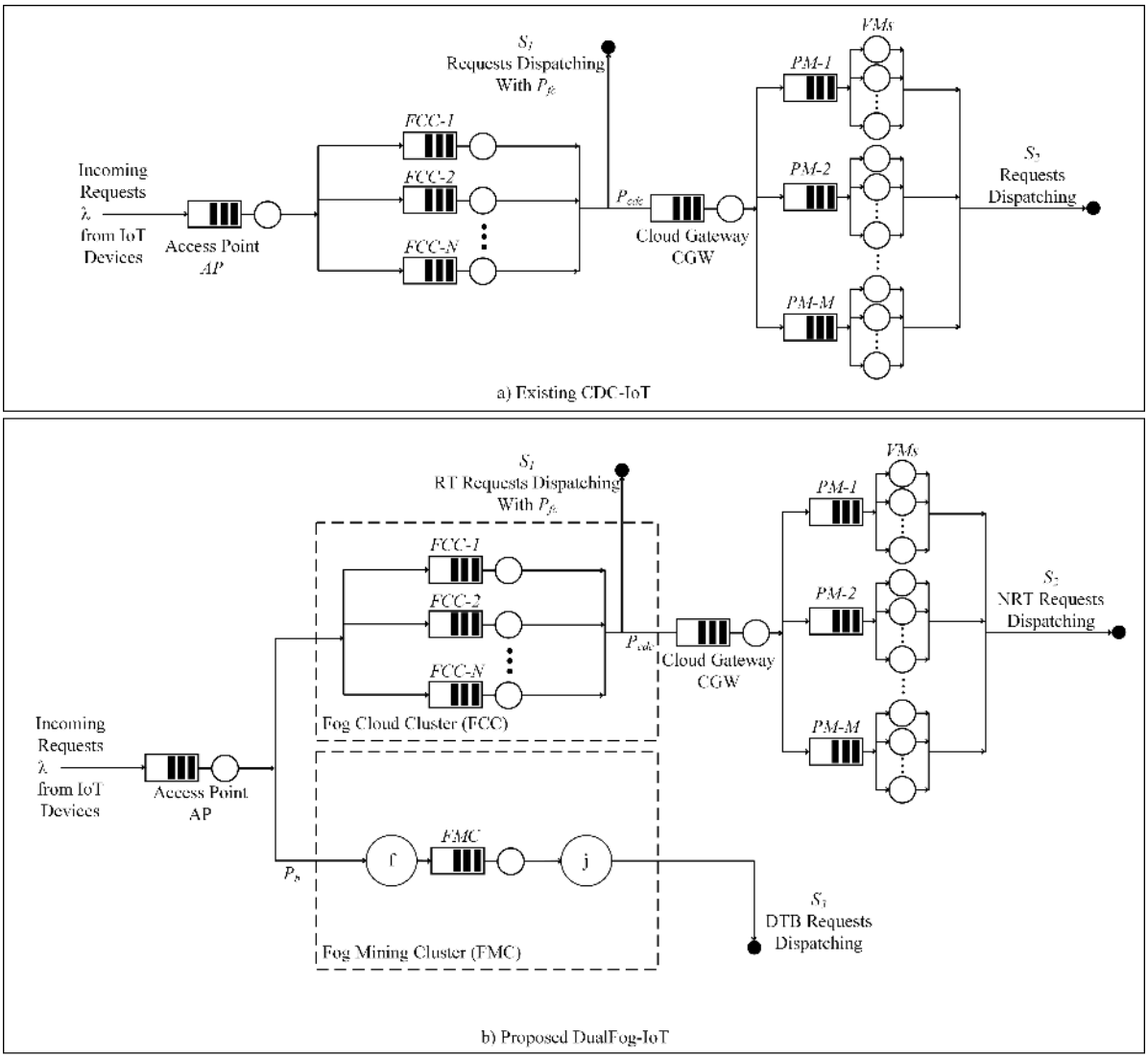


**FIGURE 5.** Queuing model for FC-IoT and DualFog.

*a: Use case of NRT requests*

Figure 4 (c) shows the data collection scenario from online shopping application for customized recommendation system. Consider a very simple online shopping scenario, the application collects the data for a number of similar products from different makes varying in quality, price and style. Each activity related to product is recorded, such as, customers visited, customer added to likes, customer added to shopping cart. The recommendation system pushes the related products on customer's wall in future, for which he/she expressed interest by performing any or all of above given activities. This scenario belongs to NRT business application, it needs to collect data from customers, and store the historical data for recommendation system to establish the meaningful analysis for business owners. Such requests are transferred and executed over the CDCs.

## IV. SIMULATION SETUP

### A. QUEUING MODEL FOR PROPOSED DualFog

The simulation is performed separately for existing CDC-IoT and DualFog-IoT architectures. In both simulations the resources related to Fog, which is FCC in proposed DualFog-IoT, and the CDC-IoT are identical, they work exactly as in existing CDC-IoT. The comparison is made for revealing the differences before and after integration of Blockchain in existing framework. The simulation modeling is done in JMT version 1.0.3 on MacBook Pro 2011, 13-inch version, Operating System EI Capitan with 2.3 GHz Intel Core i5, 6 GB memory, 500 GB SSD, and 384 MB Graphics card.

Figure 5 (a) shows the CDC-IoT simulation model, where all the incoming requests are forwarded to Fog Layer, a number of tasks get involved in processing there locally and eventually leaves the system at departure station $S_1$ with probability of $P_{fc}$ after completion, while the remaining tasks $P_{cdc}$

**TABLE 1.** Simulation Parameters for CDC- IoT architecture.

| Parameters | Description | Values |
|---|---|---|
| $\lambda$ | Request Arrival Rate (Req/s) | 300 to 3000 |
| $1/\mu_e$ | Mean Fog Computing Service Time (s) | 0.005 |
| $1/\mu_g$ | Mean Request at Cloud Gateway (s) | 0.0003 |
| $1/\mu_c$ | Mean VM Service Time (s) at each PM in Cloud | 0.02 |
| $C_e$ | Capacity of requests at each Fog Node | 300 |
| $C_c$ | Capacity of requests of each PM at cloud | 500 |
| $C_g$ | Capacity of requests at Cloud Gateway | 3000 |
| $Pfc$ | Probability of request being served at Fog | 0.6 |
| $P_{cdc}$ | Probability of request forwarded to main Cloud | 0.4 |
| $FCC$ | Number of Stations at Fog Layer | 3 |
| $PM_m$ | Number of Physical Machines over Cloud Layer | 5 |
| $VM_n$ | Number of Virtual Machines in each PM | 5 |
| $Q_e$ and $Q_c$ | Queue Policy and Drop Rule of Fog Layer | FCFS and Drop |

**TABLE 2.** Additional simulation parameters for DualFog-IoT.

| Parameters | Description | Values |
|---|---|---|
| $1/\mu_m$ | Mean Service Time of Mining-Pool (s) | 0.05 |
| $C_n$ | Capacity of requests at Memorypool (Access Point) | $\infty$ |
| $C_m$ | Capacity of requests of Mining-Pool | 300 |
| $C_f$ | Capacity of requests of Fork Station | 300 |
| $B_{size}$ | Batch Size at Fork/Join Stations | 300 |
| $P_b$ | Probability of request forwarding to Blockchain | 0.4 |
| $Q_b$ | Queue Policy and Drop Rule of Blockchain Layer | FCFS and BAS |

are forwarded to CDC for processing, the tasks have been processed at CDC departs at station $S_2$. In contrast to that, Figure 5 (b) shows the proposed DualFog-IoT, which appends an additional layer Fog Mining Cluster (FMC) adjacent to Fog (FCC), and is dedicated as a computation pool for block mining (mining cluster). Now, not only RT and NRT requests, but the DualFog-IoT architecture also consider Blockchain requests in system. Thus, incoming RT and NRT requests which belongs to Configuration 1, and Configuration 2 are forwarded to FCC layer and works similarly as mentioned above in CDC-IoT. While the Blockchain requests belongs to Configuration 3, are forwarded to FMC. The FCC, CDC and FMC, all layers have their respective sinks as $S_1$, $S_2$, and $S_3$. The mathematical modeling and formulation for CDC-IoT systems can be seen from [28], [94], [98]. And the mathematical modeling and formulation for blockchain integration can be seen in [68], [99].

Table 1 shows the simulation parameters used to simulate CDC-IoT Model as shown in Figure 5 (a). Table 2 shows the additional simulation parameters related to integration of blockchain FMC as shown in Figure 5 (b). Both models are observed for obtaining a number of QoS parameters; performance curves such as: system drop rate, utilization of FCC, utilization of CDC mean, overall system utilization, mean number of requests in system, system response time, and system throughput. Furthermore, to investigate the different configurations of proposed DualFog-IoT, the number of requests leaving system per second at $S_1$, $S_2$, and $S_3$ are also obtained to see the responsiveness of proposed model.

To benchmark the proposed system, we assume that the requests sent from IoT devices are database queries or some other type of services for which the Service Level Agreement (SLA) is to receive a response from one to three seconds and the system throughput should be in between 500 to 800 requests/sec. The purpose of SLA in any client server model is to establish a contract between the service provider and service consumer, it is assumed as a foundation of customer's trust in the service provider [102], [103].

Describing the parameters for both models from table 1 and table 2. All the incoming requests in both models from IoT devices are Poisson processes with arrival rate $\lambda$ (the number of requests per second). The incoming Poisson processes means that inter-arrival time of incoming data is independent and exponentially distributed random variable with $1/\lambda$. To make it simple, we assume that incoming IoT data is being served as FCFS (First Come First Served) among all the queue stations, while the queuing policy is Drop Rule for AP, FCC, CGW and PMs, while it is Block After Service (BAS) for FMC. BAS pause the incoming requests on reaching a certain set limit, which is the block size in blockchain, in our case it is 300. The AP receives the incoming data and forward them with probability $P_{fc}$ (RT and NRT tasks) to FCC, and $P_b$ to FMC. AP is modeled as *M/M/1* queue with infinite queue length to prevent from the loss of incoming IoT data from devices.

The CGW serves as a load balancer for Physical Machines (PMs) in CDC. The processing time of CGW is independent identically distributed (i.i.d) exponential random variable with mean rate $1/\mu_g$. FCC nodes ($FCC_1$ *to* $FCC_N$) are i.i.d with service time $1/\mu_e$ and are implemented as $M/M/1/C_e$ queue. In FMC the Fog Miner with service rate $1/\mu_m$ is implemented as *M/M/1* queue and finite capacity $C_m$. The number of Fog Miners (FM) can be increased to participate in the mining process as a mining pool, where the incoming jobs should be distributed among all the FMs and satisfies the specified mining time ($1/\mu_m$). Thus, we considered only single FM in our simulation to keep it simple, because even with increased number of FMs we cannot decrease the service time due of difficulty level of hash puzzle in blockchain mining as shown in equation 2.

There is one set of fork and join station surrounding FMC, the fork station is with finite capacity is $C_f$, and triggers a number of requests after reaching certain threshold $B_{size}$ as a block size. The join station combines the jobs after being

served by FM to reform the batch. The CDC is a resourceful service station, and have multiple PM, where each PM have a number virtual machines (VM) running on a single hardware which are simulated by increasing number of servers in each PM queue station, thus the cloud datacenter is simulated by using $M/M/VM_n/C_c$.

## V. RESULTS

In this section we present results obtained by simulating both, the DualFog-IoT and existing CDC-IoT. It is obvious that to have blockchain at any layer may decrease the system throughput and increases number of requests in system and response time. But the key is to bring up a setup with minimum compromises to inherit the benefits of blockchain in IoT ecosystem. All the presented results in this section are comparing both architectures on QoS performance indices, The simulation is performed for ten times by varying the arrival rate each time, which is from 300 to 3000 per second. The results obtained are represented by line curves where the square and triangle markers indicates the occurrence of increased arrival rate. Blue lines representing the proposed DualFog-IoT while the magenta shows the results obtained from simulation of CDC-IoT. Vertical axis is number of requests/second, and the horizontal axis is increasing the arrival rate.

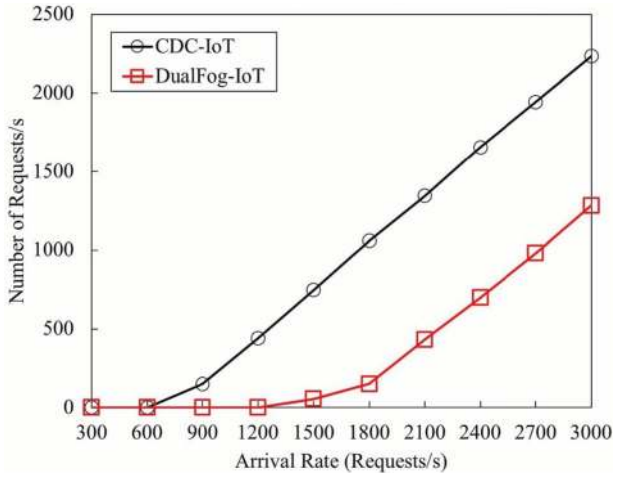


**FIGURE 6.** System drop rate.

Figure 6 shows the number of packets lost or dropped during the transmission. It is a well-known fact that packet lost or drop occurs due to large number of packet flow over a network which goes beyond its capacity (network congestion). As blockchain is a peer to peer network, and all the full nodes keep a copy of shared ledger, thus the packet loss or drop ratio is very less or negligible. The simulation results are evident to that, in CDC-IoT, after 600 requests/s, system starts facing high number of packet losses, and the count of packet loss keeps growing with increased number of incoming requests/s. So that when arrival rate of requests/s reaches to 3000, the number of requests dropped is 2233. In contrast to that proposed DualFog-IoT has proved to be no-lossy up to 1200 requests/s, and starts experiencing packet loss at 1500 requests/s, where the number of dropped packets is 55, when the incoming request/s reaches to 1800, the packet is 153, the constant exponential rate of packet loss can be observed from 2100 to 3000 requests per second. When the arrival rate hits 3000 requests/s the maximum drop rate is 1283. The average drop rate of CDC-IoT architecture is 31.9%, while the average of drop rate for DualFog-IoT is only 11.9%.

As the CDC is built with large number of hardware and software resources, thus the capital and operational cost (CAPEX and OPEX) is very high. Furthermore, CDC doesn't only consume the huge electric power but also carbon emission is a big threat to environment. Besides that, the expensive management of giant CDCs has also raised the pricing of services. There is ongoing research as discussed in section II, the research groups are enthusiastic for minimizing the energy consumption, and carbon emission of CDCs to promote the greencloud concept.

Figure 7 (a) shows the computing resource utilization for Fog layer in CDC-IoT and FCC layer in DualFog-IoT. The CDC-IoT architecture system utilization reaches to 100% for Fog layer when the arrival rate reaches to 900 requests/s. And for DualFog-IoT FCC utilization, when arrival rate reaches 1200 requests/s the utilization of FCC starts to operate at 100%. There is a minor indication of increased efficiency on FCC layer in DualFog-IoT here. But a huge difference can be observed in Figure 7 (b), where the utilization of CDC resources is compared for both architectures. In CDC-IoT, the CDC hardware resource utilization reaches 100% when arrival rate reaches 900 requests/s. And in DualFog-IoT, the utilization of hardware resources starts from 10% and when arrival rate reaches 900 requests/s the utilization becomes 30%, after that, the utilization of hardware resources remains under 32% throughout the simulation. However, on average the DualFog-IoT hardware resource utilization for CDC is 28% only, while the average of CDC in CDC-IoT is 92%.

As in DualFog-IoT, we have a mining cluster also, and we already know that there is no any idle time in mining operation of blockchain. There is always a block awaiting in queue to get served, even if its empty, the mining operation always needed to be perform [68], so it is obvious that, the utilization of mining station FMC is 100% from very beginning. We have two fog stations FCC and FMC in our proposed model, to compare both architectures in terms of resource consumption, Figure 8 shows overall system utilization of CDC-IoT architecture which includes Fog and CDC layers; however, the DualFog-IoT includes FCC, FMC and CDC. It can be seen clearly from Figure 8, that the DualFog-IoT still out perform even after adding intense utilization of mining operation of FMC (100%). Therefore, the overall system resource utilization of CDC-IoT is 92% while the DualFog-IoT is still at 72%.

Figure 9 shows the impact of varying workload on the systems response time. It is clear that the response time of both

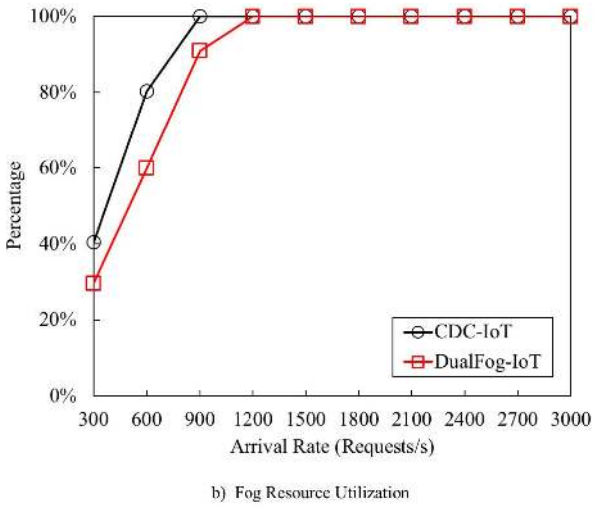


**FIGURE 7.** Resource utilization of FC-IoT vs. DualFog IoT.

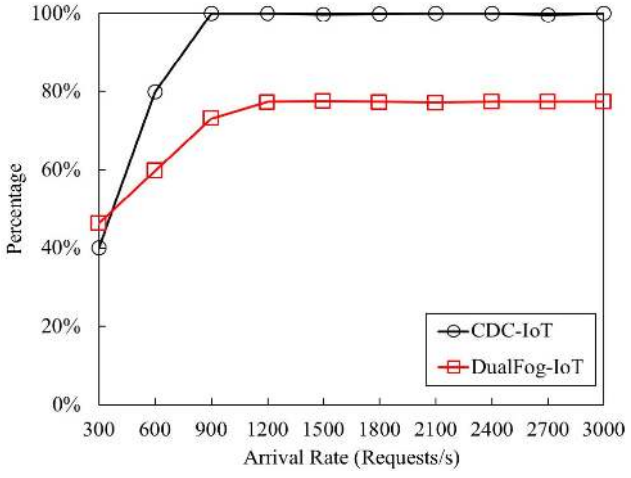


**FIGURE 8.** Overall system resource utilization.

systems increases by elevating arrival rate. Up to the incoming workload of 600 requests/s the CDC-IoT architecture delivers a good performance, and is considered as low latent.

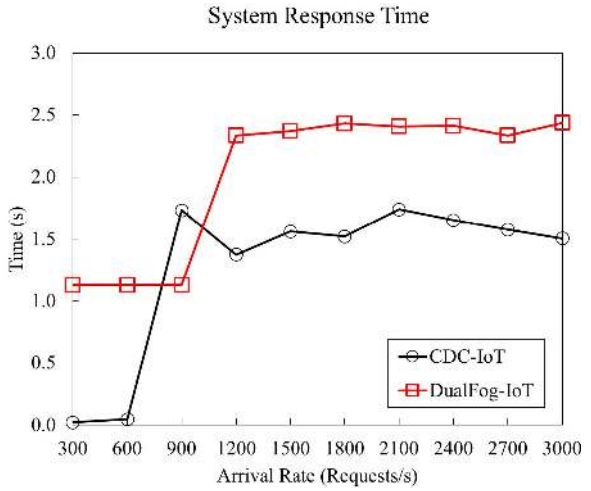


**FIGURE 9.** System response time.

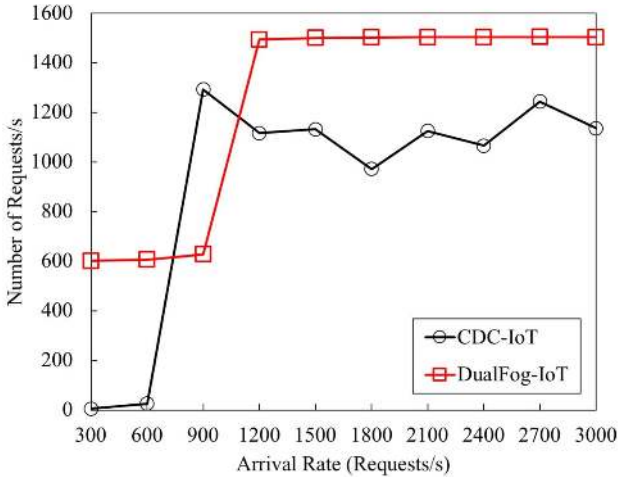


**FIGURE 10.** Mean number of requests in system.

However, with the increase of arrival rate of 900 requests/s to 3000 requests/s the system response time is also increases in between 1.3s to 1.7s. On the other side the proposed architecture response time is high and is long latent from very beginning, in start the response time is 1.1 requests/s and when the arrival rate hits in between 1200 and 3000 the response time increases reaches to a persistent rate of 2.3 and 2.4 requests per second. However, it should be noted that the DualFog-IoT still doesn't violate the SLA of system response time, as stated in section IV.

Figure 10 is the mean number of requests available in the system at any given time. The use of dedicated blockchain layer has an impact to increase number of requests in system. It can be seen that for CDC-IoT up to the arrival rate of 600 requests/s the mean number of requests in the system are under 30 only; however, a rapid rise can be observed when the number of incoming requests/s increases. From 900 to 3000 requests/s the average of 1130 requests are always in the system queue, waiting for to be served. The DualFog-IoT

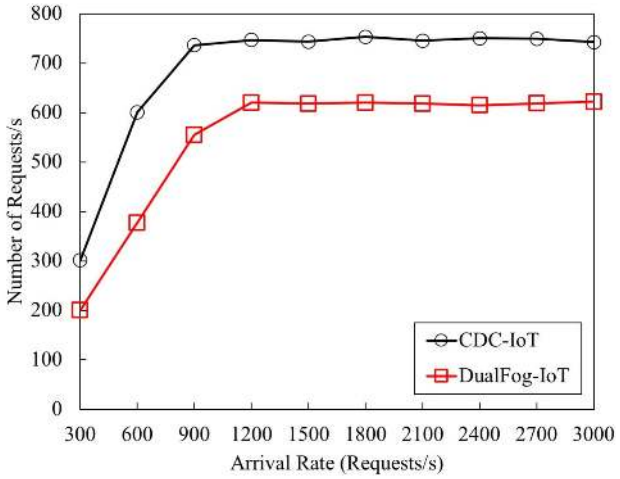


**FIGURE 11.** System throughput.

**TABLE 3.** Comparison of CDC-IoT and DualFog-IoT.

| QoS Parameters | Average | | Outperformer (△) Underperformer (□) | |
|---|---|---|---|---|
| | CDC-IoT | DualFog-IoT | CDC-IoT | DualFog-IoT |
| System Drop Rate | 957.59 | 359.9 | □ | △ |
| Fog Utilization (%) | 92 | 88 | □ | △ |
| Cloud Utilization (%) | 92 | 28 | □ | △ |
| Overall system utilization (%) | 92 | 72 | □ | △ |
| System Response Time | 1.29 | 2.01 | △ | □ |
| System # of Requests | 998.52 | 1235.03 | △ | □ |
| System Throughput | 687.11 | 546.67 | △ | □ |

starts with 600 requests pending in system, that is because of the accumulation of jobs in AP and Fork station for creating a block, and when the arrival rate becomes 1200 requests/s the number of requests in the system has also increased.

This increased number of requests in pending are due to the accumulation of requests for block, the size of a single block is restricted to 300 requests only. Thus, the number of requests in service and number of requests ready to get served immediately upon release of mining resource are exposing as increased number of requests in system along with regular RT and NRT requests. In any Blockchain-based systems, this situation cannot be avoided, because there are always jobs in the system waiting to form a block and this count will always remain in there. Furthermore, with the increased arrival rate the accumulation of requests in overall system has also been influenced, and raised up to 1500 requests for proposed model, which is the sum of requests available in FCC, PMs at CDC, awaiting requests in memory-pool (AP), and the Fork stations and FMC stations.

Figure 11 shows the system throughput, according to our simulated model the existing architecture is able to complete 300 to 745 requests/s for the arrival rate of 300 to 3000 requests/s. However, the DualFog-IoT can complete 200 to 630 requests/s in response to 300 to 3000 arrival requests/sec.

It is fact that blockchain integration in IoT comes with a number of compromises on QoS, which is already predicted by several researchers and proved by our results discussed until now. But it is also fact that in return, blockchain has secure, tamperproof, trustless and a distributed system to offer.

The results presented in this section provides several performance indices related to QoS, and presented a healthy comparison of both CDC-IoT and proposed DualFog-IoT. Table 3 further provides the summary of those results, it is very clear that, the proposed DualFog-IoT out performs in terms of system drop rate, computing resource utilization for fog, cloud and overall system. While the CDC-IoT architecture outperforms in system response time, mean number of requests in system and system throughput. However, the DualFog-IoT still satisfies the agreements of service parameters in terms of system response time and system throughput.

It is also worth noting that blockchain in comparison to cloud computing is an immature technology, and the simulation presented in this paper follows the current standards and stats of blockchain in Ethereum, which is in its phase of improvements. Ethereum co-founder Vitalik Buterin said in an interview with Abra that *"Ethereum blockchain right now can process 15 to 20 transactions a second, really we need like 100,000 transaction a second to be a viable platform in future."* [104]. Thus, it is not so far when blockchain can outperform with less latent block mining process. Moreover, even if we consider blockchain in its current status and settings, the results presented in this paper tells that the delay tolerant applications of IoT should run a trustless society on the top of blockchain platform. By doing this not only CDCs will be offloaded, but also this will bring a huge difference in energy consumption and carbon emission in environment which is currently a big challenge for researcher's community.

In section III, we suggested three configurations of the proposed model for dealing with three categories of incoming requests. We assume that there are three type of requests coming from IoT devices, RT, NRT, and DTB application requests.

Figure 12 shows the throughput of three type of requests capture at the departing station of the proposed model $S_1$, $S_2$, and $S_3$. The RT requests departed at $S_1$ from FCC Layer are represented by blue line with + marker, NRT requests forwarded to cloud and leaving at departure station $S_2$ are represented by black line with circular marker, while the

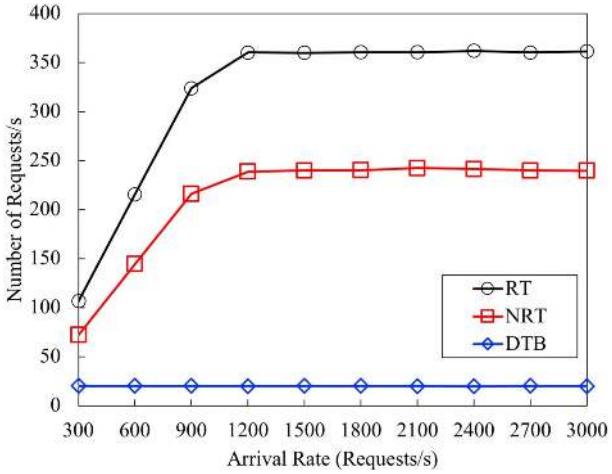


**FIGURE 12.** Number of completed requests/s for three configurations in DualFog-IoT.

**TABLE 4.** Split ratio of RT vs. NRT requests.

| Simulation Number | Split Ratio (Realtime vs. Non Realtime) | System Number of Requests | System Response Time | System Drop Rate | System Throughput | Utilization | |
|---|---|---|---|---|---|---|---|
| | | | | | | FCC | CDC |
| 1 | RT=0.2, NRT = 0.8 | × | × | × | × | ✓ | ✓ |
| 2 | RT = 0.4, NRT = 0.6 | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3 | RT = 0.6, NRT = 0.4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4 | RT = 0.8, NRT = 0.2 | ✓ | ✓ | ✓ | ✓ | ✓ | × |

DTB application requests leaving at $S_3$ and are represented by red line with asterisk marker. It can be seen in Figure 12, that incoming RT requests are being served on priority at FCC layer, while the NRT requests are performed at CDC, thus facing certain delays. However, as the current stats of Ethereum suggests, the blockchain layer is constrained to process only a limited number of requests/s. The average throughput at $S_1$, $S_2$ and $S_3$ are: RT is 318 requests/s, NRT is 212 requests/s and DTB is 20 requests/s.

## VI. ANALYSIS AND OPTIMIZATION OF DualFog-IoT

In this section further, analysis and optimization of proposed DualFog-IoT is presented. Figure 13 shows the impact of varying number of virtual machines at cloud layer. Figure 13 (a) to (f) presents System Number of Requests, System Response Time, System Drop Rate, System Throughput, Utilization of Resources at Fog and Cloud Layer, and Throughput of each configuration. The axis x shows the variation of number of VMs in cloud environment, which essentially mean to vary the number of servers in this simulation, instead of varying PMs, the same result is obtained by varying VMs in here. All the results presented before are conducted with 5 VMs per PM, in this simulation all other parameters are exactly same as shown in table 1 and table 2, only the allocation of computing resources ($VM_n$ in this case) is changing in each iteration. The resulting graphs shows the average of each simulation iteration executed by increasing number of VM by 1; and the arrival rate is also varying in each simulation ($\lambda = 300$ to 3000).

Figure 13 (a) to (f) shows that when number of $VM_n$ is 2, all QoS parameters are satisfactory. At a particular time when there are two number of $VM_n$, System number of requests shown in Figure 13 (a) are 1266, System response time is 2.97, system throughput is 547.51, and System drop rate is 507.9. However, the utilization of cloud resources is 82.02%, even if we further decrease $VM_n$ to 1, the utilization of cloud resources becomes 95.6%, but a drastic raise can be observed in system number of requests and response time. And also drop rate and throughput are affected here, drop rate has increase from 507.9 to 588.6 and overall system throughput has reduced from 547.51 to 444.97. Furthermore, same effects can be observed in throughput of RT and NRT requests. So, the optimum number of allocated resources for cloud layer $VM_n$ is 2 in our presented scenario, which is the saving of almost 60% computing resources than existing CDC-IoT.

Keeping the number of $VM_n$ to two, the proposed DualFog-IoT model is further analyzed for handling RT and NRT requests by varying the probability of incoming RT and NRT requests at Fog and Cloud layers respectively. Probability of variation considered in each simulation is as, in first simulation the RT=0.2 and NRT = 0.8, in second simulation RT = 0.4 and NRT = 0.6, in third simulation RT = 0.6 and NRT = 0.4 and in fourth simulation RT = 0.8 and NRT = 0.2.

The number of DTB requests is unchanged in Figure 14 (f), as it is a well-known fact that public blockchain is not good at handling the increased number of requests due to its limitations of time-consuming consensus mechanism. Thus, no any change is being made in the split ratio of forwarded requests to FMC and FCC at AP. Simulation one Figure 14 (f) shows throughput of RT requests is 105, and NRT requests is 283. In simulation two, RT is 211 and NRT is 272, simulation three RT is 316, and NRT is 211 and simulation four has RT is 422 and NRT is 105 as a throughput. Table 4 shows the summary of probability of split ratio for RT and NRT requests in the system. According to simulations conducted in Figure 14, Table 4 shows satisfactory performance as (✓) and unsatisfactory performance as (×).

On the basis of Table 4 it can be easily predicted, that when the allocation of more computing resources is required at cloud layer, or the resources can still be minimized as in the case of simulation 4.

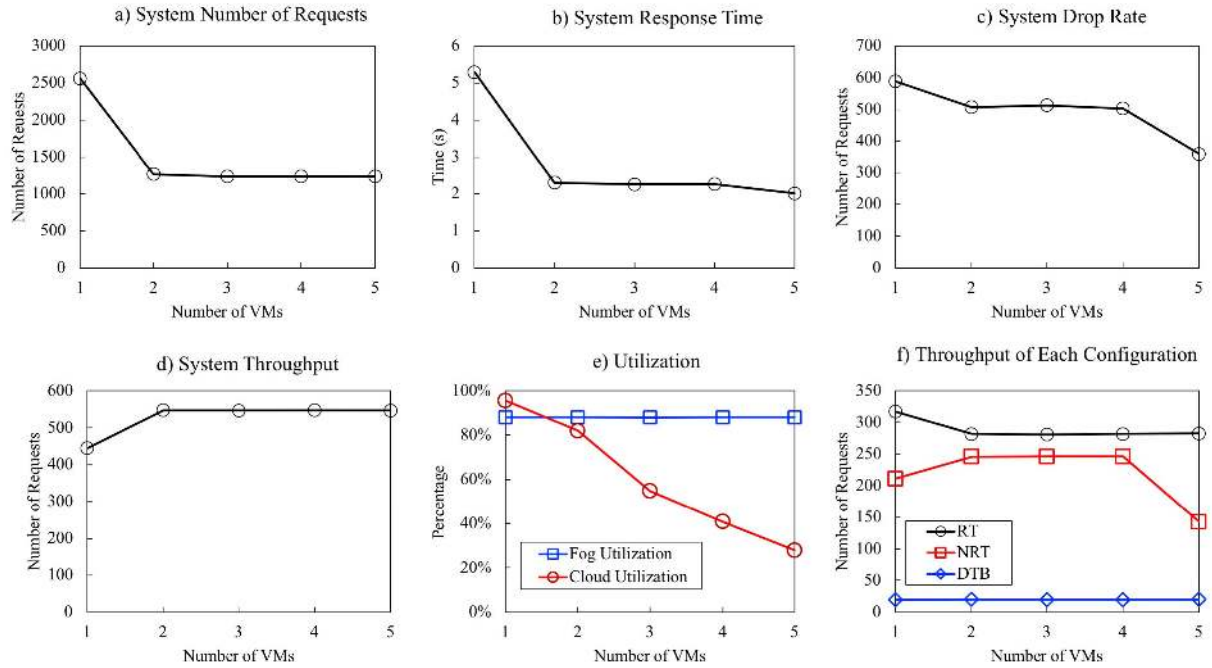


**FIGURE 13.** Varying Number of Computing Resources in Cloud Layer of proposed DualFog-IoT (a) System Number of Requests (b) System Response Time (c) System Drop Rate (e) System Throughput (e) Utilization of Fog and Computing Resources (f) Throughput of each configuration.

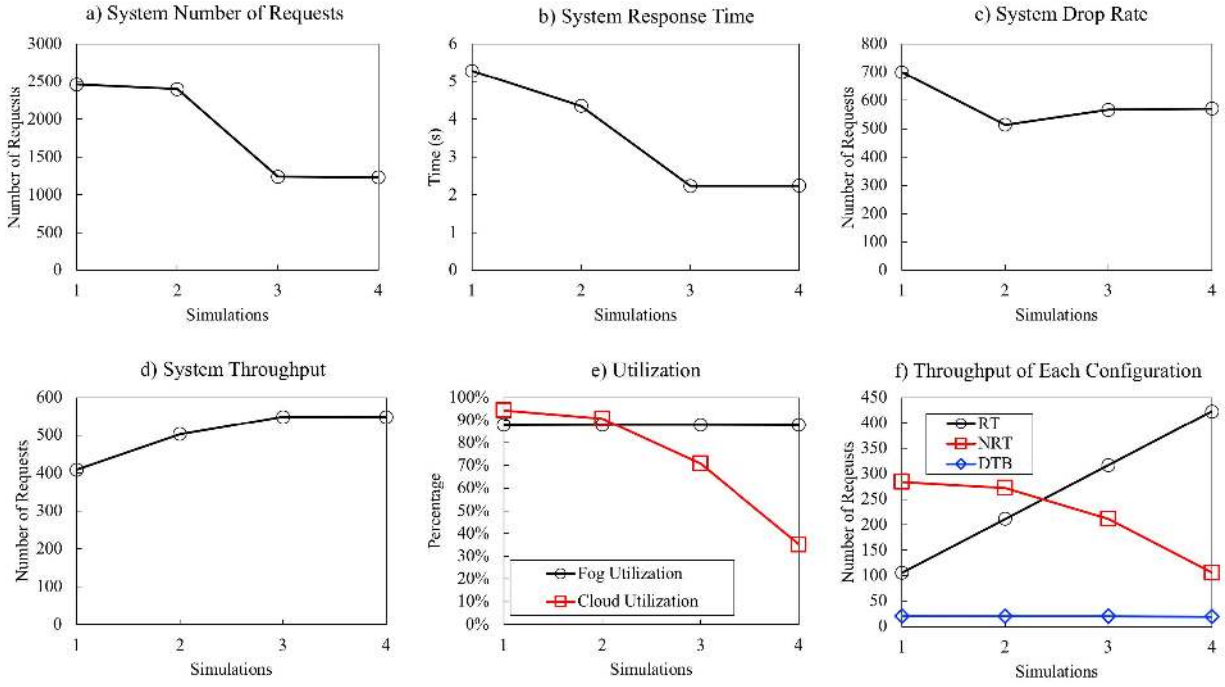


**FIGURE 14.** Varying ratio of RT and NRT requests (a) System number of requests (b) System Response Time (c) System Drop Rate (e) System Throughput (e) Utilization of Fog and Computing Resources (f) Throughput of each configuration.

## VII. LIMITATIONS

It should also be noted, that in our simulation model, all the incoming messages from IoT devices follows Poisson arrival, and also the service time of all the stations used in simulation is exponentially distributed. However, in real systems the incoming requests may vary and follows different patterns (like streaming and burst arrivals which are common with IoT environment) depending on the content and type of data. Where the contents maybe coming from sensors, smart phones, business, traffic density etc. And similarly,

the required service time for each type of data may always not be exponential. But, it is also worth noting that, for obtaining adequate approximation of real systems, the Poisson arrival and exponential service time has been used literature [28], [67], [99], [105], [106].

## VIII. FUTURE RECOMMENDATIONS

As discussed earlier, thinking of integration of blockchain in IoT would results in latent responses and reduced number of throughput. And, it is challenging to find a suitable solution to provide the services of blockchain for creating a trustless society with minimum upgradation in existing IoT ecosystem. We proposed DualFog-IoT, considering the limitations of blockchain, the proposed model is an optimum solution for its integration in IoT, and the results presented in this paper supports our hypothesis. However, three configurations proposed in this paper are solely on the basis of type of applications, further service layer agreements and policies are required for this type of integration. As fusion of Blockchain and IoT would become the huge change in entire communication ecosystem, thus remaking policies and prioritizing needs is one of the primary requirements of this technological amendment, and should be considered for future research directions.

## IX. CONCLUSION

In recent years several research efforts have been taken to integrate the blockchain in IoT. Most of the available approaches propose the integration of blockchain at device level and requires an entire shift of working paradigms of existing Internet of Things (IoT) technology. Which is not suitable solution mainly because IoT devices are resource constrained and blockchain requires substantial amount of computing resources. Some other proposals suggest to integrate the blockchain at one of the layers of existing Centralized Datacenter based IoT (CDC-IoT) like at Fog and/or at cloud. These proposals mainly focus to deal with the issues like; security, privacy, processing power, storage capacity and reliable communication; and leaving behind the issues related to response to real-time applications, industrial data analytics and energy consumption.

In response to that we propose a DualFog-IoT architecture, which segregates the computing resources of Fog layer in to two, the first part is named as Fog Cloud Cluster (FCC), and another is Fog Mining Cluster (FMC). The proposed architecture comes up three configurations namely: Real-Time (RT), Non-Real Time (NRT), and Delay Tolerant Blockchain (DTB) application requests. The Access Point (AP) in between Device layer and DualFog layer works as a filter for these configurations, the RT and NRT application requests are forwarded to FCC, from which RT requests are performed locally at FCC, while the NRT requests are forwarded to the cloud datacenter (CDC). However, the incoming DTB type of requests are kept on hold over AP for accumulation to the size of a block. Once the block is formed it is forwarded to the FMC for mining. To validate the usability of our proposed DualFog-IoT architecture, we used queuing network simulation Java Modeling Tool (JMT) to simulate both the proposed DualFog-IoT and existing CDC-IoT models.

The presented results in section V shows that proposed DualFog-IoT outperform by reducing the drop rate and utilization of computing resources at FCC and CDC layer. Saving computing resources, doesn't only mean to minimize the CAPEX and OPEX but it eventually reduces power consumption and carbon emission in environment. Furthermore, the responsiveness of system has also been recorded for proposed three configurations of DualFog, and the average throughput/s for different applications is as: RT is 318, NRT is 212 and DTB is 20 requests per second.

Results presented in section V, shows that cloud resources are underutilization. Thus, the analysis and optimization of proposed DualFog-IoT is also presented in section VI, which shows the feasibility of proposed architecture by tuning the computing resources and the RT vs. NRT request ratios.

As expected the integration of blockchain in DualFog-IoT has its visible impact on system response time, mean number of requests in system and system throughput. But yet, the proposed model has not violated the agreements of service, and satisfying the specified SLAs.

Hence it is concluded that, blockchain integration with IoT is applicable and it should be done, but the matter is how wisely we handle it. The proposed architecture provides a base system for future Internet technologies. This integration doesn't only inherit blockchains' benefits, but will also have a large impact on the quality of life by reducing the carbon emission of giant CDCs.

## REFERENCES

[1] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.
[2] *Cisco Internet Business Solutions Group (IBSG)*, IEEE 802.11 Standard, CISCO, San Jose, CA, USA, Apr. 2007, p. C1-1184.
[3] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2012, pp. 257–260.
[4] B. Fitzgerald, "Software crisis 2.0," *Computer*, vol. 45, no. 4, pp. 89–91, Apr. 2012.
[5] M. Collina, G. E. Corazza, and A. Vanelli-Coralli, "Introducing the QEST broker: Scaling the IoT by bridging MQTT and REST," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 36–41.
[6] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, *Vision and Challenges for Realising the Internet of Things*, vol. 3, no. 3. Luxembourg City, Luxembourg: Cluster of European Research Projects on the Internet of Things, European Commission, 2010, pp. 34–36.
[7] G. White, A. Palade, C. Cabrera, and S. Clarke, "IoTPredict: Collaborative QoS prediction in IoT," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2018, pp. 1–10.
[8] N. Javaid, A. Sher, H. Nasir, and N. Guizani, "Intelligence in IoT-based 5G networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 94–100, Oct. 2018.
[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2017.
[10] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, Aug. 2015.

[11] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. 10th Int. Conf. Wireless Algorithms, Syst., Appl.*, 2015, pp. 685–695.
[12] P. Li, J. Li, Z. Huang, C.-Z. Gao, W. Bin Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Comput.*, vol. 21, no. 1, pp. 277–286, Mar. 2017.
[13] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.
[14] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.
[15] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating Internet of Things and cloud computing and the issues involved," in *Proc. 11th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2014, pp. 414–419.
[16] *Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog*. Accessed: Feb. 24, 2018. [Online]. Available: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[17] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 287–292.
[18] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, 2012, p. 13.
[19] M. Saad, "Fog computing and its role in the Internet of Things: Concept, security and privacy issues," *Int. J. Comput. Appl.*, vol. 180, no. 32, pp. 7–9, 2018.
[20] Í. Goiri, R. Beauchea, K. Le, T. D. Nguyen, M. E. Haque, J. Guitart, J. Torres, and R. Bianchini, "Greenslot: Scheduling energy consumption in green datacenters," in *Proc. Int. Conf. High Perform. Comput., Netw., Storage Anal.*, 2011, pp. 1–11.
[21] A. Khosravi and R. Buyya, "Energy and carbon footprint-aware management of geo-distributed cloud data centers: A taxonomy, state of the art, and future directions," in *Sustainable Development: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2018, pp. 1456–1475.
[22] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.
[23] R. Memon, J. Li, J. Ahmed, M. Nazeer, and M. Ismail, "Cloud-based vs. blockchain-based IoT: A comparative survey and way forward," in *Frontiers of Information Technology & Electronic Engineering*. Springer, 2019. [Online]. Available: http://www.jzus.zju.edu.cn/iparticle.php?doi=10.1631/FITEE.1800343
[24] "Fog computing and the Internet of Things: Extend the cloud to where the things are," Cisco Syst. Inc., San Jose, CA, USA, White Paper, 2015. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf
[25] M. Ficco, C. Esposito, Y. Xiang, and F. Palmieri, "Pseudo-dynamic testing of realistic edge-fog cloud ecosystems," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 98–104, Nov. 2017.
[26] *OpenFog Consortium*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.openfogconsortium.org/
[27] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of iot devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct./Nov. 2018, pp. 1–8.
[28] S. El Kafhali and K. Salah, "Efficient and dynamic scaling of fog nodes for IoT devices," *J. Supercomput.*, vol. 73, no. 12, pp. 5261–5284, Dec. 2017.
[29] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, Jan. 2017.
[30] A. Banafa, "IoT and blockchain convergence: Benefits and challenges," *IEEE IoT Newslett.*, Jan. 2017. Accessed: Feb. 23, 2018. [Online]. Available: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html
[31] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.
[32] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. p. 9. [Online]. Available: https://www.bitcoin.org
[33] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, Dec. 2018.
[34] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino, L. Raso, M. Castiglione, E. Pinci, D. Del Vecchio, G. Colle, A. R. Proto, G. Sperandio, and P. Menesatti, "A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain," *Sensors*, vol. 18, no. 9, p. 3133, Sep. 2018.
[35] C. Qu, M. Tao, and R. Yuan, "A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes," *Sensors*, vol. 18, no. 9, p. 2784, Aug. 2018.
[36] *Slock.it—Blockchain + IoT*. Accessed: Feb. 24, 2018. [Online]. Available: https://slock.it/
[37] *Enabling the Future of IoT Filament*. Accessed: Feb. 24, 2018. [Online]. Available: https://filament.com/technology
[38] *Ambisafe Software*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.ambisafe.co/
[39] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
[40] *Trusted IoT Alliance*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.trusted-iot.org/
[41] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
[42] Multichain. (2018). *Multichain | Open Source Blockchain Platform*. Multichain. Accessed: Apr. 25, 2019. [Online]. Available: https://www.multichain.com/
[43] JPMorgan Chase & Co. (2019). *Quorum | J.P. Morgan*. QuorumTM Advancing Blockchain Technology. Accessed: Apr. 25, 2019. [Online]. Available: https://www.jpmorgan.com/global/Quorum
[44] H. Di A. Company. (2019). *Hdac | Hdac*. HDAC Blockchain IoT. Accessed: Apr. 25, 2019. [Online]. Available: https://www.hdactech.com/en/Hdac/hdac.do
[45] (2019). *Eth(Embedded)-Ethereum Clients on Embedded Devices*. Accessed: Apr. 25, 2019. [Online]. Available: http://ethembedded.com/
[46] (2019). *Armbian Ethereum client for NanoPC-T4*. Accessed: Apr. 25, 2019. [Online]. Available: http://ethraspbian.com/
[47] (2019). *Raspnode*. Accessed: Apr. 25, 2019. [Online]. Available: http://raspnode.com/
[48] (2019). *Bitmain*. Accessed: Apr. 25, 2019. [Online]. Available: https://www.bitmain.com/about
[49] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
[50] C. Pahl, N. El Ioini, S. Helmer, and B. Lee, "An architecture pattern for trusted orchestration in IoT edge clouds," in *Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2018, pp. 63–70.
[51] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[52] M. Farhadi, D. Miorandi, and G. Pierre, "Blockchain enabled fog structure to provide data security in IoT applications," Jan. 2019, *arXiv:1901.04830*. [Online]. Available: https://arxiv.org/abs/1901.04830
[53] T. Alam, "IoT-fog: A communication framework using blockchain in the Internet of Things," Mar. 2019, *arXiv:1904.00226*. [Online]. Available: https://arxiv.org/abs/1904.00226
[54] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," in *Proc. 10th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2018, pp. 561–564.
[55] M. Bertoli, G. Casale, and G. Serazzi, "JMT: Performance engineering tools for system modeling," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 36, no. 4, pp. 10–15, 2009.
[56] "Cisco fog computing solutions: Unleash the power of the Internet of Things," Cisco Syst. Inc., San Jose, CA, USA, White Paper, 2015. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-solutions.pdf
[57] P. Maiti, J. Shukla, B. Sahoo, and A. K. Turuk, "Mathematical modeling of QoS-aware fog computing architecture for IoT services," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2019, pp. 13–21.
[58] M. Iorga, L. Feldman, R. Barton, M. Martin, N. Goren, and C. Mahmoudi, "Fog computing conceptual model," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Pub., 2018, pp. 500–325.
[59] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in *Big Data and Internet of Things: A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014, pp. 169–186.

[60] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, 2012, p. 13.
[61] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2014, pp. 464–470.
[62] M. Aazam and E.-N. Huh, "Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2015, pp. 687–694.
[63] I. Abdullahi, S. Arif, and S. Hassan, "Ubiquitous shift with information centric network caching using fog computing," in *Computational Intelligence in Information Systems* (Advances in Intelligent Systems and Computing), vol. 331, 2015, pp. 327–335.
[64] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," in *Proc. ASE BigData SocialInform.*, 2015, p. 28.
[65] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 826–834.
[66] G. Seibold and S. Samman, "Consensus immutable agreement for the Internet of value," KMPG, China, Tech. Rep., 2016. [Online]. Available: https://home.kpmg/cn/en/home/insights/2016/09/blockchain-consensus.html
[67] R. A. Memon, J. Li, J. Ahmed, A. Khan, M. I. Nazir, and M. I. Mangrio, "Modeling of blockchain based systems using queuing theory simulation," in *Proc. 15th Int. Comput. Conf. Wavelet Active Media Technol. Inf. Process. (ICCWAMTIP)*, Dec. 2019, pp. 107–111.
[68] R. A. Memon, J. P. Li, and J. Ahmed, "Simulation model for blockchain systems using queuing theory," *Electronics*, vol. 8, no. 2, p. 234, Feb. 2019.
[69] M. Jabłczynska, K. Kosc, P. Ryś, R. Ślepaczuk, P. Sakowski, and G. Zakrzewski, "Why you should not invest in mining endeavour? The efficiency of BTC mining under current market conditions," Dept. Econ. Sci., Univ. Warsaw, Warsaw, Poland, Working Papers 2018-18, 2018.
[70] *Trending Blockchain Cryptocurrency*. Accessed: Apr. 26, 2019. [Online]. Available: https://cryptoslate.com/
[71] E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *Proc. 25th USENIX Conf. Secur. Symp.*, 2016, pp. 279–296.
[72] Blockchain. *Bitcoin Explorer*. Accessed: Apr. 26, 2019. [Online]. Available: https://www.blockchain.com/
[73] *White Paper · Ethereum/Wiki Wiki · GitHub*. Accessed: Nov. 20, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper
[74] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi. (2015). *A Programmer's Guide to Ethereum and Serpent Acquiring the Virtual Machine*. pp. 1–20. Accessed: May 6, 216. [Online]. Available: https//mc2-umd.github.io/ethereumlab/docs/serpent_tutorial.pdf
[75] B. Singhal, G. Dhameja, and P. S. Panda, "Building an ethereum DApp," in *Beginning Blockchain*, Berkeley, CA, USA: Apress, 2018, pp. 319–375.
[76] *Home-Hyperledger*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.hyperledger.org/
[77] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, Jul. 2016, p. 4.
[78] (2019). *Blockchain Platform User*. Accessed: Apr. 29, 2019. [Online]. Available: https://www.rsk.co/
[79] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[80] (2019). *Blockchain Platform | MultiChain*. Accessed: Feb. Apr. 27, 2019. [Online]. Available: https://www.multichain.com/
[81] (2019). *Blockchain Application Platform | Lisk*. Accessed: Apr. 27, 2019. [Online]. Available: https://lisk.io/
[82] (2019). *Chronicled*. Accessed: Apr. 27, 2019. [Online]. Available: https://www.chronicled.com/
[83] P. K. Sharma, S.-Y. Moon, and J.-H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.
[84] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[85] *Streamr*. Accessed: May 12, 2019. [Online]. Available: https://www.streamr.com/
[86] M. Samaniego and R. Deters, "Internet of smart things—IoST: Using blockchain and CLIPS to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Jun. 2017, pp. 9–16.
[87] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34045–34059, 2019.
[88] A. Boudguiga, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2017, pp. 50–58.
[89] A. Hameed, A. Khoshkbarforoushha, R. Ranjan, P. P. Jayaraman, J. Kolodziej, P. Balaji, S. Zeadally, Q. M. Malluhi, N. Tziritas, A. Vishnu, S. U. Khan, and A. Zomaya, "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems," *Computing*, vol. 98, no. 7, pp. 751–774, Jul. 2016.
[90] A. P. Shveta, "Energy conservation and security issues in cloud computing: A review," *Int. J. Adv. Comput. Sci. Cloud Comput.*, vol. 2, no. 1, pp. 57–60, 2014. [Online]. Available: http://iraj.in/journal/IJACSCC/paper_detail.php?paper_id=686&name=Energy_Conservation_And_Security_Issues_In_Cloud_Computing:_A_Review
[91] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.
[92] A. Carbone, D. Davcev, K. Mitreski, L. Kocarev, and V. Stankovski, "Blockchain based distributed cloud fog platform for IoT supply chain management," in *Proc. 8th Int. Conf. Adv. Comput., Electron. Elect. Technol. (CEET)*, 2018, pp. 51–58.
[93] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[94] S. El Kafhali and K. Salah, "Performance analysis of multi-core VMs hosting cloud SaaS applications," *Comput. Standards Interfaces*, vol. 55, pp. 126–135, Jan. 2018.
[95] *Rinkeby: Ethereum Testnet*. Accessed: May 9, 2019. [Online]. Available: https://www.rinkeby.io/#stats
[96] *Testnet, Testing Network—Bitcoin Glossary*. Accessed: May 9, 2019. [Online]. Available: https://bitcoin.org/en/glossary/testnet
[97] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, "SimBlock: A blockchain network simulator," Jan. 2019, *arXiv:1901.09777*. [Online]. Available: https://arxiv.org/abs/1901.09777
[98] S. El Kafhali and K. Salah, "Performance modelling and analysis of Internet of Things enabled healthcare monitoring systems," *IET Netw.*, vol. 8, no. 1, pp. 48–58, Jan. 2018.
[99] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queueing theory," Aug. 2018. [Online]. Available: https://arxiv.org/abs/1808.01795
[100] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.
[101] Z. A. Khan, "Hybrid meta-heuristic optimization based home energy management system in smart grid," *J. Ambient Intell. Humanized Comput.*, vol. 10, pp. 4837–4853, Dec. 2018.
[102] S. K. Garg, A. N. Toosi, S. K. Gopalaiyengar, and R. Buyya, "SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter," *J. Netw. Comput. Appl.*, vol. 45, pp. 108–120, Oct. 2014.
[103] M. A. Khoshkholghi, M. N. Derahman, A. Abdullah, S. Subramaniam, and M. Othman, "Energy-efficient algorithms for dynamic virtual machine consolidation in cloud data centers," *IEEE Access*, vol. 5, pp. 10709–10722, 2017.
[104] *Crypto Bites: A Chat With Ethereum Founder Vitalik Buterin—Abra*. Accessed: May 3, 2019. [Online]. Available: https://www.abra.com/blog/crypto-bites-a-chat-with-ethereum-founder-vitalik-buterin/
[105] K. M. Chandy and C. H. Sauer, "Approximate methods for analyzing queueing network models of computing systems," *ACM Comput. Surv.*, vol. 10, no. 3, pp. 281–317, Sep. 2002.
[106] K. Xiong and H. G. Perros, "Service performance and analysis in cloud computing," in *Proc. 5th World Congr. Services (SERVICES)*, 2009, pp. 693–700.

**RAHEEL AHMED MEMON** received the bachelor's degree in computer systems engineering from the Mehran University of Engineering and Technology, Pakistan, in 2005, and the M.S. degree in computer engineering from Myongji University, South Korea, in 2012. He is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, University of Electronic Science and Technology of China. He is also a Faculty Member with the Department of Computer Science, Sukkur IBA University, Pakistan. His current research interests include Internet of Things, blockchain, fault tolerant networking, embedded systems, and image processing.

**JIAN PING LI** is currently a Professor and the Head of International Center for Wavelets Analysis and its Applications (ICWAA), University of Electronic Science and Technology, China. He has published hundreds of technical articles and is the author/co-author of 26 books on the subject of computer science and wavelet. He is the Chairman of many International Conferences and also founder of several Journals in the field of wavelet and computer science. His research interests include wavelet theory, image processing, and pattern recognition.

**MUHAMMAD IRSHAD NAZEER** received the master's degree in computer science from the National University of Computer and Emerging Sciences, Pakistan, and the Ph.D. degree in computer science from Shah Abdul Latif University, Pakistan. He is currently working as an Assistant Professor with Sukkur IBA University. His research interests include core computing, algorithms, computer networks security, and cryptography.

**AHMAD NEYAZ KHAN** received the bachelor's and master's degrees in computer application from Aligarh Muslim University, India, in 2009 and 2012, respectively. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His area of research include information security, image processing, reversible data hiding in encrypted images, machine learning, and Internet of Things.

**JUNAID AHMED** received the B.E. degree in telecommunications engineering from the Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2010, and the M.S. degree in electrical and electronics engineering from Eastern Mediterranean University (EMU), North Cyprus, Turkey, in 2015. He is currently pursuing the Ph.D. degree in non-destructive testing and structural health monitoring using infrared thermography with UESTC, Chengdu, China. He is also a full-time Faculty Member with the Electrical Department, Sukkur IBA University, Pakistan. His current research interests include wavelet processing, super-resolution, quantitative non-destructive testing and evaluation, sparse representations and low rank matrix factorization, and tensor decomposition.