Article

Blockchain-SDN based Energy Optimized and Distributed Secure Architecture for IoTs in Smart Cities

Md. Jahidul Islam [1], Anichur Rahman [2,3,*], Sumaiya Kabir [1], Md. Razaul Karim [3], Uzzal Kumar Acharjee [4], Mostofa Kamal Nasir [3], Shahab S. Band [5,6*], Amir Mosavi [7,*]

[1] Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh; jahidul.jnucse@gmail.com; sumaiya@cse.green.edu.bd
[2] Department of Computer Science and Engineering, National Institute of Textile Engineering and Research (NITER), Dhaka, Bangladesh; anis.mbstu.cse@gmail.com
[3] Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh; razaulkarimce15004@gmail.com; kamal@mbstu.ac.bd
[4] Department of Computer Science and Engineering, Jagannath University, Dhaka, Bangladesh; ukacharjee@gmail.com
[5] Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam; Shahaboddin.shamshirband@tdtu.edu.vn
[6] Future Technology Research Center, College of Future, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan
[7] Department of Mathematics and Informatics, J. Selye University, 94501 Komarno, Slovakia, Kálmán Kandó Faculty of Electrical Engineering, Obuda University, 1034 Budapest, Hungary, and the Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam; amir.mosavi@kvk.uni-obuda.hu
* Correspondence: Shahab S. Band (e-mail: shamshirbandshahaboddin@duytan.edu.vn); Anichur Rahman (e-mail: anis.mbstu.cse@gmail.com); Amir Mosavi (e-mail: amir.mosavi@kvk.uni-obuda.hu)

Abstract: Insecure and portable devices in the smart city's Internet of Things (IoT) network are increasing at an incredible rate. Various distributed and centralized platforms against cyber-attacks have been implemented in recent years, but these platforms are inefficient due to their constrained levels of storage, high energy consumption, the central point of failure, underutilized resources, high latency, and etc. In addition, the current architecture confronts the problems of scalability, flexibility, complexity, monitoring, managing & collecting of IoT data, and defend against cyber-threats. To address these issues, the author presents distributed and decentralized Blockchain-Software Defined Networking (SDN) based energy-optimized architecture for IoT in smart cities. Thus, SDN continuous observing, controlling, managing IoT devices activities and detect possible attacks in the network; Blockchain provides adequate security & privacy against cyber-attacks, reduces the central point of failure issues; Network Function Virtualization (NFV) are used to saving energy, load balancing, as well as increasing the lifetime of the entire network. Also, we introduce a Cluster Head Selection (CHS) algorithm to reduce the energy consumption in the presented model. Finally, we analyze the performance using various parameters (e.g. throughput, response time, gas consumption, communication overhead) and demonstrating the result that provides higher throughput, lower response time, lower gas consumption than existing works for smart cities.

Keywords: SDN; IoT; NFV; Blockchain; SDN Controller; Cluster; OpenFlow; Security; Privacy.

1. Introduction

The world is getting smarter over time because of modern technologies. People can do myriad things that could not be thought of before. To make our habitats more elegant, IoT is lending so many contributions. Nowadays a countless number of sensors from different categories are connected together to move our lives forward. The IoT devices collect data from the real-world and can send them to a processing system where the data could be transferred into a valuable decision. The idea of using RFID to recognize a sensor among the millions of nodes is very impressive and effective in the field of IoT [1]. Some studies show that the approximate amount of devices could be 75 billion by 2025 [2]. That's why the risk of getting attacked by online intruders became higher and it became very difficult to manage such kind of gigantic information on time.

However, IoT devices accumulate informative data in a scattered way as there is no system to arrange the collections of data followed by any systematic as well as scientific procedures. To decorate the huge amount of scattered data, SDN is used with IoT applications with a central controller to support the [3] network configuration and management. It can control the behavior of the data dynamically and change the operational procedures programmatically without hampering the main physical architecture. When there are some vulnerabilities, SDN can easily detect the anomalies and can take some pre-steps to inhibit any kinds of attacks primarily. Apart from these merits, SDN can perform their operations with multiple centralized controllers.

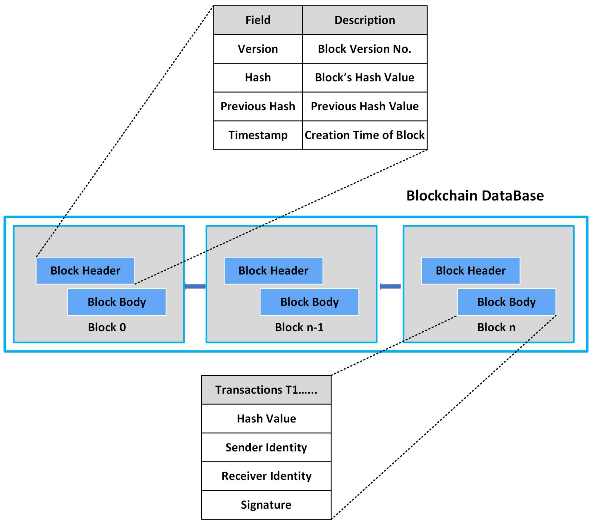

Figure 1. Blockchain Structure

Although SDN is one of the emerging technology which comes with the advantages of managing a massive amount of raw information and primary security, being centralized system causes another major issue into the performance. If any problem occurs in the center point of the controllers, the whole system will be affected and destroyed. On the other hand, DoS and DDoS attacks can cause multiple controller failures [5]. To defeat the individual point of failure, decentralized Blockchain technology comes into action. This decentralized technology can be integrated with SDN based IoT applications where hash values are used to chain the blocks together, and each and every piece of the transaction is permanently saved, as shown in Fig. 1. Security and privacy could be enhanced by integrating this Blockchain technology. A block of code known as Smart Contract (SC) is run to verify and validate a transaction. Once a data transaction is validated, the information is stored in a storage and the index of the data with some other overheads is stored in the block, which is added to the public ledger. The ledger is immutable and impossible to change it by any intruder. Thus Blockchain can prevent the attacks from trespassers and as the transactions are handled by the SC programmatically, once the rules and regulations are established, there is nothing to be worried about the transaction process.

Furthermore, energy consumption is a critical issue while there will be billions of smart devices are connected across the area and such kind of architecture will be applied. The power is required to transmit the information collected by the IoT gateway. So it is also a piece of interest to take care of the amount of energy. Clustering the devices into various groups and selecting one of them to transfer the data to the processing station as the cluster head can lead the action to decrease the power consumption. There are many factors to select the head and some researchers have already proposed different algorithms to choose the Cluster Head (CH). Another modern technique to virtualize the functionality is also very feasible in these types of smart architectures. NFV provides communication services by turning the practicalities of IoT devices into a virtualization [6]. It is the application system where the system is resilient if it gets any changes in the traffic load and failures. To provide dependable communication in networks, different technologies are fused. So it is reasonable to be raised the complexity whenever these technologies will be implemented. Several solutions have been presented by many researchers. The solutions are not capable of fulfilling the criteria, such as some of these solutions leave more security but not perfect in terms of reliability. Some authors proposed a Blockchain-based SDN application, but the architecture is not asserted [8].

Motivating by the above premises, the author presents an energy-optimized and Blockchain-SDN based secure architecture. A CHS method has proposed that selects CH among the clusters with the highest residual energy that balances the energy among the IoT devices. Moreover, SDN controllers dynamically managed IoT device's operational activities that increase security & privacy. In addition, decentralized Blockchain technology is used to reduce the malicious activities of the network also provides security & privacy in the proposed network.

1.1. Contributions of the study

The contributions of this paper as follows:

- Design a distributed and decentralized architecture for IoT the ecosystem which reduces the existing challenges through the use of technologies Blockchain, SDN, and NFV.
- Implement the SDN network on the mininet-wifi emulator and the Blockchain network using Ethereum technology to detect and mitigate the cyber attack in the IoT networks.
- Also, an CHS algorithm is designed for energy optimization among the IoT devices where the highest residual energy is selected as a CH in the cluster.
- Evaluate the performance of the proposed model with two existing works using various simulation parameters that are carried out (e.g., throughput, response time, gas consumption, and communication overhead). We also take into account the attack scenarios (DDoS) for various applications in the proposed model.

1.2. Paper organization

The remaining of the research has been formed as follows: we have studied and discussed the literature review in Section 2. After that, Section 3 presents a distributed architecture for IoT; CHS procedure; Security mechanism flowchart. Moreover, discussions and result analyses of the proposed model are provided in Section 4 comparison with existing works. In addition, the author's conclusion of this paper in Section 5.

2. Literature Overview

Some researchers have addressed in recent years based on emerging leading technology such as Blockchain, IoT, NFV, and SDN technologies. In this section, we are going to represent some literature's overview of recent works:

2.1. IoT with Smart Cities

Stojkosk et al. [9] presented an IoT framework for a smart home under the consideration of home energy management and architectural challenges and solutions. They also emphasized on the data processing issues. They identified a holistic and cloud-centric model integrated with different components of IoT. The authors also analyzed the state of art IoT solutions into their smart home system. They have:

- Analyzing the stream and next challenges for the IoT based on results.
- Smart home defining for a holistic framework with key characteristics and parameters
- A splendid explanation of a holistic framework based smart home management model

In [10], the authors discussed the essential IoTs and intelligent structures for energetic building blocks. They also set the direction for energy optimization and the next management systems for building propagation. Additionally, they also dealt with some of the technical opportunities offered and the professional disputes IoT faces in a smart building. Mehmood et al. [11] introduced the IoT-enabled model for categories of smart cities and networks, possible prospects, and significant desires. Several wireless technologies such as SIGFOX, 6LoWPAN, and IEEE 802.11p were also expended. Furthermore, they highlighted some challenges and directions for future smart technology research. In another research, Hui et al. defined the significant necessities for making a smart home management [12]. Authors remarked seven unique requisite commendations for in-casing the extraordinary quality of the intelligent home control efficiently.

2.2. Cluster Head Selection Approaches

Kumar et al. introduced clustering techniques, which apportioned the extensive system into tiny clusters where every cluster its cluster head (CHs) [13]. Those CHs appropriated the method of period analysis various admittance for fulfilling time grooves to each link. They also mentioned the energy utilization of hops that aided the network to assist in various times. Similarly, Angel et al. presented an Enhanced Energy Efficient Clustering Algorithm (EEECA) for lessening strength tuberculosis in plucking a Cluster Head (CHs) in Mobile Wireless Sensor Networks [14]. On the other study, Al-Baz et al. addressed a special version of the LEACH protocol named Node Ranked–LEACH, which validated the Node Station (NS) algorithm based on system lifetime [15]. In addition, they also promised to succeed in the arbitrary method choice as an algorithm, which in other LEACH variants provides instant failure for different cluster heads. Further, they have also approached varied parameters such as throughput and performance packet ratio, reducing the packet delay and the sensor's energy expenditure. In a similar work, Zhao et al. recommended [16] a transformed LEACH-based cluster-head selection algorithm for WSNs. Additionally, they illustrated different networking perspectives, such as network continuance, energy maintenance, and data volume during the simulation phases.

2.3. IoT with SDN

Kalkan et al. considered the security of various SDN inventions and based on security demands, and they suggested the most appropriate security mechanism in [17]. The authors also discoursed future challenges in the area of IoT environment with a role-based comptroller for preserving security appointed as Rol-Sec for SDN. Moreover, Bull et al. introduced an SDN-based security scheme for the IoT network in [19]. The authors also proposed architecture that unmistakably described the discovery and impediment of the technique of flooding assails for TCP and ICMP. Then, In [20], the authors refreshed different aimed SDN architecture and security solutions for IoT from 2012 to 2016. They analyzed and compared various existing solutions on SDN based on the IoT. Another secure IoT structure based on SDN has been depicted in [22]. Next, In [30], for secure Black SDN-IoT authors proposed a distributed architecture for smart cities with the NFV concept. To improve accessibility,

Table 1. Terminologies and Description in Alphabetically Ordered

Notations	Definition
API	Application Programming Interface
BC	Blockchain
CH	Cluster Head
CHS	Cluster Head Selection
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
IoT	Internet of Things
LEACH	Low-Energy Adaptive Clustering Hierarchy
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
PoW	Proof of Work
QoS	Quality of Service
RPC	Remote Procedure Call
SC	Smart Contact
SDN	Software Defined Networking
SDK	Software Development Kit
TCP	Transmission Control Protocol
WSN	Wireless Sensor Network

protection, and privacy, they used multiple distributed SDN controllers in their proposed architecture. Vandana et al. aimed at a security-based framework for applying SDN to the IoT ecosystem. In addition, Mukherjee et al. presented an SDN basis of disseminated IoT network using NFV execution for smart cities in [3]. The authors also implemented NFV into SDN-IoT architectural network to train cost-efficient, reliable, and springy intelligent cities. Furthermore, they mentioned the cluster head selection procedure and addressed the multiple controllers in the SDN environment. Secure mechanics, introduced by Liu et al. [23] has proposed for handling various assails. The authors proposed SDN for the Middlebox arrangement and flow table capacity constraints . Additionally, they also demonstrated the experimental results of the suggested M-G model and improved the overall safety and perceptive constancy in the IoT network.

2.4. IoT-SDN with Blockchain

Rahman et al. proposed “DistBlockSDN” architecture for smart cities in [26]. Furthermore, they presented a cluster head selection approach for collecting sensors data with low energy dissipation. Besides, the authors evaluated the performances in different parameters such as throughput and packet arrival rate carefully using Blockchain technology. In another research, Sharma et al. [29], through the use of Blockchain technology, proposed an efficient cloud architecture to improve security. However, the proposed model with distributed cloud infrastructure provides the computing infrastructures with secure, minimal cost access. Furthermore, they evaluated their proposal using some performance metrics. But, their performance is not yet the absolute one. The implication of Blockchain with cloud-based IoT is reviewed in [4]. After describing the Blockchain method and classification, the authors discussed the need for Blockchain before implementation in IoT. They analyzed when an organization should use Blockchain in IoT applications and provided an optimized architecture for IoT. After analyzing the IoT based applications security issues, challenges, efficiency, and feasibility, the authors found Blockchain as a solution in [44] and [45]. Moreover, Dorri et al. analyzed the smart home’s functions and core components based on Blockchain for IoT for security and privacy purposes [46]. They used a local and private Blockchain that provides IoT gadgets with secure access control and keeps a time-ordered transaction history for each smart home tier.

Table 2. Existing Work Analysis

Authors	Key Technologies	Architecture	Application	Issues Address	Blockchain Implementation Platform
Sharma et al. [1]	Blockchain, SDN	Centralized, Distributed	IoT Ecosystem	Security & Privacy	Ethereum Network
Rahman et al. [26]	Blockchain, SDN	Centralized, Distributed	Smart City	Security & Privacy	Ethereum Network
Anich et al. [35]	Blockchain, SDN	Centralized, Distributed	Smart City	Security & Privacy	Ethereum Network
Ghandour et al. [32]	Blockchain	Decentralized, Distributed	Smart City	Security & Privacy	Hyperledger Fabric
Xu et al. [33]	Blockchain, Smart Contract	Decentralized, Distributed	IoT Networks	Security & Privacy	-
Sharma et al. [34]	SDN	, Centralized, Distributed	Edge Computing	Energy	-
Sharma et al. [36]	Blockchain, SDN	Centralized, Distributed	Smart City	Security & Privacy	Ethereum Network
Reyna et al. [37]	Blockchain, SDN	Decentralized, Distributed	IoT Networks	Security & Privacy	Ethereum & Hyperledger
Rahman et al. [38]	Blockchain, SDN	Centralized, Distributed	IoT Ecosystem	Security & Privacy	Ethereum Network
Rahman et al. [39]	Blockchain	Decentralized	IoT Ecosystem	Security & Privacy	Hyperledger Fabric
Sharma et al. [29]	Blockchain, SDN	Centralized, Distributed	IoT Networks	Security & Privacy	Ethereum Network
Novo et al. [40]	Blockchain	Centralized, Distributed	IoT Networks	Scalability	Ethereum Network
Gu et al. [41]	Blockchain	Decentralized, Distributed	Cloud Computing, IoT Networks	Security & Privacy	Ethereum & Hyperledger
Sharma et al. [42]	Blockchain	Distributed	Automotive Industry & Smart city	Security & Privacy	Ethereum

Table 3. Current Research Gaps: SDN & Blockchain Solution

Research Questions	Summary
Is the existing IoT network secured?	IoT networks are still suffering numerous security concerns including privacy, non-repudiation, authenticity, integrity, and confidentiality. In creating a sustainable IoT network, SDN & Blockchain can be an effective solution.
Can scalability issues in IoT be solved by SDN?	Programmable & centralized nature of the SDN can be the scalability solution of billions of IoT devices.
Can scalability issues in IoT be solved by Blockchain?	Widely Distributed peer to peer networking system of the Blockchain can be the solution to scalability problems for billions of IoT devices.
Can data integrity/reliability issues in IoT be solved by SDN & Blockchain?	Secure SDN controllers, consensus protocol & SC can be solution data integrity/reliability problems.
Can Blockchain solve central point failure/fault tolerance issues in IoT?	Decentralized nature of the Blockchain can be the solution of central point failure/fault tolerance.

3. Proposed Blockchain-SDN based Distributed Architecture

Taking the above problem into consideration, the authors propose a distributed Blockchain-SDN based architecture for smart city, as shown in Fig. 2, we consider the emerging technology such as IoT, SDN, and Blockchain to specify the smart cities. The proposed model consists of several layers, including the perception layer where the smart device provides data for users. Then, the edge layer produces a report on the data that is provided by the perception layer and also processing data efficiently. Furthermore, the cloud layer is used to store the desired data, also provide services securely by the Cloud Service Providers (CSPs). Furthermore, the SDN and Blockchain performances entirely depend on the performance of every layer successfully.

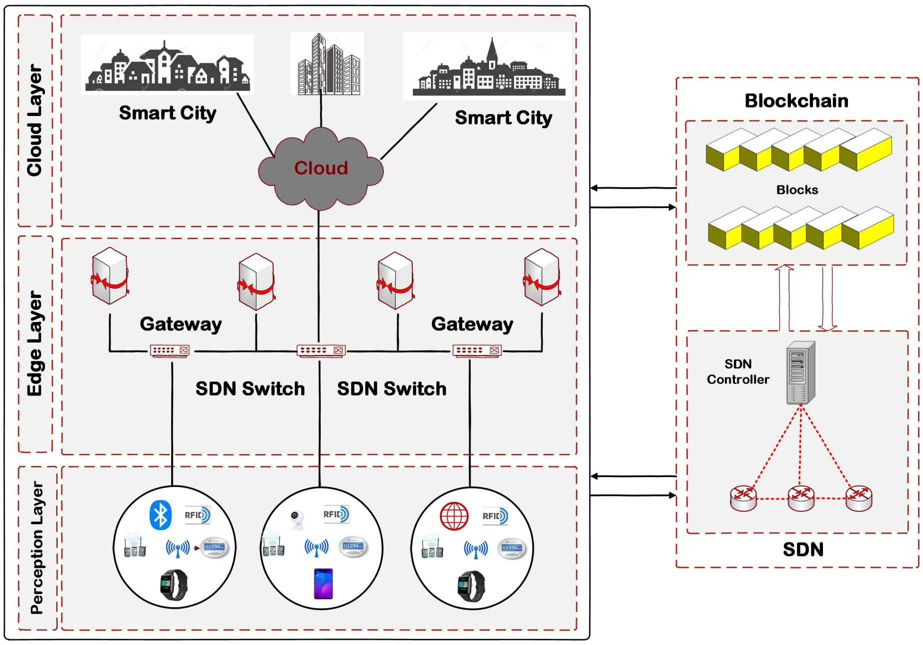

Figure 2. Proposed Architecture for Smart Cities

However, we separate various steps for explaining our proposed architecture. At first, we provide a energy efficient cluster head selection algorithm to select a cluster head (CH) with energy consumption in the perception layer environment, as shown in Fig. 4. In the SDN environment, the SDN has been organized into two convenience planes, such as the data plane and the control plane. In addition, we also present the SDN-IoT architecture for passing raw data through SDN-IoT standard gateway protocol data layer. Besides, we use the NFV that provides physical specification and decreases energy consumption effectively. Also, it comprises load balancing, conservation of energy and electronic network scale [30], [47]. Further, FloodLight is SDN controller that helps to forward the filtering data to the control layer in the SDN environment efficiently using OpenFlow based SDN routing protocol. In addition, controllers ensure that all data is filtered by the data layer of the SDN platform.

After that, we address Blockchain technology with a distributed ledger for accomplishing the transaction process one block to another through the communication channel. This process can be capable of providing security and privacy to the proposed architecture more confidentially. Most importantly, the block data is stored by the cloud layer conditionally. If the data is valid, then the data is placed into data centers accordingly, as depicted in Fig. 3. After completing the Blockchain transaction, cloud data is going through the desired applications, including the smart home, traffic, building, hospital, payment system, and so on.

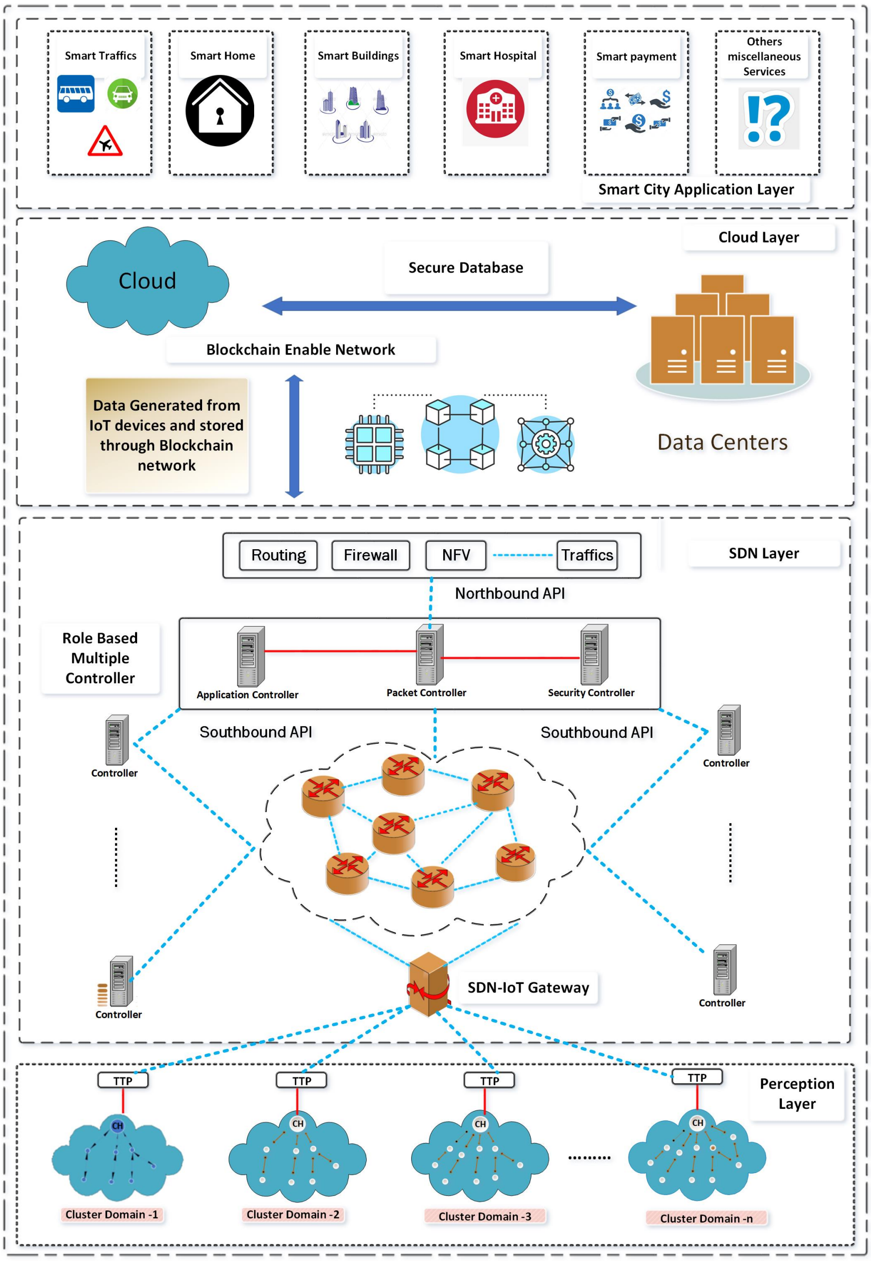

Figure 3. Edge Enable Service Architecture

3.1. *Energy Efficient Cluster Head Selection Method*

IoT devices can forward data with the help of common SDN gateways. Also, the dynamic SDN controller can filter the IoT data. Further, the proposed architecture provides security that helps to transmit the data to the cloud layer. But, it performs efficiently if the IoT devices can be able to select energy-efficient cluster heads. In this part, the authors have proposed an energy-efficient cluster head selection algorithm in this section, which is shown in Fig. 4.

3.1.1. **Cluster Head Selection**

Cluster heads selection one of the essential part of the proposed scheme. For increasing the network's lifetime, Cluster Heads (CHs) are evenly distributed among the system. At the beginning of the algorithm, sorting each node according to their energy values ((E_i^N)) and choosing the highest

Table 4. Notations of the CHS Method

Notations	Definition
n_i	Number of IoT devices
C_i	Clusters of the IoT devices
E_i^{res}	IoT devices residual energy
E_i^{th}	Threshold value of energy
ζ	Cluster Head
E_i^N	Sorted list o f nodes based on energy
D	Distance between the nodes
BS	Base Station
DBS	Distance from the Base Station
$NDBS$	Net Distance from the Base Station
C_i^{Emax}	Maximum energy of the clusters

energy node that is primarily considered as a CH among the cluster and other nodes are considered as the member of each cluster. After that, calculate the distance from one to the other nodes using *Euclidean Distance*. Also, computing the sum of the distance of all nodes from one node. Then, calculating the distance of all nodes from the Base Station (BS) and also calculates the net distance (NDBS) from the base station to all nodes. Then, compute the residual energy of the IoT devices based on the min(NDBS) and maximum energy C_i^{Emax} respectively. In addition, E_i^{res} indicates the residual energy, and E_i^{th} represents the threshold energy, which means that CH has considerably more energy to carry out its operation. Further, before going to sleep, each node transmits data to the CHS. Finally, data sent to the base stations after collecting the data by the CHs through a standard SDN gateway. Only can eligible CHs get permission for routing into an efficient path.

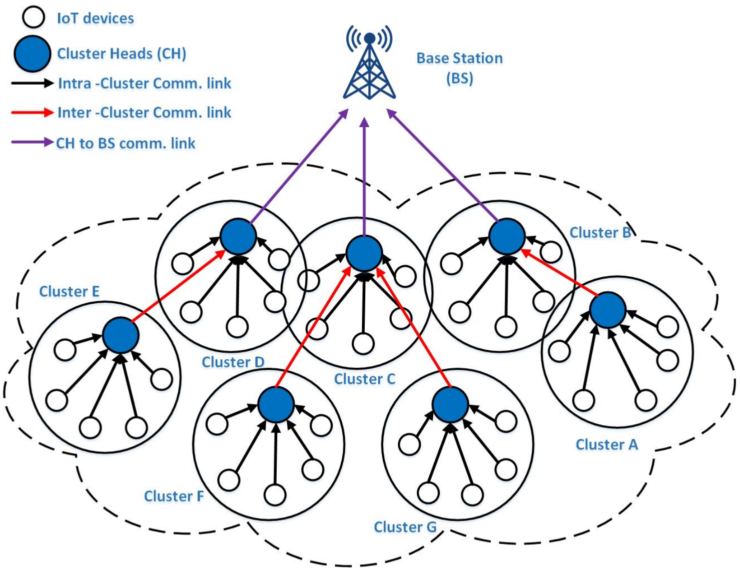

Figure 4. Clusters Head Selection Procedure

Table 5. Comparison of Proposed Algorithm with Existing Works

Works	IoT devices sorting with energy values	Euclidean Distance	Optimization	Energy Savings
Rahman et al. [26]	✓	×	×	✓
behera et al. [27]	×	×	✓	×
Aslam et al. [43]	×	×	✓	✓
Anich et al. [35]	✓	×	×	✓
Farman et al. [28]	×	✓	×	✓
Proposed	✓	✓	✓	✓

doi:10.20944/preprints202011.0552.v1

Algorithm 1: Proposed Energy Optimized Cluster Head Selection Algorithm

```
Require:
    • $N_i$ : Number of IoT devices
    • $C_i$ : Clusters of the IoT devices
    • $E_i^{res}$ : IoT devices residual energy
    • $E_i^{th}$ : Threshold value of energy
Ensure: Cluster Head selection $(\zeta)$
Initialize Cluster Head $\zeta \leftarrow 0$
while (1) do
    for $i \leftarrow 1$ to $N-1$ do
        $min = i$
        for $j \leftarrow i+1$ to $N$ do
            if $(E_j < E_{min})$ then
                $min = j$
            end
            $swap(E_j, E_{min})$
        end
        Compute sorted list of all IoT devices energy values $(E_i^N)$
    end
    return Sorted List of Nodes Based on Energy$(E_i^N)$
    for $i \leftarrow 1$ to $N$ do
        for $j \leftarrow 1$ to $N$ do
            $d_{ij} \leftarrow D(E_i^N)$
            $D_i \leftarrow D_i + d_{ij}$
        end
    end
    for $i \leftarrow 1$ to $N$ do
        $DBS_i \leftarrow D(BS_i, C_i)$
        $NDBS_i \leftarrow NDBS_i + D_i$
    end
    for $i \leftarrow 1$ to $N$ do
        $E_i^{res} \leftarrow [min(NDBS_i)$ && $(C_i^{Emax})]$
        Compute residual energy$(E_i^{res})$
        if $(E_i^{res} \geq E_i^{th})$ then
            $\zeta \leftarrow E_i^{res}$
        end
    end
    return Cluster Head $(\zeta)$
end
```

3.2. Enhancing security of the proposed architecture through Blockchain and SDN

We have heterogeneous IoT devices that ability to exchange information, execute transactions but need to be secure communication. Therefore, a secure data transmission method needs to be present, shown in Fig. 5. Blockchain and SDN can provide secure data transmission in the overall networking system. Where the SDN controller provides security and network services to IoT devices. Also, discards the malicious packets from the SDN domain. Moreover, enhancing the safety and decreasing the energy consumption of the IoT devices. In addition, Blockchain provides security,

doi:10.20944/preprints202011.0552.v1

privacy, confidentiality, integrity, etc. The distributed and decentralized architecture of Blockchain ensures the security of billions of IoT devices. Moreover, the security mechanism is presented in the flowchart, as depicted in Fig. 6. In flowchart, IoT devices request for SDN controller, then devices are registered in the SDN controller, and an IP address for each IoT device is allocated. Even, all IoT device operational activities & transactions are monitored for security purposes in the SDN controller. Furthermore, IoT devices are blocked by the SDN controller if any malicious behavior is found. Then, IoT devices IP addresses are registered in public Blockchain networks to prevent them from registering in other clusters.

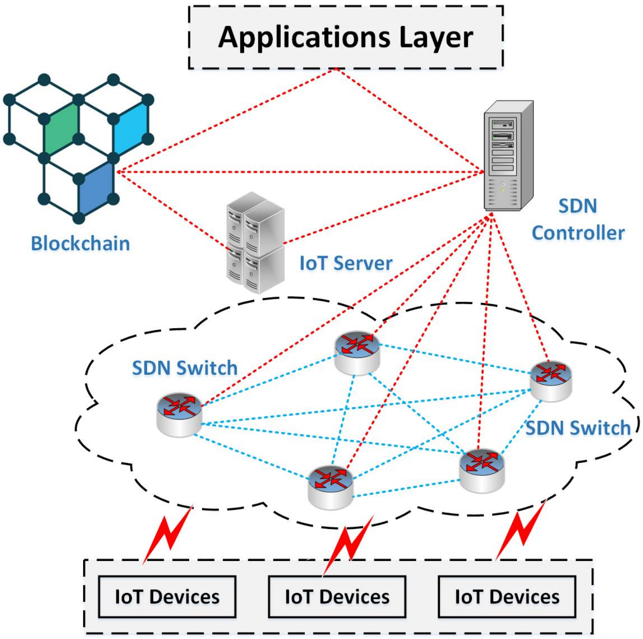

Figure 5. Secure Data Transmission through Blockchain and SDN Domain

3.3. The role of Network Function Virtualization (NFV) into SDN-IoT System

Networking devices can offer users different types of services. Every user always expects the networking devices to provide secure data. The authors have presented SDN-IoT architecture with NFV in this section from that expectation. In architecture, Network Function Virtualization Infrastructure (NFVI) provides the SDN-IoT infrastructure virtualization facilities, as shown in Fig. 7. Also, an SDN has effectively organized [48] as two distinct planes, such as a data plane and control plane with SDN multiple controllers.

Besides, the data layer receives data from the clustering domains; also, SDN-IoT standard gateway protocol can manage the smart devices data efficiently. After that, the control layer provides some SDN controllers such as security, application, packet, key, intrusion, and crypto controller. The security controller, which aims to perform all security issues for a desirable model. Again, the packet controller provides the networking packet management strategy into the network, and other controllers perform their operation in a particular way for the presented architecture. Finally, In the NFVI environment, the control plane also conveys the different virtual services like virtual storage, virtual networking as well as virtual computing [3].

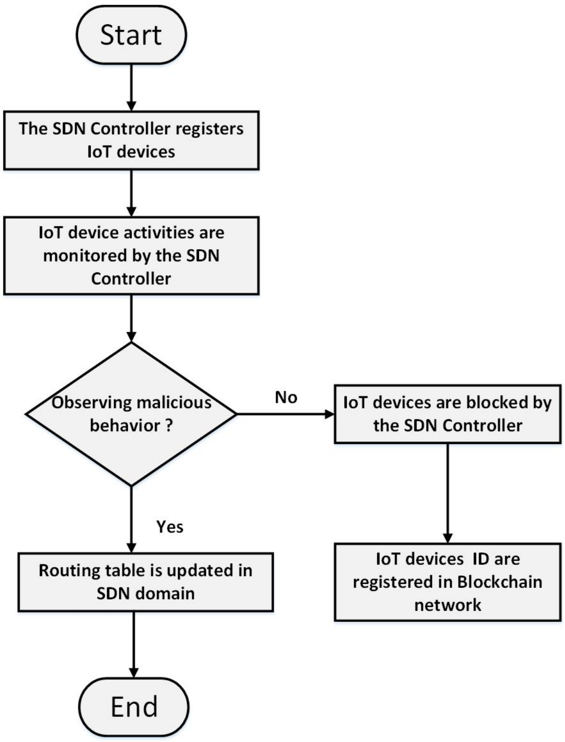
Start
The SDN Controller registers IoT devices
IoT device activities are monitored by the SDN Controller
Observing malicious behavior ?
No
IoT devices are blocked by the SDN Controller
IoT devices ID are registered in Blockchain network
Yes
Routing table is updated in SDN domain
End

Figure 6. Security Mechanisms Flowchart

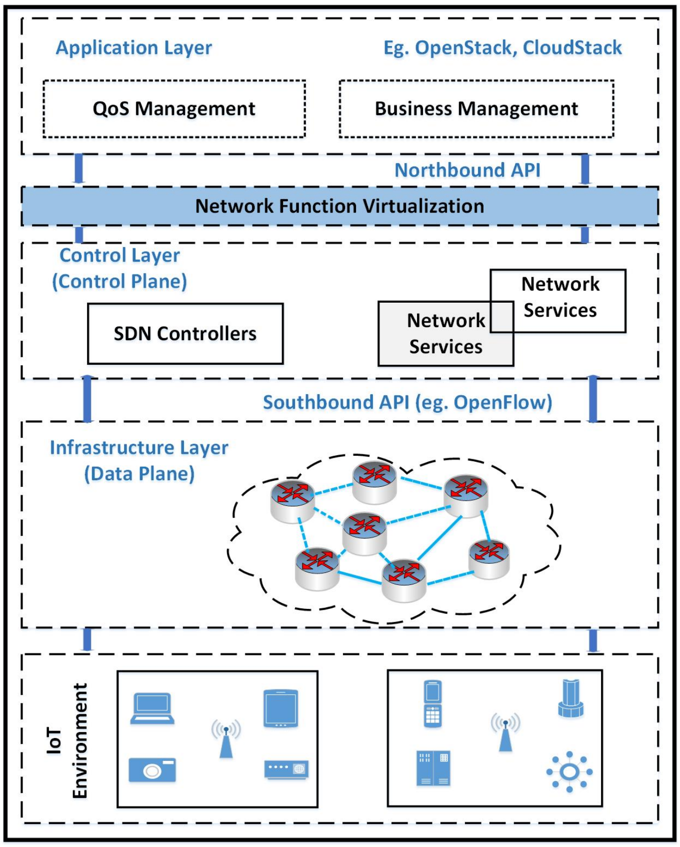
Application Layer
Eg. OpenStack, CloudStack
QoS Management
Business Management
Northbound API
Network Function Virtualization
Control Layer (Control Plane)
SDN Controllers
Network Services
Network Services
Southbound API (eg. OpenFlow)
Infrastructure Layer (Data Plane)
IoT Environment

Figure 7. SDN-IoT on NFV Architecture [30].

3.4. Distributed Blockchain Procedure for Smart City

IoT ecosystem supplies integrity, availability, confidentiality, authentication, a non-repudiation & access control through Blockchain Technology [49]. Also, Blockchain contains some key components such as decentralization, transparency, autonomy, immutable, anonymity, as well as the open-source system. We have presented an SDN-IoT based model with NFV using a distributed Blockchain approach. This distributed Blockchain is utilizing the distributed multiple controllers. Blockchain is a decentralized grouped ledger with no authorization or no individual control the ledger. Every striving leads or confirmed the ledger. Miners verify the latest activities and so placing all of them inside the global ledger. Usually, every 5 to 10 minutes a block is surely extricated—Miners attempt to create a terrifying statistical perplexity based on a cryptographic hash algorithm. The found solution is called the Proof-of-Work (PoW). Appended to the arrangement is the newly mined block. When creating the particular block by the miners, it proceeds to add to the several BC. After adding a block in the BC, it is stimulating to work in remodeling data through the block chiefly because it requires turning all of the subsequent blocks. As well as, any particular block which will get matched to the BC, the part requires consensus in any the vast preponderance nodes from the various networks.

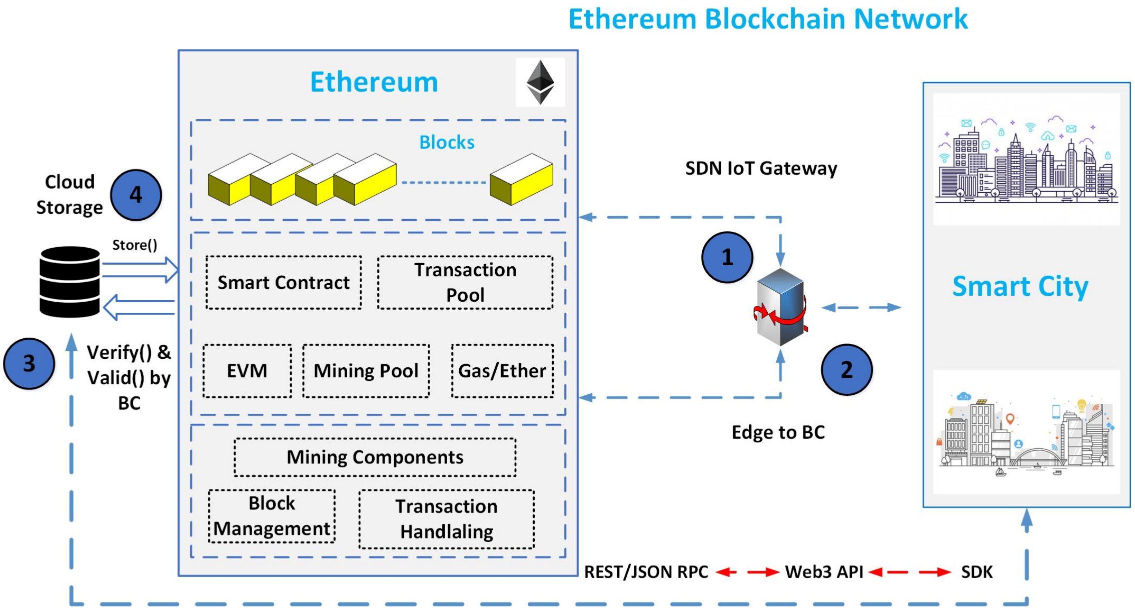

Figure 8. Distributed Blockchain Approach for Smart Cities

After that, we have addressed the decentralized Ethereum Blockchain network approach in a wide tremendous networking systems, which is shown in Fig. 8. This architecture allows the transmission of data from the IoT devices to the SDN Gateways. Then, the information is stored in the database and sent to the Smart city for further decision. But before making any changes to the storage, the transaction are validated by the Smart Contract following some mining procedures under the Ethereum Blockchain Network system. Ethereum will store the data into the cloud storage after the verification and stores the indices by means of blocks. Through the REST or JSON RPC following some other API and SDK which will help to run the Smart Contracts to verify and validate the data request information, Smart City will be able to interact with the cloud storage.

3.5. Smart City on Cloud Application

Approachability, usability, data safety & security have been provided by a smart city. These cities can be capable of utilizing smart education, energy, health, farming, environment, home, hospital, transport, and building, etc [26]. Our presented model can be capable of controlling several smart pieces of equipment like a smart door, window, light, fan, AC as well as smart phone by using

Blockchain with SDN-IoT gateway. When any request of access is captured which is unauthorized, it is inhibited by the Firewall. The information is preserved into the cloud to make the data availability easier. Smart transport decreases vehicle traffic collision. Furthermore, intelligent fans, light can save the electricity and in the smart home, including stylish door & window can protect our home from intruder suitably. In a similar way, a smart city application has been improved our lifestyle. Besides, IoT enabled devices are the key components for a smart city model. Finally, the main goal of a smart city on a cloud storage are fashionable civilization, society, governance as well as smart technology [50].

4. Evaluation Results and Analysis

4.1. Simulation Environment setup

To assess the efficiency of the proposed model simulation parameters are shown in Table 6 with their corresponding values. Where author has used network emulator (Mininet 2.2.1) for topology setup. Among the general parameters, Wireshark is used for the packet analyzer. In SDN platform, there are 6 Floodlights SDN controllers and 5 OpenFlow based switches are used through a couple of Gateways. Moreover, Ethereum as a Blockchain platfrom with dynamic number of transactions is used where block size is 4 bytes. Some other parameters are also highlighted in the table including no. of IoT devices, devices speed, data rate, packet sizes, energy & trust values of IoT devices. Moreover, we have used Ubuntu 16.04 LTS(Linux) OS, Intel(R) Core(TM)-i5-10210U CPU @ 160GHz-2.11GHz, 8.00GB RAM, 1TB ROM, and 512GB SSD for getting the expected results.

Table 6. Simulation Environment

	Parameters Name	**Values**
General Parameters	Packet Analyzer	Wireshark
	Mobility Model	Random Waypoint Model
	Traffic Type	Constant Bit Rate (CBR)
	Type of Antenna	Antenna/Omni Antenna
	MAC Protocol	Mac/802.11
	Cloud storage platform	OpenStack
SDN Parameters	No. of SDN Controllers	6
	OpenFlow switches	5
	Gateways	2
	Types of SDN Controllers	FloodLight
	SDN Routing Protocol	OpenFlow
Blockchain Parameters	Blockchain platform	Ethereum
	Number of transactions	Variable
	Block size	4 bytes
	Block header	80 bytes
	Proof type	Proof of Work (PoW)
Others Parameters	Simulation Area	3000m X 3000m
	Number of IoT devices	100
	IoT devices speed	10 m/s
	Simulation Times	400s
	Data Rate	12 Mbps
	Initial Energy Values of IoT devices	12-15 j
	Initial Trust value	5 j
	Node Transmit Packet Size	512-1024 bytes

4.2. Throughput

We have evaluated the throughput (i.e., network throughput relates to how many transaction requests can be transmitted from origin to destination within a reasonable period) of the proposed model, as shown in Fig. 9. However, we have observed that the throughput starts from 100 transaction requests for each of the systems such as core, DistArch-SCNet, and proposed model efficiently.

When the number of requests is 400, all model performances are almost the same. Furthermore, when the number of transaction requests is reached at 1200, the proposed architecture shows much more throughput than the core model. For 2400 requests proposed model shows higher throughput compared to the existing model. In addition, with increasing the number of requests, throughput also increases and the proposed system much better performance than DistArch-SCNet and Core model in the network.

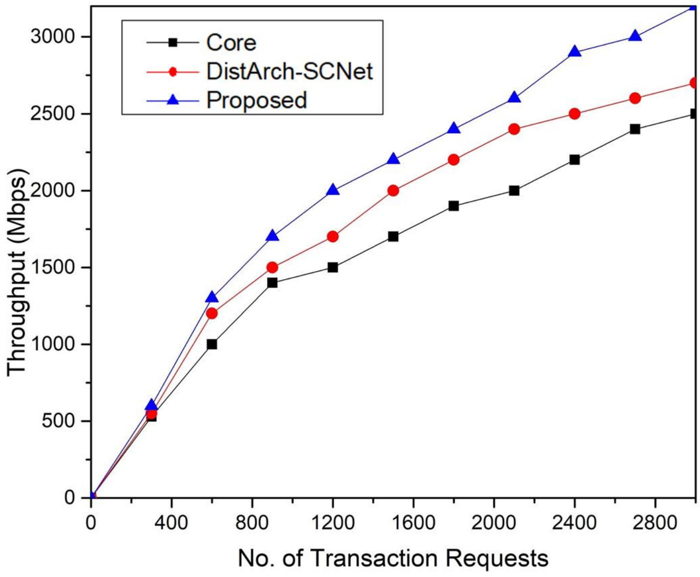

Figure 9. Throughput with Respect to the Number of Transaction Requests

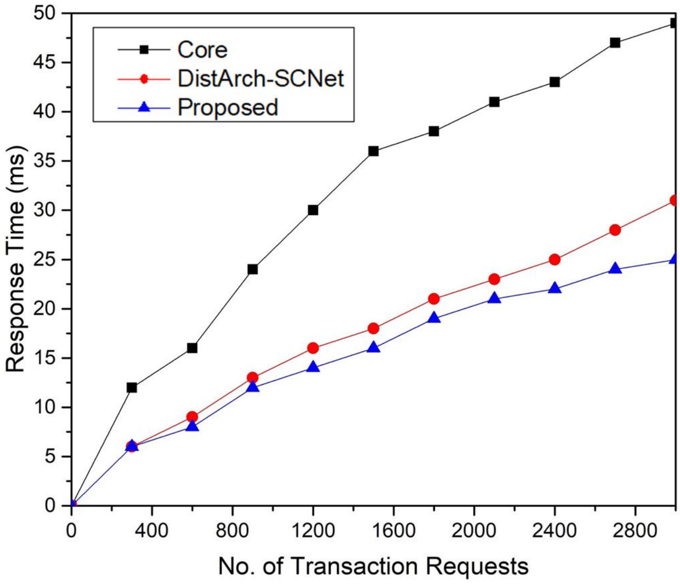

Figure 10. Response Time with Respect to the Number of Transaction Requests

4.3. Response Time

The time duration needed to get the very first reply from the system is cited as response time. It is more beneficial to have lower latent period comparing to the existing scheme. The response time of the proposed model is presented in Fig. 10 which also draws the superiority of this system over the core model and DistArch-SCNet. At the beginning, when the number of transactions is about 400, DistArch-SCNet and proposed model take same period of time to respond, but the core model starts to show higher response time from the starting point. It's clearly noticed that the core model needs considerably more time to reply with the action of a request with the increasing number of transactions. If the requests are limited to 1200 approximately, the proposed model and DistArch-SCNet show almost same performance, but if the amount of requests raises over 1200, the proposed model responds with a shorter time equating to the SCNet. With increasing the transaction requests(Over 1600 requests) Core model performance worst than other model where DistArch-SCNet and proposed architecture performs around similarly in the network.

4.4. Gas Consumption

Fig. 11 shows the no. of transactions request with respect to the time(ms) and gas consumption. Gas consumption is the price that must be paid for valid transaction of the minor nodes. At the beginning of the small no. of transactions, the gas consumption is not so high. After that as the no. of transactions increases, the gas consumption increases linearly with the time. However, the cost of the transactions is necessary to illustrate in the proposed model. The experimental result shows how the gas consumption varied in terms of time(ms) when the no. of transaction changes.

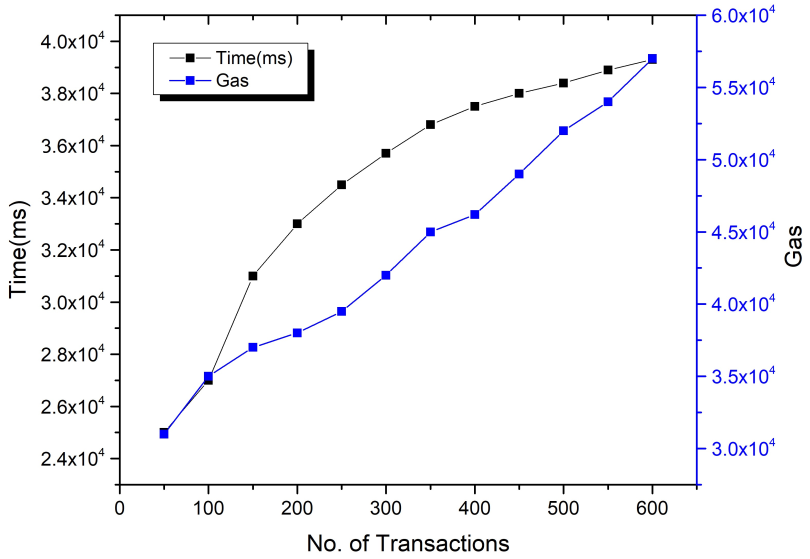

Figure 11. Gas Consumption with Respect to the Time(ms) and Number of Transactions

4.5. Communication Overhead

We analyzed the communication overhead comparisons are shown in Fig. 12. For less no. of nodes(10) core, proposed, and DistArch-SCNet model communication overhead is almost similar. Moreover, for 30 nodes, both proposed model and DistArch-SCNet are still perform identically. However, with increasing the number of nodes, overhead is also progressing. Further, it is clearly shown that proposed architecture better performance shows a linear way compared to

doi:10.20944/preprints202011.0552.v1

the DistArch-SCNet and core model. After comparing the overhead communication comparisons effectively in the presented system model based on the proposed and DistArch-SCNet scheme, we clearly identified that our proposed model shows better performances compare with the DistArch-SCNet system.

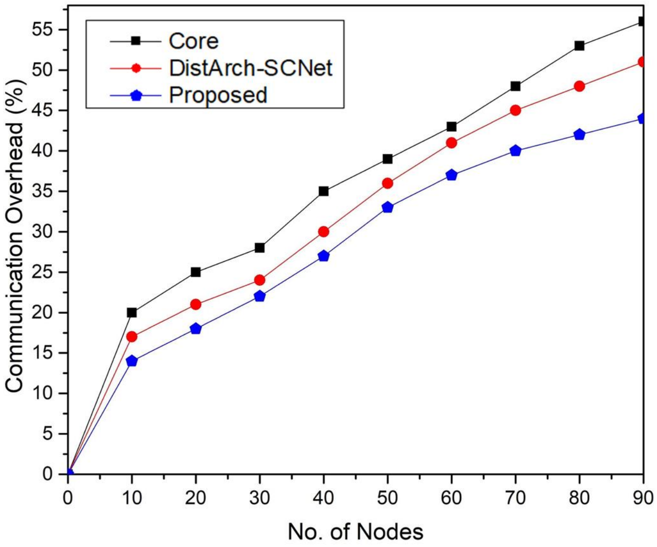

Figure 12. Communication Overhead(%) Comparisons with Respect to the No. of IoT Devices

4.6. CPU Utilization during DDoS Attack

Now, for analyzing CPU utilization, we have applied the DDoS attacks in our projected environment during various application are running continuously.

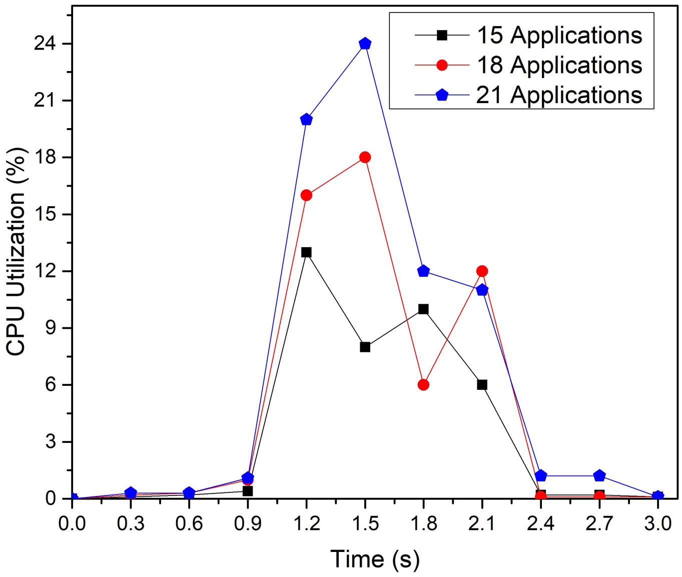

Figure 13. CPU Utilization Scenario during DDoS Attack

We utilized a learning method for recording CPU utilization during a DDoS attack. Fig. 13 shows average output of the CPU utilization in different applications based on prop scheme, when DDoS attacks are performed. This attack started at 0.9s of the simulation, with increasing the time, the attack rate also climbs up. In continuing the attack after a certain period of time (1.5s), we have noticed that DistB-SDIoT provides adequate protection against this attack efficiently and the CPU can get back into the stable situation after a fluctuation. The vulnerability of CPU utilization lasts for a short period and depends on the number of applications opened at that moment. Moreover, our presented system enhances the performances of different application, safe from other numerous attacks as well.

5. Conclusion

Blockchain and SDN technologies are yet unfledged in recent research, and it's all services and performances that are in the growing as yet. These fields have a lot of challenges, risks, and threats. Moreover, a few numbers of researchers have addressed these threats and try to overcome these challenges. To overcome these problems, the author presents a Blockchain-SDN based distributed model for smart cities with NFV. Also, the author introduces an energy-optimized cluster head selection algorithm to select a cluster head in an efficient procedure. Moreover, the SDN controller monitors and manages the activities of the IoT devices; Blockchain are used to detect & reduce the cyber-attacks in the IoT networks. Finally, the experimental result shows that the proposed architecture performs better compared to the existing architecture (Core and DistArch-SCNet) in terms of throughput, response time, gas consumption, communication overhead, which notably increases the throughput and reduces the response time, overhead, and gas consumption. Though we have considered various parameters nevertheless there are several limitations still remain. The author does not consider the end to end delay, network bandwidth, other network vulnerabilities, and various passive & active attacks (including Flooding attack, Sybil attack, MITM, and etc.). In the future, we intend to develop an energy-efficient edge computing model with the help of SDN, NFV and Blockchain technology taking such ongoing problems into consideration.

References

1. P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: A distributed Blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.
2. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 27 11 2016.
3. B. K. Mukherjee, M. S. I. Pappu, M. J. Islam, and U. K. Acharjee, "An SDN based Distributed IoT Network with NFV Implementation for Smart Cities," *In progress: 2nd International Conference on Cyber Security and Computer Science (ICONCS-2020)*, Springer, 2020.
4. T. M. FERNNDEZ-CARAMES and F.-L. PAULA, "A review on the use of Blockchain for the internet of things," *Open Access Journal*, vol. 86, May 2018.
5. G. Yao, J. Bi, and L. Guo, "On the cascading failures of multi-controllers in software defined networks," *in 2013 21st IEEE International Conference on Network Protocols (ICNP)*, pp. 1–2, Oct 2013.
6. Ghafoor, Huma and Koo, Insoo An Integrated Cognitive Radio Network for Coastal Smart Cities, Applied Sciences, volume 9, number 17, pages 3557, year 2019, Multidisciplinary Digital Publishing Institute.
7. M. Ojo, D. Adami, and S. Giordano, "A sdn-iot architecture with nfv implementation," in *Globecom Workshops (GC Wkshps), 2016 IEEE*. IEEE, 2016, pp. 1–6.
8. P. K. Sharma, S. Park, Singh, Y.-S. Jeong, and J. Hyuk Park, "Distblocknet: A distributed Blockchains-based secure sdn architecture for iot networks," *Advances in network services chain, IEEE Communications Magazine*, September 2017.
9. B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.
10. D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 269–283, 2017.

11. Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.
12. T. K. Hui, R. S. Sherratt, and D. D. Sánchez, "Major requirements for building smart homes in smart cities based on internet of things technologies," *Future Generation Computer Systems*, vol. 76, pp. 358–369, 2017.
13. A. Kumar *et al.*, "Energy efficient clustering algorithm for wireless sensor network," Ph.D. dissertation, Lovely Professional University, 2017.
14. K. J. C. Angel and E. G. D. P. Raj, "Eeeca: Enhanced energy efficient clustering algorithm for mobile wireless sensor networks," in *2017 World Congress on Computing and Communication Technologies (WCCCT)*. IEEE, 2017, pp. 267–270.
15. A. Al-Baz and A. El-Sayed, "A new algorithm for cluster head selection in leach protocol for wireless sensor networks," *International journal of communication systems*, vol. 31, no. 1, p. e3407, 2018.
16. L. Zhao, S. Qu, and Y. Yi, "A modified cluster-head selection algorithm in wireless sensor networks based on leach," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 287, 2018.
17. K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Communications Magazine*, no. 99, pp. 1–7, 2017.
18. R. Kirichek, A. Vladyko, M. Zakharov, and A. Koucheryavy, "Model networks for internet of things and sdn," in *Advanced Communication Technology (ICACT), 2016 18th International Conference on*. IEEE, 2016, pp. 76–79.
19. P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for iot devices using an sdn gateway," in *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE, 2016, pp. 157–163.
20. S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network (sdn) based internet of things (iot): A road ahead," in *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, 2017, p. 10.
21. O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in *Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on*. IEEE, 2015, pp. 688–693.
22. C. Vandana, "Security improvement in iot based on software defined networking (sdn)," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 5, no. 1, pp. 2327–4662, 2016.
23. Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "Sdn-based data transfer security for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 257–268, 2017.
24. S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black sdn for the internet of things," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*. IEEE, 2015, pp. 190–198.
25. R. Muñoz, L. Nadal, R. Casellas, M. S. Moreolo, R. Vilalta, J. M. Fàbrega, R. Martínez, A. Mayoral, and F. J. Vílchez, "The adrenaline testbed: An sdn/nfv packet/optical transport network and edge/core cloud platform for end-to-end 5g and iot services," in *2017 European Conference on Networks and Communications (EuCNC)*. IEEE, 2017, pp. 1–5.
26. A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "DistBlockSDN: A Distributed Secure Blockchain based SDN-IoT Architecture with NFV Implementation for Smart Cities," *In Progress: International Conference on Innovation in Engineering and Technology (ICIET)*, vol. 23, p. 24, IEEE, 2019.
27. T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "Residual energy-based cluster-head selection in wsns for iot application," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132–5139, 2019.
28. H. Farman, B. Jan, H. Javed, N. Ahmad, J. Iqbal, M. Arshad, and S. Ali, "Multi-criteria based zone head selection in internet of things based wireless sensor networks," *Future Generation Computer Systems*, vol. 87, pp. 364–371, 2018.
29. 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, 2017.
30. M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, "Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 2019, pp. 1–6.
31. P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, p. 61, 2020.

doi:10.20944/preprints202011.0552.v1

32. A. G. Ghandour, M. Elhoseny, and A. E. Hassanien, “Blockchains for smart cities: a survey,” in *Security in Smart Cities: Models, Applications, and Challenges*. Springer, 2019, pp. 193–210.
33. Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, “A blockchain-based storage system for data analytics in the internet of things,” in *New Advances in the Internet of Things*. Springer, 2018, pp. 119–138.
34. P. K. Sharma, S. Rathore, Y.-S. Jeong, and J. H. Park, “Softedgenet: Sdn based energy-efficient distributed network architecture for edge computing,” *IEEE Communications magazine*, vol. 56, no. 12, pp. 104–111, 2018.
35. A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, “Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management,” *IEEE Access*, vol. 8, pp. 140 008–140 018, 2020.
36. P. K. Sharma and J. H. Park, “Blockchain based hybrid network architecture for the smart city,” *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.
37. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with iot. challenges and opportunities,” *Future generation computer systems*, vol. 88, pp. 173–190, 2018.
38. A. Rahman, U. Sara, D. Kundu, S. Islam, M. J. Islam, M. Hasan, Z. Rahman, and M. K. Nasir, “Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, 2020.
39. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, “Trust chain: Establishing trust in the iot-based applications ecosystem using blockchain,” *IEEE Cloud computing*, vol. 5, no. 4, pp. 12–23, 2018.
40. O. Novo, “Blockchain meets iot: An architecture for scalable access management in iot,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
41. Y. Gu, D. Hou, X. Wu, J. Tao, and Y. Zhang, “Decentralized transaction mechanism based on smart contract in distributed data storage,” *Information*, vol. 9, no. 11, p. 286, 2018.
42. P. K. Sharma, N. Kumar, and J. H. Park, “Blockchain-based distributed framework for automotive industry in a smart city,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4197–4205, 2018.
43. S. Aslam, N. U. Hasan, J. W. Jang, and K.-G. Lee, “Optimized energy harvesting, cluster-head selection and channel allocation for iots in smart cities,” *Sensors*, vol. 16, no. 12, p. 2046, 2016.
44. I. P. C. Tselios and S. Kotsopoulos, “Enhancing sdn security for iot-related deployments through Blockchain,” *Third International Workshop on Security in NFV-SDN*, December 2017.
45. L. Siva Sankar, S. M., and M. Sethumadhavan, “Survey of consensus protocols on Blockchain applications,” *International Conference on Advanced Computing and Communication Systems*, August 2017.
46. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” *2ND IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things*, 2017.
47. Y. Li and M. Chen, “Software-defined network function virtualization: A survey,” *IEEE Access*, vol. 3, pp. 2542–2553, 2015.
48. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “Openflow: enabling innovation in campus networks,” *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.
49. S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, “Blockchain for iot security and management: Current prospects, challenges and future directions,” in *2018 5th International Conference on Networking, Systems and Security (NSysS)*. IEEE, 2018, pp. 1–9.
50. H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, and P. Siano, “Iot-based smart cities: a survey,” in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*. IEEE, 2016, pp. 1–6.