An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security

Abbas Yazdinejad, Reza M. Parizi, *Senior Member, IEEE*, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

Abstract—Internet of Things (IoT) is a disruptive technology in many aspects of our society, ranging from communications to financial transactions to national security (e.g., Internet of Battlefield / Military Things), and so on. There are long-standing challenges in IoT, such as security, comparability, energy consumption, and heterogeneity of devices. Security and energy aspects play important roles in data transmission across IoT and edge networks, due to limited energy and computing (e.g., processing and storage) resources of networked devices. Whether malicious or accidental, interference with data in an IoT network potentially has real-world consequences. In this article, we explore the potential of integrating blockchain and software-defined networking (SDN) in mitigating some of the challenges. Specifically, we propose a secure and energy-efficient blockchain-enabled architecture of SDN controllers for IoT networks using a cluster structure with a new routing protocol. The architecture uses public and private blockchains for Peer to Peer (P2P) communication between IoT devices and SDN controllers, which eliminates Proof-of-Work (POW), as well as using an efficient authentication method with the distributed trust, making the blockchain suitable for resource-constrained IoT devices. The experimental results indicate that the routing protocol based on the cluster structure has higher throughput, lower delay, and lower energy consumption than EESCFD, SMSN, AODV, AOMDV, and DSDV routing protocols. In other words, our proposed architecture is demonstrated to outperform classic blockchain.

Index Terms—Internet of Things, energy efficiency, security, blockchain, proof of work, software defined networks, SDN

1 Introduction

With the advancement of the Internet and the underpinning technologies such as the Internet of Things (IoT) and blockchain, we have observed the emergence of new trends such as smart city and smart nation. The form of presentation and receipt of informational services (e.g., e-Learning, e-Governance, e-business and e-service marketing), for example, have also changed due to the requirements of these technologies. With the rapid growth of IoT, which is predicted to increase by about 20 to 50 billion worth of industry by 2020, IoT continues to affect all areas of human life, including communications [1], [2]. However, IoT faces challenges, such as those associated with the lack of a central controller, heterogeneity of devices, multiple attacks, and comparability [3].

Security and energy consumption are among the most pressing challenges in the IoT domain [4]. For example, IoT devices have limitations due to heterogeneity in energy resources and processing, and therefore this result in potential bottlenecks in communication and implementation of security solutions [3], [5]. Recently, fog (edge) computing has been shown to be a viable architecture to address some of the challenges associated with IoT resource limitations [6]. There are, however, unresolved security issues. [7], including IoT-specific issues. In fact, new solutions with features such as confidentiality, availability, and high security along with energy efficiency for IoT devices in communication with each other are required [8]. Confidentiality ensures only authorized users can access the messages. Integrity and binding relevant parties to a transaction ensure that the message is sent to the destination, and any modification can be detected [3]. Availability ensures that any data service is available at any time it is needed, while considering consumed energy among heterogeneous devices, as IoT devices are mostly low-energy and have low computing capability. Minimizing energy consumption, without affecting performance and security, is also an important consideration for data transmission in an IoT network [9], [10]. This necessitates the design of a new architecture for IoT networks.

In general, to balance the need for security and minimizing energy consumption for IoT in physical layers, network layers, and applications running on the IoT, we need to provide an architecture with the required capabilities [11]. Thus, we explore the potential of software-defined networking (SDN) and blockchain to implement such an architecture [12].

SDN is a new architecture of the network in which the control plane is separated from the data plane, and has two main elements, namely: *controller* and *switch*. The switch is tasked with packet forwarding, and the controller implements policies, management, and programmability of specific network

- *A. Yazdinejad and A. Dehghantanha are with the Cyber Science Lab, School of Computer Science, University of Guelph, Guelph, ON N1G 2W1, Canada. E-mail: abbas@cyberssciencelab.org, adehghan@uoguelph.ca.*
- *R.M. Parizi is with the Department of Software Engineering and Game Development, Kennesaw State University, Kennesaw, GA 30060. E-mail: rparizi1@kennesaw.edu.*
- *Q. Zhang is with the IBM Thomas J. Research Center, Yorktown Heights, NY 10598. E-mail: q.zhang@ibm.com.*
- *K.-K.R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249. E-mail: raymond.choo@fulbrightmail.org.*

Manuscript received 18 Dec. 2018; revised 28 Dec. 2019; accepted 12 Jan. 2020. Date of publication 15 Jan. 2020; date of current version 10 Aug. 2020. (Corresponding author: Kim-Kwang Raymond Choo.) Digital Object Identifier no. 10.1109/TSC.2020.2966970

switches through a protocol such as OpenFlow [13]. The SDN controller can bring full control over the network, communication and remote control, intelligent management, high flexibility and programmability. Moreover, the SDN controller provides the ability to implement centralized and secure network services such as security, routing, energy consumption, and bandwidth management, and can prevent unauthorized access to network resources [13], [14], [15]. SDN boasts easy management and network programmability issues for the management of millions of new IoT devices are being sold every day. SDN functions can be combined with the IoT to enhance network performance. Besides, the dynamic nature of IoT devices results in network configuration changes, which can be monitored and managed through the SDN controller [16]. The lack of a central controller is one of the major issues in the IoT network, which can be achieved by using the SDN controller to provide a centralized controller for communication with the IoT devices [17]. One of the major concerns today in SDN is how to improve its security. File transfer in SDN can be more secure, for example by utilizing blockchain [18], [19]. The security-by-design nature of blockchain can be utilized across the SDN network because it protects the privacy and resource availability against untrusted users about the energy efficiency approach of the IoT devices [17].

Blockchain underpins Bitcoin's transactions verification [20]. Beyond financial transactions, blockchain has been employed to create intelligent accounting offices, medical information collection, e-government, and distributed cloud storage [20], [21], [22]. It consists of a chain of blocks that contains specific information and uses distributed and flexible peer-to-peer network management instead of centralized management. The connection is possible in a completely secure state without the need for an intermediary [12], [20], [23], [24], [25]. With the capability of blockchain, we address the challenges and limitations of the IoT using the SDN controller capabilities for creating a secure and energy-efficient architecture. The P2P's nature of this technology is to protect the security, privacy, stability, reliability, and solution of the single point of failure (SPOF) problems [25].

The idea of incorporating blockchain and SDN in the IoT network could be very useful and applicable due to their unique capabilities. Inspired by this, we propose a new blockchain-enabled architecture for SDN controllers in IoT networks. The proposed architecture by blockchain layer allows a distributed P2P network where, without a trusted intermediary, untrusted individuals can interact in a verifiable manner with each other in each cluster (SDN domain). This facilitates secure interaction between IoT devices in each SDN domain. It is, however, acknowledged that blockchains (especially those with Proof of Work (POW) consensus protocols) could complicate the computation aspects, including bandwidth overhead and delay; thus, may not be suitable for IoT devices. To overcome this issue, our proposed architecture provides a customized and IoT-friendly blockchain, which effectively eliminates the traditional blockchain's overheads via an efficient authentication method (presented in Algorithm 1) with distributed trust by the SDN controller in each cluster. More specifically, IoT devices use a non-changeable private distribution ledger in each cluster that is centrally managed by the SDN controller. To optimize POW, the entry of selfish nodes is prevented, and proper routing protocol in the SDN controller is used in the proposed architecture for IoT devices. We have used a cluster structure to optimize energy consumption and enhance security.

1.1 Goals of the Study

The focus of this research is to provide a new blockchain-enabled architecture for SDN controllers in IoT networks. The specific objectives are as follows:

- Provide a cluster architecture using blockchain-based SDN controllers with distributed network management for IoT devices.
- Devise and utilize IoT-compatible (computational and energy-wise) public and private blockchains in the proposed architecture. Both public and private blockchains are employed for providing P2P communication and secure access control to IoT devices and their associated data.
- Provide a secure and energy-efficient mechanism for file transferring between IoT devices in an SDN domain via a new routing protocol suited for the cluster structure and to circumvent computational limitations of IoT devices.

1.2 Paper Organization

The rest of this paper is organized as follows: Section 2 presents the extant literature. In Section 3, we introduce the proposed architecture and its inner workings including file transfer process between IoT devices, and security and energy efficiency improvement mechanisms. In Section 4, we present the results using both simulation and analytical evaluation on the performance and the efficiency of the architecture and its routing protocol and, finally, the last section reports the conclusions and future work.

2 Related Work

In this section, we review related research studies that focused on the integration of IoT with SDN and blockchain.

The rapid growth of IoT has created new communication interfaces to which traditional distributed architectures, protocols, and techniques may not be sufficient to address unprecedented challenges of the IoT domain, particularly those related to security and energy [25], [26]. Recently, blockchain and SDN have attracted researchers and practitioners attention to provide solutions for current challenges and limitations in IoT space [25], [26].

DistBlockNet [27] is a model of IoT architecture that uses a blockchain to confirm the security of the Flow Rules Tables and distribute them among IoT devices. This architecture is based on the principles of distributed features in SDN for generating a plan based on principles of security and comparability in the IoT network. It benefits from the ability to automatically isolate threats by updating the flow rules tables using blockchain. This architecture does not however take into account the amount of energy consumed by IoT devices and their resource limitations. Moreover, energy consumption issues, in turn, could raise security challenges in the architecture.

In another work [12], Blockchain Security over SDN (BSS) implements a security strategy on SDN. In fact, it delivers file transfer to the SDN securely by means of blockchain. The use of the Ethereum platform and the opendaylight controller integrated with the openstack controller in this work indicates that files can be securely shared among SDN users based on distributed P2P. This approach has not been evaluated according to the IoT specification, as it merely addresses the issue of secure transmission, and the areas of comparability without considering the limitations of resources and energy used.

The authors in [26] optimized a blockchain-based solution for IoT devices in smart home. Their proposed lightweight architecture eliminates classical blockchain's overheads. Architecture provided by the distributed trust was used to reduce the processing time of authentication. However, the proposed architecture does not take into account the comparability and energy resources constraints of IoT devices. The lack of routing in its hierarchical structure among IoT devices can also further lead to security problems and more energy consumption. Similar to this work, Dorri *et al.* [3] proposed a blockchain-based architecture for IoT users that describes the architecture of the example of a smart home. It uses two types of public and local blockchains for communication and uses a blockchain-based authentication mechanism. In their evaluation, the Cooja simulator was used, and compared with the BC-based approach. Their results demonstrated that there was a decrease in overhead and delay due to clustering of nodes in a network overlay. They do not consider investigating the applications of framework to other IoT domains, also their work does not take into account the significant challenges and aspects of IoT, energy consumption and availability.

In [28], a distributed cloud architecture of a classical blockchain was provided, where the fog node located on the edge of the network consists of distributed SDN controllers in the network. Their architecture consists of three layers of cloud, fog, and devices, and the distributed cloud architecture was based on low-cost and blockchain on-demand access. In our view, this architecture requires consideration of the principles and challenges posed by IoT, such as energy consumption, communication between devices, and resource limitations of IoT devices.

Sharma *et al.* [29] developed a hybrid network architecture for smart city based on the idea of blockchain. This hybrid architecture is divided into two core network and edge network to achieve efficiency. This hybrid architecture utilizes centralized features and distributed network architecture and uses a design for the POW to maintain security and privacy. The evaluation of the architecture addresses aspects such as delay, hash rate, and block, but does not consider the IoT energy consumption issues and security analysis. Furthermore, efficient deployment of edge nodes and enabling of caching technique at the edge nodes seem to be challenging in this hybrid network architecture.

Similarly, the authors in [30], proposed a smart-city-based block-VN-based car network architecture. Block-VN is a reliable and secure architecture that operates in a distributed manner based on a distributed transmission management system. They considered a network system of vehicles with the blockchain and used network-centered paradigms and the data on vehicles. In their tested scenario, this study explores the principles of inter-vehicular network design, while not addressing the evaluation parameters and IoT challenges.

Hammi *et al.* [31] designed a robust, transparent, flexible, and energy efficient mechanism called BCTrust that uses the classical blockchain authentication mechanism for computation, storage, and energy limitation. This work considered wireless sensor networks as a part of the IoT. It uses a cluster structure and a cluster head called CPAN, which has an encryption key and allows secure transmission of transactions through a blockchain. The direction in evaluating this method is the use of the C language and the Ethereum blockchain. It must be said that this mechanism does not have a significant influence on the effectiveness of comparisons on performance metrics, including energy.

In [32], blockchain was used for building the IoT systems as well as their control and configuration. In their method, Ethereum was used because of the possibility of using smart contracts. In this work, the keys are managed using RSA public key encryption, so that the public keys are stored in Ethereum and private keys are kept on separate devices for easy configuration and management. Limitations such as memory of IoT devices were not taken into account for maintaining the whole chain and their energy consumption in this work.

3 Proposed Architecture

In the proposed architecture, distributed network management for IoT devices is implemented using an IoT-tailored blockchain and SDN controller in a cluster structure. Fig. 1 illustrates a high-level representation of the proposed architecture in which the SDN controllers are connected to one blockchain, so that IoT devices can communicate. SDN controllers generate a distributed P2P network, such as what is seen in Bitcoin. The two main purposes of this architecture are to enhance the security of communication between IoT devices, and to reduce energy consumption among them.

Large networks usually cannot operate efficiently without organized structures, which is why we were motivated to use a cluster structure [33]. In this architecture, each cluster is called an SDN domain. To reduce the network delay and overhead in each SDN domain, the SDN controller acts as a cluster head. Each SDN domain will have a coordinator (cluster head) responsible for the activation of IoT devices. The heterogeneous IoT devices are among other components in this architecture that are connected to the SDN controller. The controller is the coordinator of each cluster, and it responds to needs, enforces policies, and monitors the use of IoT devices in each SDN domain. Cloud storage is another component of this architecture used for storing transactions and public blockchains between SDN controllers and in some cases, used when IoT devices are to store their data in the cloud.

Centrally managed systems are a good target for illegal exploitation and cybercrime attacks [34]. The nature of the P2P of a blockchain protects the security and integrity of data and the elimination of the SPOF, which creates the incentive for us to use these features of the blockchain in a distributed relationship between the SDN controllers in the

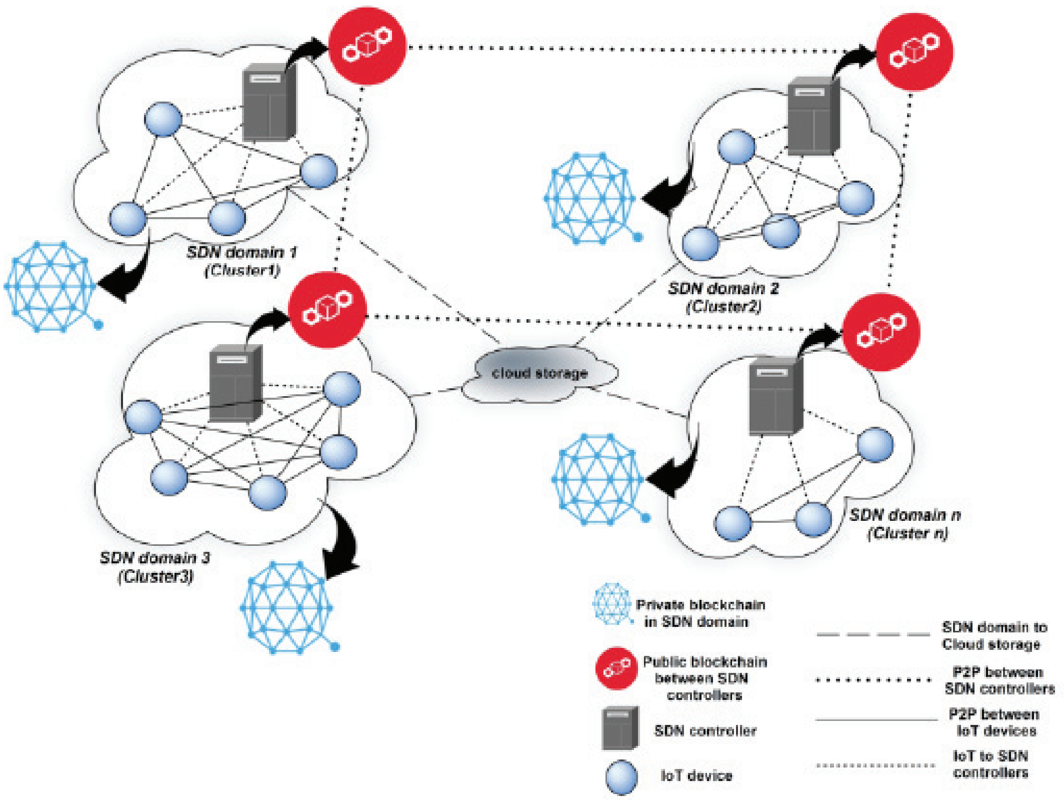

Fig. 1. Proposed cluster architecture using blockchain-based SDN controllers.

proposed architectural cluster structure. The P2P network distributed between controllers and the removal of intermediaries for secure communication contributes to creating a secure and comparable design in the proposed architecture. The P2P connection among the IoT devices can be observed inside the SDN domain.

We utilized public and private blockchains in our architecture. Public and private blockchains share the common principles of distributed ledger technology, supporting decentralized P2P networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions. In our context a public blockchain is created by cluster heads and stored between cluster heads (as shown in Fig. 2).

In the public blockchain, a new SDN controller with IoT devices can be added to this cluster architecture as if a new block is generated, and the history of completed transactions among the controllers would be available for it. A public blockchain network is completely open and SDN domains can join and participate in the network. One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale. To resolve this issue, we used a cluster-based structure in our architecture. In the public blockchain, we have considered the limitations in energy consumption and processing power, and we have solved the energy and security problem by the removal of the appropriate POW through the SDN controller and the authentication method used in each cluster. Blocks (SDN controller with IoT devices) are joined to the public blockchain without the need of POW process, which decreases the appending overhead and energy consumption significantly in the public blockchain. Also, resource limitations of IoT devices are not practically suited for high level and complex security methods thus, we used the SDN controller for managing required processes in each SDN domain via a private blockchain.

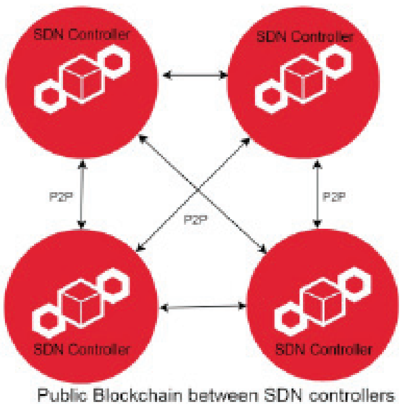

Fig. 2. Public blockchain between SDN controllers in proposed architecture.

In the architecture, the private blockchain is placed between the SDN controller and IoT devices in a SDN domain, as shown in Fig. 3. A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. We used authentication method in each SDN domain through SDN controller. In the private blockchain, the SDN controller uses an authentication and verification method (as explained in Section 3.2). Due to the specificity of private blockchains, the identity of the individuals involved in the transactions is clear. Such individuals are allowed access to data that are relevant to them. In each

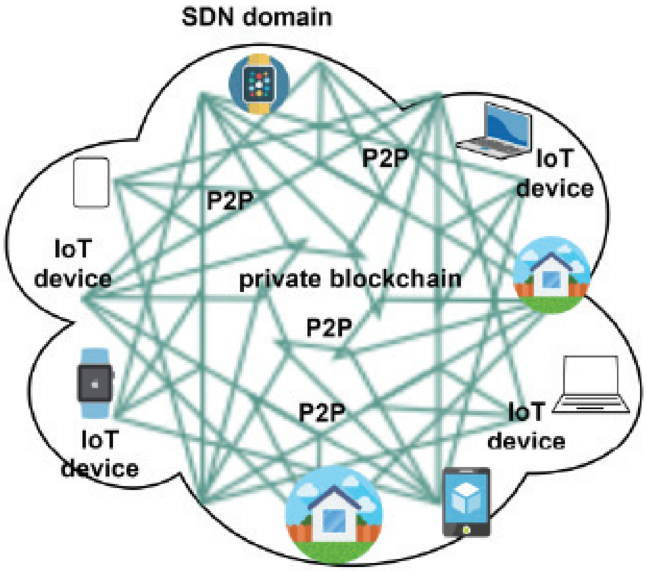

Fig. 3. Private blockchain between SDN controller and IoT devices.

SDN domain, there is a private blockchain that keeps track of transactions and has a policy energy efficiency to enforce IoT devices policy for incoming and outgoing transactions. All transactions to or from the SDN domain are stored in a private blockchain.

Each SDN controller (cluster head) has a unique public key, known by other SDN controllers in the network, used for generating new blocks or adding new SDN domain so that other SDN controllers could authorize the block generator. Each IoT devices is free to change its SDN domain or cluster if it experiences excessive energy consumption or delays. When an IoT device in a SDN domain is authenticated by the controller, the cluster head will store its identity under a transaction in the public blockchain. Then, the cluster head shares a public key and a private key to carry out the exchanges of that IoT device with its own SDN controller and other IoT devices. Whenever an IoT device intends to migrate to another cluster, it sends a request for membership to the new cluster head. The destination cluster head checks the public blockchain in order to ensure the identity of the applicant IoT device. When the new cluster head verifies the identity of the applicant IoT device, it sends a request for getting the public key related to that IoT device to the cluster head of the previous IoT device. After receiving this key, the cluster also confirms this new IoT device, and this transaction is registered in the public blockchain.

The public and private blockchain are employed for providing secure access control to the IoT devices and their data. Besides, each blockchain generates an immutable time-ordered history of transactions that is linkable to other tiers for giving specific services in the SDN domains.

3.1 File Transfer Between IoT Devices in an SDN Domain in the Proposed Architecture

In our proposed architecture, each IoT device has a public and private key that securely carry out transactions in blockchain by the policies of the SDN controller. If an IoT device is to send a packet into its cluster, it publishes it using its public key and signs it with its private key. Considering the public key of the sender, other members check the authenticity of the packet sent in the block format. If the IoT device is allowed to share the file, other members in the cluster will authenticate it, and this block will be stored in the private blockchain and the file is sent to the recipient. If the IoT device is to send a file to the receiver outside of its cluster, after the public key is published, the SDN controller notices that there is an IoT device in the other cluster and requests its membership to its cluster head. Eventually, after the IoT device is transferred to the desired cluster, the file will be sent to the recipient.

Let's assume, there is a private blockchain among the IoT devices inside a cluster (A1, A2, A3, and A4), as shown in Fig. 4, the following steps will be taken for the file transfer process:

Step 1. A1 wants to transfer its file to A4.
Step 2. A transaction is signed by A1, it is published with the public key and signed with the private key of the transaction (file).
Step 3. The block is broadcasted using the public key across the entire network. If there is no IoT device in this cluster, the SDN controller will send that IoT device to another cluster (SDN controller).
Step 4. The network IoT devices authenticate the transaction according to the public key. In fact, by considering the public key, the sender authenticates the packets.

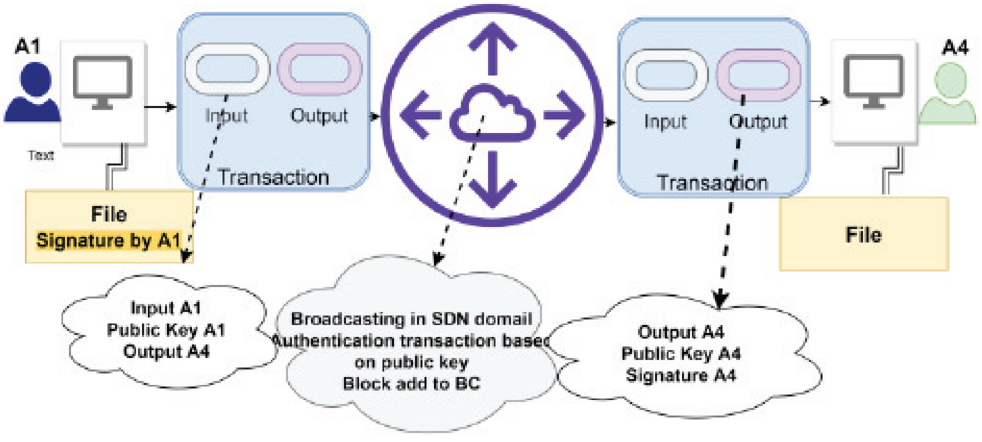

Fig. 4. Secure file transfer between two IoT devices in an SDN domain.

Step 5. A block is added to the chain, which makes transactional transparency.

Step 6. The file is transferred from the sender to the receiver, and only the receiver can decode the file.

3.2 Enhancing Security and Energy Efficiency in the Proposed Architecture

Open (public) blockchains basically use a consensus mechanism known as POW to commit a new block into the ledger. Because the use of POW which requires a lot of resources, in terms of energy or processing resources, using blockchains in IoT domain has been almost impractical [3]. Moreover, the issue of comparability requires a consensus among miners and also increases the delay. Hence, we propose a cluster structure used by the SDN controller and an authentication method with distributed trust (presented in Algorithm 1) to solve the POW problem at public POW-based blockchains (known as classical blockchains), which will be reducing time overheads and energy consumption). Communications within clusters and between cluster heads are regarded as transactions in public and private blockchains. Blocks are added to the public blockchain without the POW, which completely reduces the overhead imposed by original POW. For the authentication method by the SDN controller, we use distributed trust to ensure that the received blocks are valid and to decrease the overhead for verifying blocks. When a block is generated, its hash is created by the SDN controller. Whenever its data changes, its hash changes and is calculated by the controller. The hash of the block is what makes the chain, and this whole approach provides a secure method.

In IoT devices within the proposed architecture, we have the ability to share data, carry out transactions, and consider features via smart contracts. Furthermore, we have heterogeneous devices with security and multiple energy resources in each SDN domain. Hence, it is necessary to present a suitable routing protocol in the proposed architecture in order to take into account the energy efficiency and energy consumption for IoT devices in each SDN domain. Using the SDN Controller available in each SDN domain, the possibility of presentation of network services to IoT devices are provided by the controller. The proposed protocol can prevent the access of malicious and selfish nodes to the SDN domain, so that in addition to increasing security, it can decrease energy consumption, as IoT devices are mostly low-power and have little computational ability. Energy consumption plays an important role in data transfer in each SDN domain. The security and energy efficiency mechanisms are summarized in a flowchart, as shown in Fig. 5.

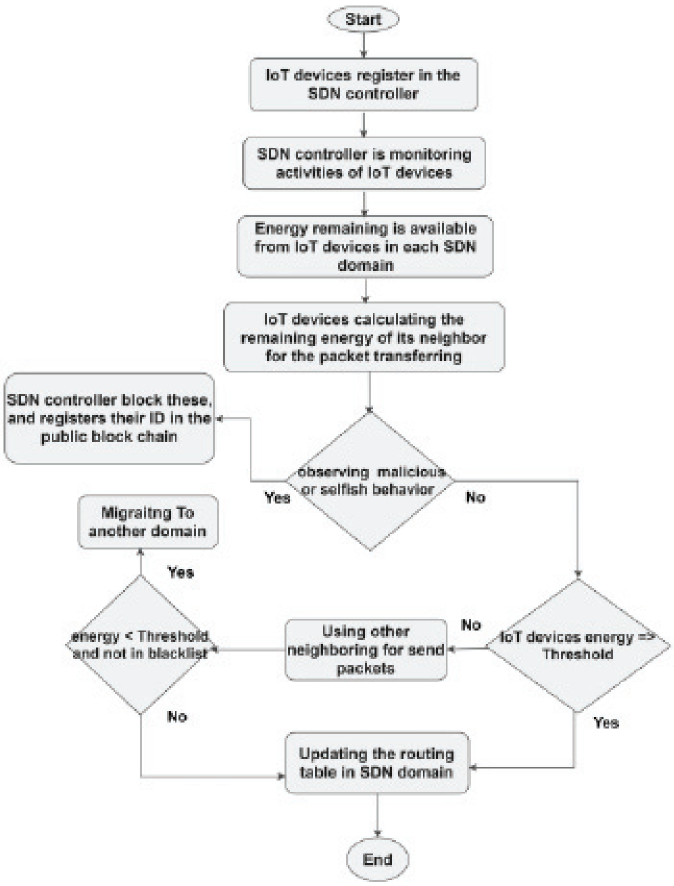
Start
IoT devices register in the SDN controller
SDN controller is monitoring activities of IoT devices
Energy remaining is available from IoT devices in each SDN domain
IoT devices calculating the remaining energy of its neighbor for the packet transferring
SDN controller block these, and registers their ID in the public block chain
observing malicious or selfish behavior
Yes
No
Migraitng To another domain
Yes
energy < Threshold and not in blacklist
Using other neighboring for send packets
No
IoT devices energy => Threshold
No
Yes
Updating the routing table in SDN domain
End

Fig. 5. Flowchart of the security and energy efficiency mechanisms in proposed architecture.

As depicted in the figure, IoT devices must first register in the SDN controller. The SDN controller gives a unique IP address to each IoT device in each SDN domain, then a public and a private key are allocated to it. The SDN controller is aware of the energy status of the IoT devices and monitors its activities and transactions. In each private blockchain of each SDN domain, a set of data are available from the energy sources and energy remaining from IoT devices. Each IoT device has the capability to calculate the remaining energy of its neighbor for the packet transfer. Each IoT device sends packets based on the amount of energy sent to the controller or other devices for the transaction. If the amount of energy exceeds the threshold, it transfers its packet, or uses other neighboring nodes. The controller of the nodes with malicious behavior or selfishly send packets to neighbors, blocks their energy resources when they trespass the threshold. And further, it registers their IDs in the public blockchain so that they cannot register in other clusters. A node registered in an SDN controller is authenticated in another SDN domain because its public key is valid in the public blockchain. For other SDN controllers, if a node has energy below the threshold, it can migrate to other SDN domains. In order to maintain the SDN domain's lifetime, if nodes are below the threshold and are not listed in blacklist, they can migrate to another SDN domain and receive their private keys from the new SDN controller for the transaction. When IoT devices are in the different clusters, the SDN controller can move to another cluster because its public keys are stored and authenticated in the block. The proposed algorithm used in each SDN domain for increasing security and decreasing energy consumption is formally presented in Algorithm 1.

The SDN controller enables various services to be provided by IoT devices and makes the network efficient. By the controllers in the proposed architecture, the possibility of communication of the IoT devices to the two different SDN domains is provided. In fact, the controller provides a secure network with the help of the blockchain technology, which uses P2P communication. The features of each IoT device in our architecture include the source and destination IP addresses, public and private keys, and amount of energy. SDN controllers have a list of blocked devices (blacklist) and performed transactions.

Algorithm 1. Security and Energy Efficiency

```
Parameters:
  C: object // C is the SDN controller
  C: object // C is the SDN controller
  a: object // a is the IoT device
  E: double// amount of IoT device energy
  PK1, PK2: Key // the public and private key
  Msg: Message
  authList: AddressList // list of the IoT device
  Blacklist: AddressList // list of the IoT device is blocked
  ID: Address // IP address of IoT device
  Pub_BC, Pri_BC: Blockchain
  Th: double// threshold of energy
Function: RejesterIOTdevices (AddressList list, Address id)
  //record ID address in Private Blockchain
  //give public and private key
  //return IP address of IoT device in SDN domain
Function: MonitoringbySDNcotroller (AddressList list)
  //monitor behavior and transaction between IoT devices
Function: CalculatingEnergy&maliciousIOT (AddressList
  list, double e, AddressList blacklist)
  // find information about neighbors
  //detect selfish & malicious behavior by IOT
  //calculate the residual energy of IoT device
Function: MigrationIOTdevice (AddressList blacklist,
  Blockchain Pub_BC)
  //IoT devices able to migrate base on energy consumption
  to other SDN //domain
Function: Routing (AddressList blacklist, Blockchain Pub_
  BC, Blockchain Pri_BC, AddressList list, double e) //IoT
  device will transmit the packet base on energy value
  begin
    C → this
    a (msg) → receive ()
    Rejester = RejesterIOTdevices (AddressList list, Address
    id)
    AuthList = pub_BC.SendCall (msg: address)
    Monitor = MonitoringbySDNcotroller (AddressList list)
    Behavior = CalculatingEnergy&maliciousIOT (Address-
    List list, double e, AddressList blacklist)
    If (ID = malicious or selfish) then
      ID = blacklist.AddressList STATE
    Else if (energy_ID > th) STATE
      S= Routing (AddressList blacklist, Blockchain Pub_
      BC, Blockchain Pri_BC, AddressList list, double e)
      STATE
      Send (C: address, msg)
    Else
      ID = MigrationIOTdevice (AddressList blacklist,
      Blockchain Pub_BC)
    If (a. Rejester (msg, PK1, PK2)) then Pri_BC.S (msg:
    address)
end
```

TABLE 1
Notations

Notations	Description
Te	The transmission energy
B	The size of the packet
E	The energy required to accept the packet
b	The energy dissipation in channels
d	Distance between the two nodes
dt	Distances threshold
R	Receiving energy
A	Current energy of each IoT
C	Calculated remaining energy
Ei	Primary energy
Etotall	Energy consumed by controllers and IoT devices
Nt	The number of transactions
m	The number of controllers
i	The number of IoT devices
EI	Energy consumed by IoT devices
W	The number of various paths
Ec	Energy consumed by controller
λi	ith IoT device at rate
ρ	Probability of the packets must send
Qm(i)	Probability of m packets in the ith IoT devices
μi	Rate of packet receives
Wsi	The mean packet processing time

The *protocol* presented below is used to achieve energy efficiency. A summary of notations used in the paper is given in Table 1.

In short distances, Equation (1) is used to calculate the transmission energy based on the distance and the environment's features. At near distances b = 2

$$T = B \times d^b \quad if \quad d \leq d_t. \tag{1}$$

For long distances, Equation (2) is used (b = 4)

$$T = B \times E \times d^b \quad if \quad d > dt. \tag{2}$$

Consumed energy of packets received for each IoT devices is calculated via Equation (3). R is the receiving energy

$$R = E \times B. \tag{3}$$

Current energy of each IoT device is calculated via Equation (4) (A)

$$A = T \times R. \tag{4}$$

The remaining energy is calculated via Equation (C) where Ei is the primary energy of each IoT node

$$C = Ei - A. \tag{5}$$

3.3 Illustrative Example: Smart City Case Study

Smart cities are a frame for addressing the unique challenges of living in cities by combining new technologies like, Internet of Things, transaction management, and business planning [35]. In this section, we illustrate the use of our architecture in a smart city environment. Based on our proposed architectural features, we use the cluster structure of scaleability to resolve geographic problems. We have the communications between clusters in the smart city that they are SDN domains with IoT devices. SDN controllers are the coordinator of the each SDN domain and monitors IoT devices' activities. With the help of the proposed architecture equipped with blockchain and SDN, we get a secure and energy efficient communication in smart cites, we used routing protocol that it is appropriate for IoT limitations. Fig. 6, shows a possible architecture of IoT nodes in a smart city using our approach.

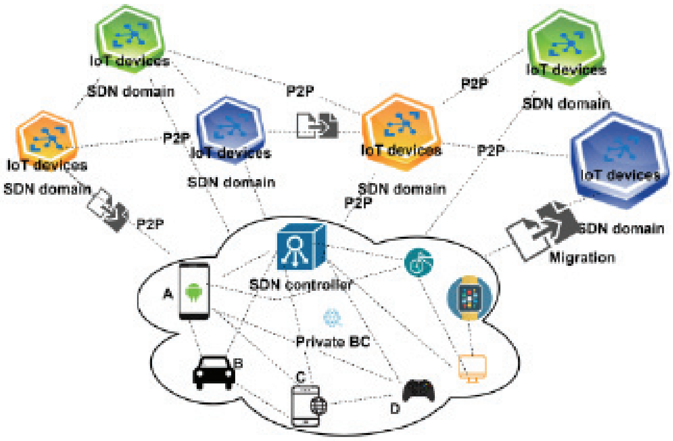

Fig. 6. Use of proposed architecture in smart city.

TABLE 2
Stimulation Parameters

Simulation Parameters	Values
Simulator	mininet-wifi / Ethereum / Pyethereum
Number of SDN controllers	6
Type of SDN controller	Opendaylight
Number of IoT devices	90
Number of SDN domain	6
Simulation time	100 s
Mobility model	Random waypoint model
Traffic Type	Constant Bit Rate (CBR)
IoT devices speed	10 m/s
Type of Antenna	Antenna/Omni Antenna
MAC protocol	Mac/802.11
Initial Energy value of IoT device	10-15 j
Initial Trust value	5 j
Area	1000 m * 1000 m
Packet size	512 Byte

Depending on the need, there is the possibility of migration of IoT devices form SDN domain including lack of energy, delays in the response from the SDN controller or displacement in the geographical range. Referring to the figure, device A can use the communication path via device B for transmitting packets to device C because less distance and less energy are spending on transmission instead of transmitting to device C directly. Also, they are securely interacted by private blockchain in this SDN domain. In the SDN domain routing protocol focus on security and energy efficient communication based on the algorithm presented in the previous section. Device D will be able to use the communication path via device A for taking packet data from another cluster. The routing information between two SDN domains being set up on the SDN controller and public blockchain then become updated in the SDN domain. Finally, the messages will be exchanged between both devices.

4 Evaluation Results and Analysis

We first evaluate the throughput, performance, and energy efficiency of the proposed architecture using simulation (Section 4.1). Further, we present the analytical evaluation of the proposed routing protocol (Section 4.2). Then, we evaluate the proposed routing protocol in the proposed architecture and compare it with well-known routing protocols, and two energy-aware IoT protocols (Section 4.3). Finally, we present a comparative summary between simulation and analytical results (Section 4.4).

4.1 Performance Evaluation

In this part, we present the implementation details, the testing environment and evaluation of the proposed architecture in terms of throughput, performance, and energy efficiency. In our work, the mininet-wifi simulator [36] and the opendaylight controller [34] were used to implement the SDN domain. For implementing blockchain parts, Pyethereum tester tool [37] under Ethereum platform was utilized (Ethereum platform in Ubuntu 18.04 LTS platform was installed). Pyethereum was used to test and evaluate public and private blockchains without interacting with the blockchain itself for the experiment purpose. We integrated blockchain and SDN for transmitted secured file or document sharing between IoT devices among the SDN domains. We installed the Ethereum in a virtual machine (VM) which has different IP addresses with other VMs, and mininet-wifi for creation of other SDN domains. This SDN topology was remotely connected to opendaylight SDN controller. The simulation environment consists of 6 clusters, i.e., 6 SDN domains, and the opendaylight controller is as a cluster head in each cluster connected to the IoT devices. In each cluster, 15 Node IoTs come with different energy resources that can be moved to other clusters if there is a delay in connection and a reduction in energy consumption. In fact, we consider the mobility affects of IoT nodes during our simulations, and the maximum speed of IoT devices are 10 m/s. The cloud storage was directly connected to the opendaylight controller and was used to store blockchains, data, and block retrievals. In order to compare the proposed architecture's overhead, another scenario (pair work) was created for simulation. In this case, we used the Blockchain Fundamental (BCF) that uses hashing and POW (i.e., classical blockchain). BCF does not consider the limitations of IoT devices and cluster structures. In fact, the POW has an energy and time overhead for IoT devices. The routing protocol whose algorithm was described in the previous section is used in our opendaylight controller architecture that offers the energy efficiency features to reduce the energy consumption of IoT devices.

We ran the simulation for 100 seconds, during which 1924 transactions were generated and the average result is 10 simulations. The metrics that were used in this evaluation include: Throughput, Packet overload, Time overhead, Response time, Energy consumption, and Bandwidth and delay efficiency. Table 2 shows the used simulation parameters.

Throughput. The number of transaction requests among IoT devices in a network, is referred to as the total throughput time or total transaction time of transactions. In Fig. 7, the difference throughput of our proposed architectural approach and the BCF method can be observed. As we used the cluster structure and optimized algorithm for IoT nodes, it helped to reduce the time overhead and processing by improving the throughput compared to BCF.

Packet Overload. The length of packets sent in classic BCF, using encryption, hashing, and POW increases the payload

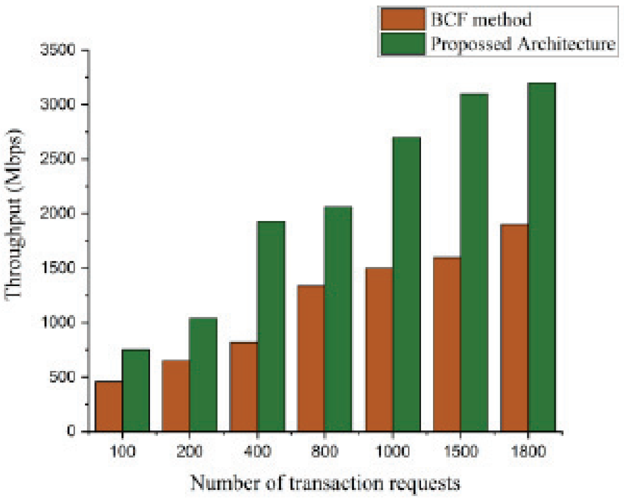

Fig. 7. Comparison throughput of the proposed architecture with BCF.

TABLE 3
Evaluation of the Packet Overhead Between Proposed Architecture and BCF Method

Type of Packet Flow	BCF (Bytes)	Proposed Architecture
IoT devices to the controller	32	4
SDN controller to storage	48	4
IoT device to IoT	16	4
IoT devices to storage	16	4

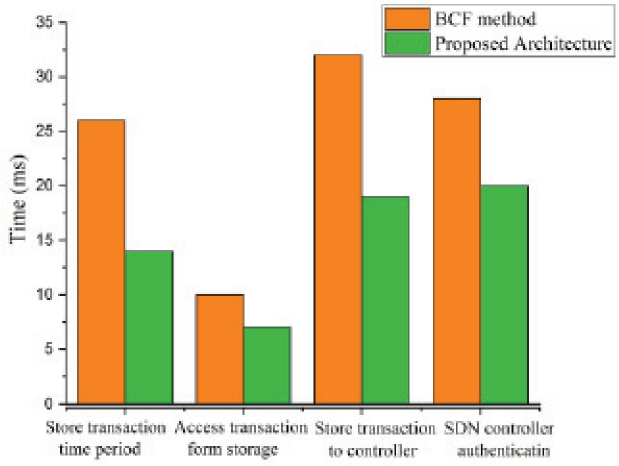

Fig. 8. Comparison of time overhead of the proposed architectural with that of the BCF method.

and packet header size. While in our method, by removing the POW and using the lower layer header [38] and the proper irradiation mechanism for the IoT network, there is less packet overhead as seen in Table 3.

Overload Time. The processing time of each transaction, when the controller responds to requests. Fig. 8 illustrates that the classic BCF method takes more time to process packets than the proposed method because it has more encryption and more POW operation in the classic method. In addition, our method uses the proper protocol for IoT nodes, which is a fast and energy efficient packet transmissions protocol.

Response Time. It refers to the file transfer time between two IoT devices, which in our proposed method, we can observe an improvement compared to the classic method because of using the custom routing protocol in the controller. Fig. 9 shows the average response time for file transfer with different sizes between IoT nodes, in which our method has less overhead than the BCF method.

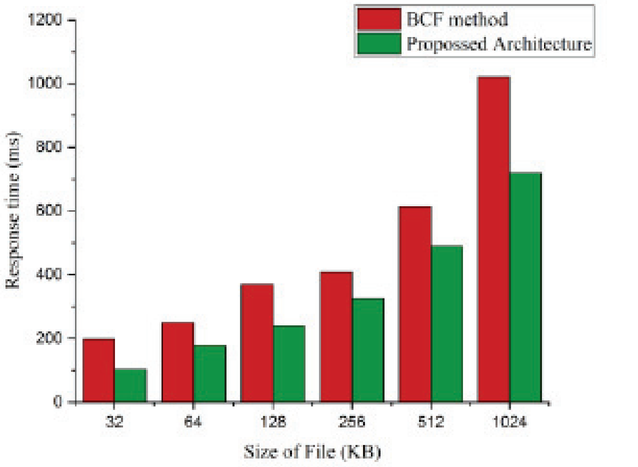

Fig. 9. Comparison of the response time of the proposed architecture with that of the BCF method.

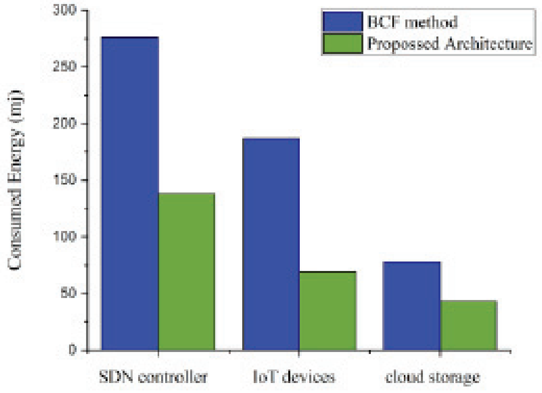

Fig. 10. Comparison of the energy consumption of the proposed architecture with that of the BCF method.

Energy Consumption. Energy consumed by controllers and IoT devise involved in the transaction. The energy consumption can be calculated using the Equation (6)

$$\text{Etotall} = Nt \times T + [(m \times Ec) + (i \times EI)]. \tag{6}$$

The BCF method for encryption, POW, and hashing is more energy consuming by controller and IoT devices during simulation. We also used the efficient energy routing protocol for transmitting and receiving packets in the proposed cluster architecture. The results of this comparison are shown in Fig. 10.

Bandwidth and Delay Efficiency. The data transfer latency in the proposed blockchain-based architecture can be improved using the SDN controller. As previously illustrated in the steps of the file transfer between IoT devices for an SDN domain, the efficiency of the proposed architecture can be also assessed in terms of delay and bandwidth. Generally, SDN controllers monitor the IoT activities in each cluster. In some cases, two given IoT devices may not be in the same cluster during file transfer. Therefore, there

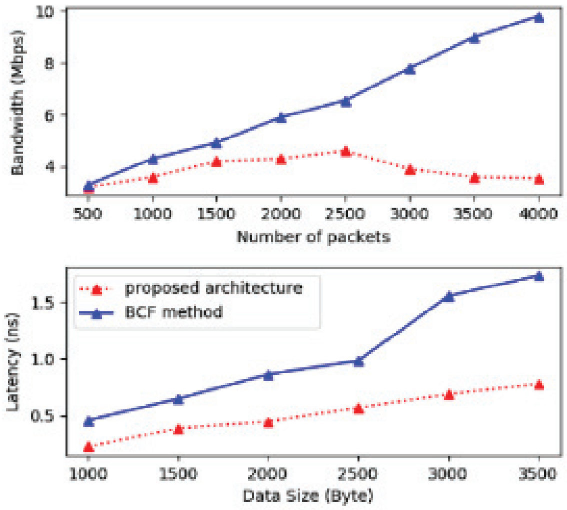

Fig. 11. The efficiency of consumption bandwidth and delay measured between proposed architecture with that of the BCF method.

are various paths between source and destination in our scenario which an SDN controller can select for transferring. In this particular evaluation, we consider the mobility model and the traffic type in form of the random waypoint model and constant bit rate (CBR) respectively. We also increased the number of packets from 500 to 4,000 packets with data size 1,000 byte to 3,500 bytes for this examination. The proposed architecture compared with the BCF method has less delay since the BCF method does not consider the amount of traffic and delay in each cluster. In Fig. 11, the latency of the BCF method is increased from 0.5 to 1.8 ns by growing the data size since the packets are in the queue and waiting for processing. However, the proposed architecture has less delay owing to having a cluster structure. The various paths between source and destination represents the number of various paths in the proposed architecture for sending, and the SDN controller concurrently sends data from various paths to reduce the transmission delay in the clusters. Also, this action causes a decrease in consuming bandwidth in each cluster and finally the entire network during transferring packets. As depicted in Fig. 11, with the proliferation of packets transferring at the path among IoT devices in the clusters, the proposed architecture is more efficient than BCF method that increases the use of bandwidth from 0.8 to 10 Mbps as the SDN controller considers the traffic of another cluster and sends packets through the most efficient path.

4.2 Analytical Evaluation of the Proposed Routing Protocol

In addition to the simulation results, this part presents the analytical evaluation based on a queueing theory to further evaluate the performance parameters: throughput, end-to-end delay, and energy in the proposed routing protocol, which are compared with the simulation results in Section 4.4. We have considered a queueing model for proposed routing protocol [12], as illustrated in Fig. 12. The SDN controller and IoT devices are modeled as queueing systems to capture the time cost of the clusters.

To analyze the performance parameters of our model, we have used an $M/H/2/1$ theory of queuing model [39], since

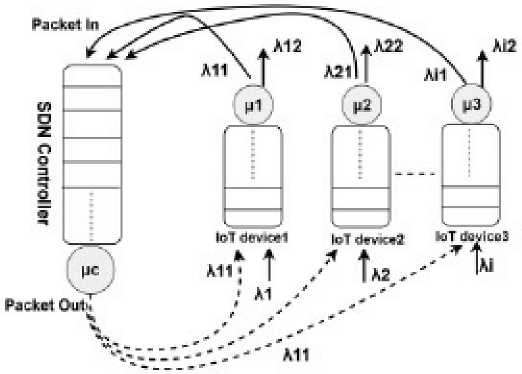

Fig. 12. Queueing model for proposed routing protocol.

we are dealing with IoT devices with a limited energy capacity. We assume that the average packet arrival rate in the ith IoT device is λi, and that the arrivals in different IoT devices are autonomous. Some incorrect and malicious packets must send to the SDN controller that this happens (ρ). here, $M/H/2/1$ which means packets arrive at the ith IoT device at rate λi and the service time is represented by $\lambda i \times \rho$ and $\lambda i \times (1-\rho)$ distribution. At this time, μ_1 with probability ρ, while it receives service at rate μ_2 with probability $1-\rho$. X state is defined by x couple (x, y), where x is all the packets in the IoT device and Y is the existing service stage. In our case, y can be only 1 or 2. The stationary distribution of our queue in the ith IoT device can be gained by putting on the Matrix-Geometric Technique [40]. We indicate the stationary probability vector Q(i) in the ensuing equations

$$Q(i) = (Q(i)_0, Q(i)_1, Q(i)_2, \ldots Q(i)_m, \ldots) \tag{7}$$

$$\rho = \frac{\lambda}{\mu} < 1 \tag{8}$$

$$Q_{(0)} = 1 - \rho \tag{9}$$

$$Q_{(m)} = (1-\rho)\rho^m. \tag{10}$$

The mean number of packets in the queueing system can be calculated as

$$N_i = \sum_{k=1}^{\infty} K\pi_k^i \tag{11}$$

$$N_i = \sum_{k=1}^{\infty} (1-\rho)\rho^k \tag{12}$$

$$N_i = (1-\rho)\sum_{k=1}^{\infty} k\rho^k = (1-\rho)\rho\sum_{k=1}^{\infty} k\rho^{k-1}. \tag{13}$$

Because $k\rho^{k-1}$ can be written as $k\rho^{k-1} = \frac{d\rho k}{d\rho}$, respectively

$$N_i = (1-\rho)\rho\sum_{k=1}^{\infty}\frac{d}{dp}p^k = (1-\rho)\rho\frac{d}{dp}\left(\sum_{k=1}^{\infty}p^k\right). \tag{14}$$

Therefore, $\sum_{k=1}^{\infty} p^k = \sum_{k=1}^{\infty} p^k - 1 = \frac{1}{1-\rho} - 1 = \frac{\rho}{1-\rho}$.

We have achieved

$$N_i = (1-\rho)\rho\frac{d}{dp}\left(\frac{\rho}{1-\rho}\right) \tag{15}$$

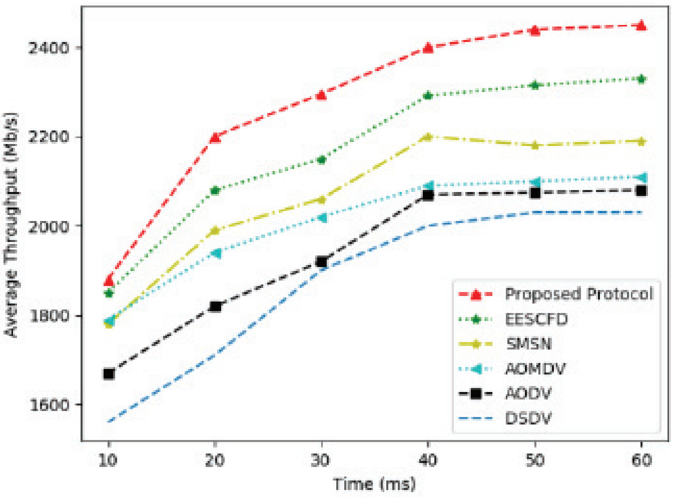

Fig. 13. Throughputs of the proposed protocol, EESCFD, SMSN, AODV, AOMDV, and DSDV protocols in mobility scenario: A comparative summary.

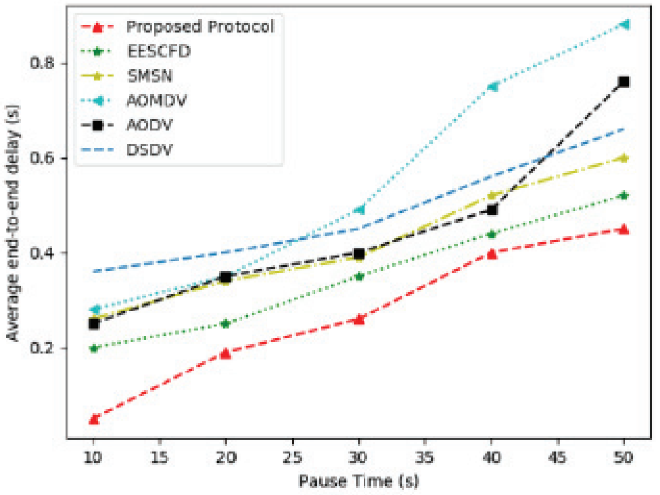

Fig. 14. Comparison of end-to-end delay of the proposed protocol with that of EESCFD, SMSN, AODV, AOMDV and DSDV protocols in mobility scenario.

$$N_i = \left(\frac{\rho}{1-\rho}\right). \tag{16}$$

Where $\rho < 1$ and $\rho = \frac{\lambda}{\mu}$, consequently

$$N_i = \frac{\lambda}{\mu - \lambda}. \tag{17}$$

Based on the Little law [41], the average packet processing time in the *i*th IoT device can be assumed by

$$W_{S_i} = \frac{1}{\lambda} N_i = \frac{1}{\mu - \lambda} \tag{18}$$

$$W_S = \sum_{i=1}^{n} \frac{\lambda_i}{\sum_{1=1}^{n} \lambda_i} W_{S_i}. \tag{19}$$

4.3 Evaluation of the Proposed Routing Protocol

Our proposed routing protocol is built upon the cluster structure and the energy and computational limitations of IoT devices. The protocol utilizes the security features of the blockchain for improving security in line with the requirements of energy efficiency, and SDN controller for authentication and verification method in each cluster. Also, the stability feature is provided via SDN controllers for the proposed protocol. The proposed protocol can adapt to considerable changes that may happen during routing in each cluster via existing SDN controllers in the same cluster or adjacent SDN controllers in neighbor clusters. As a result, our architecture provides stability for the proposed protocol. The stability of proposed protocol is managed by SDN controller since it considers the behavior of the proposed protocol during routing for selecting optimal path in other to reducing energy consumption.

In this part, we present the comparison results of the proposed routing protocol with the routing reference protocols [41] including AODV, AOMDV, and DSDV. In addition, we compared the proposed routing protocol with two clustering and energy aware IoT protocols: Energy Efficient Secured Cluster based Distributed Fault Diagnosis protocol (EESCFD) [42], and Secure Mobile Sensor Network (SMSN) [43], based on the parameters of throughput, end-to-end delay, and energy with mobility affects.

Throughput. Throughput refers to the data rate that a node can send packets over the network. In fact, it is the number of packets successfully delivered from the origin to the destination [37]. Fig. 13 shows the throughput comparison between the sixth protocols.

As observed from the figure, the average throughput values of the proposed protocol increase more than those of EESCFD SMSN, AOMDV, AODV and DSDV, and maintain its value as the time increases from 10 to 50 s. This could be mainly because of the proper receiving of packets and less packet drop. Also, with the increase of connections, the possibility of link failures increases while the proposed protocol via SDN controllers can manage the connections better in each clusters. The average throughput is plateau with the time varying from 40 sec because the amount of dropping packets increases at the time of interface queue as the buffer is getting full.

Average End to End Delay. The average time of the packet sent from the source until the time the packet is derived in the destination, which includes delay in routing, delay in release, and transmission time [38]. The results of this particular comparison are shown in Fig. 14.

Fig. 14 illustrates the average end-to-end delay versus time by taking the each time delay which we considered as simulation time for the six routing protocols. It shows that the proposed protocol performs with less delay than EESCFD, SMSN, AODV, AOMDV and DSDV with time varying from 10s-60s when simulation is started. As the simulation time increases, the average end-to-end delay increases because of number of packets generates by each source increases.

Energy. Energy expresses the percentage of energy consumed by all existing IoT devices in the network. In Fig. 15, the energy consumption of our protocol and other protocols are based on the number of connections and mobility.

As observed in the figure, it shows the consumption energy between the proposed protocol with that of EESCFD, SMSN, AODV, AOMDV and DSDV in mobility scenario. All five protocols consume more energy than proposed protocol. The reason is that our protocol benefits from an energy

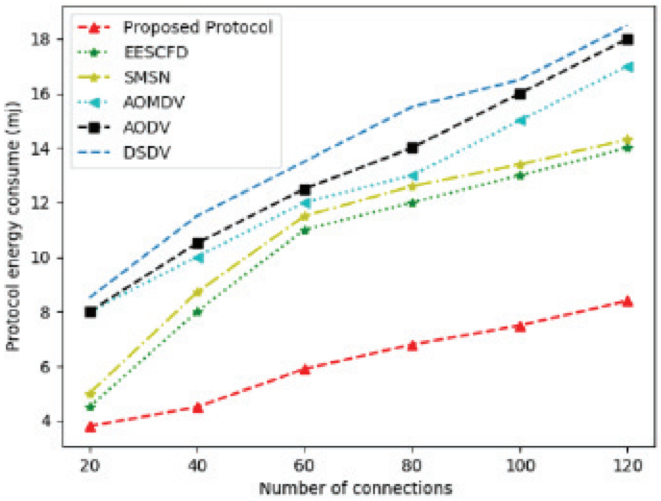

Fig. 15. Comparison of energy of the proposed protocol with that of EESCFD, SMSN, AODV, AOMDV, and DSDV protocols in mobility scenario.

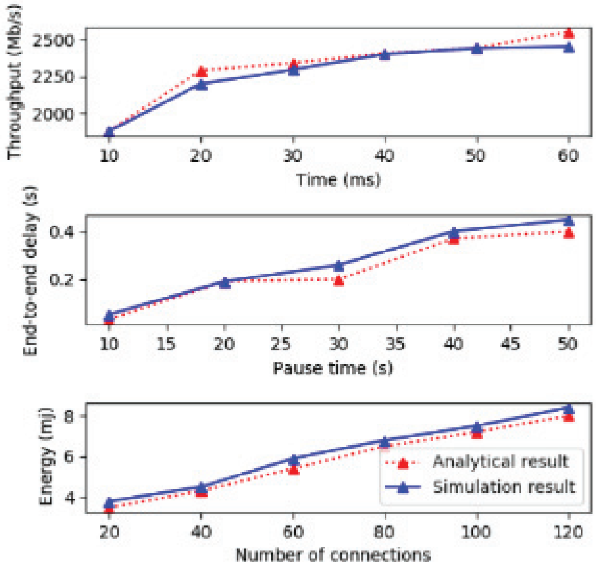

Fig. 16. Comparison of results calculated using our analytical evaluation and simulation result.

efficient approach in which routing table get updated based on node conditional and energy level in each cluster via SDN controller. Also, the results show that EESCFD protocol consumes less energy since it similarly uses a cluster based structure. DSDV protocol consumes more energy compared to all protocols. The reason could be that in DSDV lots of link failure occurs, and mostly dropped packets will be needed to retransmit on a same path. Overall, the results indicate that our routing protocol has better performance and efficiency than the peer routing protocols. This could indicate that the protocol would be promising for use in the proposed architecture for IoT devices.

4.4 Comparison of Simulation and Analytical Results

By and large, both simulation and analytical evaluation are modeling approaches, which help at providing an idea of model performance under various conditions. In fact, the analytical model is a mathematical abstraction that can be extended to address various working conditions and the simulation models prepare results for a special use case and should be run several times to balance the effect of numerical calculations. In this section, the simulation results will be compared to the analytical results of the proposed routing protocol. It is noteworthy that the simulation parameters that have been used for the simulation are listed in Table 2.

Fig. 16 presents the comparison of the throughput, end-to-end delay, and energy metrics which were calculated via our analytical evaluation in Section 4.2 and the simulation results achieved in Section 4.3. According to the comparison, we have 97 percent accuracy in the achieved results in the throughput, end-to-end delay and energy between simulation and analytical results. Consequently, the results confirm our analytical model.

5 Conclusion

Given the growing trend of IoT and the increasing needs for more intelligent and smart services, there exist many challenges and limitations in terms of security, privacy, and computing power that will need the urgent attention of research community. In order to mitigate some of these challenges, we presented an architecture for the IoT network, using two new emerging technologies, SDN and blockchain. In the cluster structure of the proposed architecture, private and public blockchains are used tailored for the IoT network. Using the routing protocol designed for IoT devices in the SDN controller and removing POW from the mix, our method managed to achieve a significant impact on reducing energy consumption and increasing the security of communication between IoT devices. Our proposed architecture is superior to BCF method in terms of throughput, performance and energy efficiency, while it offers a better routing protocol that outperformed EESCFD, SMSN, AODV, AOMDV and DSDV protocols. For future work, we intend to provide a high-level P4 architecture with the feature of the blockchain in the IoT domain and compare its efficiency parameters with our architecture.

Acknowledgments

This research was funded in part by the University of Texas at San Antonio & Instituto Tecnológico y de Estudios Superiores de Monterrey (UTSA & ITESM) Seed Funding Program, and the US National Science Foundation (NSF) Grant No. 1925723.

References

[1] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 46–59, Jan.-Mar. 2018.

[2] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput. Secur.*, vol. 88, 2020, Art. no. 101629.

[3] 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*, 2017, pp. 618–623.

[4] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, "Detecting crypto-ransomware in IoT networks based on energy consumption footprint," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 4, pp. 1141–1152, 2018.

[5] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018.

[6] P. N. Bahrami, H. H. Javadi, T. Dargahi, A. Dehghantanha, and K.-K. R. Choo, "A hierarchical key pre-distribution scheme for fog networks," *Concurr. Comput. Pract. E.*, vol. 31, 2019, Art. no. e4776.

[7] R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, and K. R. Choo, "Integrating privacy enhancing techniques into blockchains using sidechains," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, 2019, pp. 1–4.

[8] S. Rostampour, N. Bagheri, M. Hosseinzadeh, and A. Khademzadeh, "A scalable and lightweight grouping proof protocol for internet of things applications," The J. Supercomputing, vol. 74, pp. 71–86, 2018.

[9] J. Mocnej, M. Miškuf, P. Papcun, and I. Zolotová, "Impact of edge computing paradigm on energy consumption in IoT," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 162–167, 2018.

[10] A. Yazdinejad, R. M. Parizi, G. Srivastava, A. Dehghantanha, and K.-K. R. C. Choo, "Energy efficient decentralized authentication in internet of underwater things using blockchain," in *Proc. IEEE Globecom Workshops*, 2019.

[11] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[12] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in *Proc. Int. Conf. Comput. Commun. Autom.*, 2017, pp. 720–725.

[13] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Efficient design and hardware implementation of the OpenFlow v1. 3 switch on the Virtex-6 FPGA ML605," *J. Supercomput.*, vol. 74, no. 3, pp. 1299–1320, 2018.

[14] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "P4 to SDNet: Automatic generation of an efficient protocol-independent packet parser on reconfigurable hardware," in *Proc. 8th Int. Conf. Comput. Knowl. Eng.*, 2018, pp. 159–164.

[15] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Performance improvement and hardware implementation of open flow switch using FPGA," in *Proc. 5th Conf. Knowl. Based Eng. Innovation*, 2019, pp. 515–520.

[16] M. K. Pandya, S. Homayoun, and A. Dehghantanha, "Forensics investigation of OpenFlow-based SDN platforms," in *Cyber Threat Intelligence*. Berlin, Germany: Springer, 2018, pp. 281–296.

[17] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in *Proc. IEEE Globecom Workshops*, 2016, pp. 1–6.

[18] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, 2017, pp. 303–308.

[19] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2019.2937481.

[20] R. M. Parizi, A. Singh, and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security," in *Proc. Int. Conf. Blockchain*, 2018, pp. 75–91.

[21] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Serv.*, 2016, pp. 1–3.

[22] M. Pilkington, "11 blockchain technology: Principles and applications," *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar Publishing, 2016.

[23] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," in *Proc. 28th Annu. Int. Conf. Comput. Sci. Softw. Eng.*, 2018, pp. 103–113.

[24] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, 2019.

[25] R. M. Parizi and A. Dehghantanha, "On the understanding of gamification in blockchain systems," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops*, 2018, pp. 214–219.

[26] 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*, Kona, HI, 2017, pp. 618–623.

[27] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[28] 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.

[29] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, 2018.

[30] 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.

[31] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018.

[32] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol.*, 2017, pp. 464–467.

[33] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet-of-Things Des. Implementation*, 2017, pp. 173–178.

[34] M. Conti, T. Dargahi, and A. Dehghantanha, "Cyber threat intelligence: Challenges and opportunities," in *Cyber Threat Intelligence*. Berlin, Germany: Springer, 2018, pp. 1–6.

[35] D. Chen, Y. Tang, H. Zhang, L. Wang, and X. Li, "Incremental factorization of big time series data with blind factor approximation," *IEEE Trans. Knowl. Data Eng.*, to be published, doi: 10.1109/TKDE.2019.2931687.

[36] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. Rothenberg, "Mininet-WiFi: Emulator for software-defined wireless networks," in *Proc. 11th Int. Conf. Netw. Service Manage.*, Barcelona, 2015, pp. 384–389.

[37] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "A programmer's guide to ethereum and serpent," 2015. Accessed: May 06, 2016. [Online]. Available: https://mc2-umd.github.io/ethereumlab/docs/serpent_tutorial.pdf

[38] H. Mukhtar, K. Kang-Myo, S. A. Chaudhry, A. H. Akbar, K. Ki-Hyung, and S. Yoo, "LNMP- Management architecture for IPv6 based low-power wireless Personal Area Networks (6LoWPAN)," *IEEE Netw. Operations Manage. Symp.*, Salvador, Bahia, pp. 417–424, 2008.

[39] Y. Deutsch and B. Golany, "Securing Gates of a Protected Area: A Hybrid Game and Queueing Theory Modeling Approach," *Decis. Anal.*, vol. 16, no. 1, pp. 31–45, Mar. 2019.

[40] R. Bhatia and J. Holbrook, "Riemannian geometry and matrix geometric means," *Linear Algebra Appl.*, vol. 413, no. 2/3, pp. 594–618, 2006.

[41] R. R. Ema, M. A. Akram, A. Hossain, and S. K. Das, "Performance analysis of DSDV, AODV and AOMDV routing protocols based on fixed and mobility network model in wireless sensor network," *Global J. Comput. Sci. Technol.*, vol. 14, pp. 1–11, 2014.

[42] T. Ara, M. Prabhkar, and P. G. Shah, "Energy efficient secured cluster based distributed fault diagnosis protocol for IoT," *Int. J. Commun. Netw. Inf. Secur.*, vol. 10, no. 3, 2018, Art. no. 539.

[43] M. Bilal and S.-G. Kang, "An authentication protocol for future sensor networks," *Sensors*, vol. 17, no. 5, 2017, Art. no. 979.

Abbas Yazdinejad received the BSc degrees in computer engineering from the Department of Computer Engineering, Shahid Bahonar University of Kerman, Kerman, Iran, in 2014, and the MSc degree in computer system architecture from the University of Isfahan, Isfahan, Iran, in 2016. He is currently associated with Cyber Science Lab, School of Computer Science, University of Guelph (UofG), Ontario, Canada. His research interests include software defined network (SDN), blockchain, FPGA design, IoT, and network modeling.

Reza M. Parizi (Senior Member, IEEE) received the BSc and MSc degrees in software engineering and computer science, in 2008 and 2005, respectively, and the PhD degree in software engineering, in 2012. He is the director of Decentralized Science Lab (dSL), Kennesaw State University, Georgia. He is a consummate technologist and software security researcher with an entrepreneurial spirit. He is a senior member the IEEE Blockchain Community and ACM. Prior to joining KSU, he was a faculty with the New York Institute of Technology. His research interests include R&D in decentralized AI, blockchain systems, smart contracts, and emerging issues in the practice of secure software-run world applications.

Ali Dehghantanha received the PhD degree in security in computing. He is currently the director of Cyber Science Lab, School of Computer Science, University of Guelph (UofG), Ontario, Canada. He has served for more than a decade in a variety of industrial and academic positions with leading players in cyber-security and artificial intelligence. Prior to joining UofG, he has served as a Sr. lecturer with the University of Sheffield, United Kingdom and as an EU Marie-Curie International Incoming fellow with the University of Salford, United Kingdom. He has a number of professional certifications including CISSP and CISM. His main research interests include malware analysis and digital forensics, IoT security, and application of AI in the cyber security.

Qi Zhang received the PhD degree in computer science from the Georgia Institute of Technology, Atlanta, Georgia, in 2017. He is currently a research staff member with IBM Thomas J. Watson Research Center. His research interests include blockchain systems, cloud computing, big data processing, and distributed systems. He published research articles in referred journals and conference proceedings such as the *IEEE Transactions on Computers*, *IEEE Transactions on Services Computing*, *ACM Computing Surveys*, VLDB, SC, HPDC, IEEE ICDCS, IEEE ICWS, IEEE CLOUD, ICBC. He received the top five picks award in IEEE ICWS 2017. He served as a program committee member for IEEE Blockchain 2018.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the PhD degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship with the University of Texas at San Antonio (UTSA). In 2016, he was named the cybersecurity educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, Outstanding associate editor of 2018 for the *IEEE Access*, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP the *Journal on Wireless Communications and Networking* (JWCN) Best Paper Award, Korea Information Processing Society's the *Journal of Information Processing Systems* (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscrypt 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a fellow of the Australian Computer Society, and co-chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.

▷ **For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/csdl.**