IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES

Received June 8, 2020, accepted June 16, 2020, date of publication June 23, 2020, date of current version July 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004486

Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network

A. S. M. SANWAR HOSEN[1], SAURABH SINGH[2], PRADIP KUMAR SHARMA[3], (Member, IEEE), UTTAM GHOSH[4], (Senior Member, IEEE), JIN WANG[5], (Senior Member, IEEE), IN-HO RA[6], (Member, IEEE), AND GI HWAN CHO[1]

[1]Division of Computer Science and Engineering, Jeonbuk National University, Jeonju 54896, South Korea
[2]Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea
[3]Department of Computing Science, University of Aberdeen, Aberdeen AB243FX, U.K.
[4]Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN 37235, USA
[5]School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410004, China
[6]School of Computer, Information, and Communication Engineering, Kunsan National University, Gunsan 54150, South Korea

Corresponding author: Gi Hwan Cho (ghcho@jbnu.ac.kr)

This work was supported by the Institute for Information and Communications Technology Promotion (IITP), Ministry of Science and ICT (MSIT), funded by the Korea Government, under Grant 2018-0-00508.

ABSTRACT Blockchain is attracting more and more attention to its applicability in the fields of Internet of Things (IoT). In particular, it is able to store data in unalterable blocks, associated with its secure peer-to-peer in a growing problem of transaction authorization in industrial and service provisioning applications. Moreover, it facilitates decentralized transaction (TX) validation and distributed ledger. The underneath algorithm of TX selection for validation may not be effective in terms of delay of various services of the applications. Because the existing random-based or fee-based selections are a delay insensitive that does not guarantee a minimum delay of a time-critical TX. This paper proposes a blockchain-based transaction validation protocol for a secure distributed IoT network. It includes a context-aware TX validation technique, where a TX is validated by a miner with the priority of a service. Besides, we adopt the Software Defined Networking enabled gateway as a middleware between IoT and the blockchain network in which the control operations and security of the network in a largescale are ensured. The proposed network model has evaluated and compared to the Core network. The results ensure the given priority in TX validation is more delay sensitive than the existing technique to provide quality of service of the network.

INDEX TERMS Internet of Things, blockchain technology, software defined networking, delay, security and privacy.

I. INTRODUCTION

Internet of Things (IoT) is a network of smart devices that are connected through the Internet [1]. These devices being connected in industrial automation, smart city, smart home, smart healthcare, social security, logistic, and so forth are capable of data gathering and sharing [2]. This provides benefits of various aspects such as better quality of life and greater insight into business in industrial applications known as Industrial IoT (IIoT). According to a statistic [3], the overall installed IoT based connected devices is projected to amount to 75.44 billion by 2025, a five times higher than the last ten years. The IoT enabled by global Internet technology is the foremost enhancement in delivering Internet's services of making the world a connected habitation.

The devices installed in IoT applications are constrained in several aspects that are not the key concern. Rather, a multitude of devices are connected to the Internet with inadequate hardware support, low cost, and sufficient energy supply (e.i., typically devices are on board battery driven) make challenging in terms of the desired features, such as reliability, cost, delay, energy-efficiency, and security and privacy. However, while managing a largescale distributed IoT network is challenging by locally to control, Software Defined Networking (SDN) techniques [4]–[7] can be the effective one to provide control and operations along with the security.

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

Blockchain is a core technology behind Bitcoin and other crypto-currencies [8]–[13] and comes into existence since the inception of the Internet. The usage of this technology in applications drew a lot of attention in the last few years. It is increasingly appearing on manufacturers' radar screens to improve the visibility of the supply chain or to promote supplier coordination around mass customization in industry automation. Industrial applications appear to be the most promising potential for blockchain, as researchers believe it is far less feasible to improve existing technologies used to integrate the industry automation. Blockchain is a distributed database that allows direct transactions (TXs) between peers without any central authorities. This simple yet powerful concept has great implications for various institutions and services. Any business or organization that relies on the existing system (a centralized database) as a core competitive advantage can potentially be disrupted by this technology. It would be a key improvement for the applications of IoT in near future [14], [15].

In blockchain technology, TX validation, block generation, and adding blocks to the blockchain are taken place. The fundamental process is the TXs validation by miners from the unconfirmed TXs stored in the TX-Pools prior to add into a new block. The block is added to the blockchain and then, a TX is executed by the requester. The existing TX selection to validate is either random-based or fee-based. Although, the probability of selection is equally distributed in random case or the priority according to the higher fee offered, it might not be effective when service oriented time-critical TX validation delay is taken into consideration.

There are also some other factors cause the delay in a blockchain system that might have cumulative impact on the metric of a time-critical TX. The factors are described as below:

- **Propagation Delay:** The propagation delay of blockchain is defined as the variance between the times that a miner announces the discovery of a new block or a TX and the time that the information is received by other miners for a period of operations.
- **Block Size and Miners:** While a block size is too small according to the network size (i.e., number of TXs of low power and lossy network (LLN) nodes and related services), the network is not able to serve shortly. A huge queue of unconfirmed TXs become pending in the TX-Pool of a miner. On the other hand, the less the miners on the network, the less the probability of a TX to be added into a new block in a current epoch as well.
- **Speed of Web:** The Internet speed affects the processing of the operations by the participants across the network which makes the network slower as a whole.
- **Memory-Pool:** It is a special place holder where the network stores all the TXs in a queue (in a case of using temporary shared memory of the participants that stores the unconfirmed TXs initially) [16]. If the block size is not enough to cover all the TXs made over the last epoch, some TXs are left in the Memory-Pool. The delay of the TXs is intuitive.
- **Attacks:** Blockchain network has suffered from several attacks [17]. The Spam attack where an adversary constantly send lots of small TXs with low fees to the network. In Sybil attack, a compromised node generates several IDs of its own and floods the network with TXs or generates forged claims, false traffic jams for example. The Modifying TXs where an attacker changes the content of data in a TX. And in Compromised Miner attack, a miner is able to modify any data stored in a TX. These attacks are to disrupt the service and compromise the security.

Research Contributions. Based on the earlier discussion, the key contribution of this research is summarized below:

- We propose a blockchain-based transaction validation protocol for a secure distributed IoT network. It is a context-aware priority based TX validation technique in a blockchain enabled secure IoT network called CaBNet. Here, on the basis of an instance of a device, a source adds a tag in the header of a generated TX. A miner by who validates a TX, selects a TX with a priority from its TX-Pool based on the rank of the TXs, so that the average delay of a time-critical TX is minimized.
- The network adopts the SDN-Gateway (GW) which acts as a bridge between the LLN and the blockchain network. SDN provides the network control and operations, and executes different actions in counter to various vulnerabilities and attacks.
- The proposed protocol is simple yet efficient that provides a level of quality-of-service (QoS), including the important metrics such as delay and security regarding TXs, which are essential in terms of overall performance of the network.

The remainder of the paper is structured as follows. Section II reviews the related works on IoT and IIoT with blockchain. Section III points the design principles of a distributed IoT network framework. The challenges of blockchain integrated IoT network and the overview of the proposed protocol are presented in Section IV. Section V presents the performance evaluation and comparison. Besides, the limitations of the proposed protocol are highlighted in this section. The concluding remarks and future scope are given in Section VI.

II. RELATED WORKS

There are several works have been studied on IoT in industrial automation and blockchain network in the last few years in particular. The authors in [18] proposed a data-oriented machine-to-machine message communication mechanism for IIoT. It deals the requirement of flexibility, efficiency, and compatibility of cross platform in inter-module connectivity among connected devices. The communication latency of IIoT applications has been evaluated in [19]. Here, the authors dealt with estimation latency in transferring data from the

IIoT to the cloud, and vice versa. The authors in [20] presented a secure IIoT and blockchain system by proposing a credit based Proof-of-Work (PoW) mechanism. This can guarantee the security and efficiency of TXs, simultaneously. To protect the data confidentiality, the data authority management is designed to regulate the access to sensor data. In [21], the authors developed a decentralized peer-to-peer platform called BPIIoT for IIoT based on blockchain technology. This enhances the functionality of cloud-based manufacturing platforms. A scalable blockchain protocol for secure metering systems in distributed industrial plants has been proposed to provide the immutable services with strong security, reliability, and guarantee [22].

The authors in [23] proposed a concept of blockchain based logistics and supply chain networks. They addressed the basic concerns, such as overpowering trust issues as well as allowing secure and authenticated system of logistics and supply chain information exchange. The authors in [24] presented a secure and efficient framework for smart home based on blockchain and cloud computing technology. In [25], the authors proposed a blockchain based distributed framework for IIoT. They considered the requirements of automotive industries, such as supply chain management, unparalleled security, evidence integrity and secure storage, mobility solution, and transparency. The authors in [26] suggested a blockchain-based security architecture for IoT framework using SDN concept. They applied the blockchain technology in IoT network in the smart city using fog and edge computing to detect the attacks effectively. Some more research papers have been presented on IoT framework which deal with sustainable IoT for smart home and smart city network [27]–[29].

However, all the works mentioned above are either to integrate blockchain with IoT or IIoT, where the delay of a time-critical TX validation is not taken into consideration that might degrade the QoS of the network. Unlike the exiting works, the proposed CaBNet introduces a context-aware TX validation technique where a time-critical TX is given priority during the validation and hence the delay is minimized.

III. DESIGN PRINCIPLE OF A DISTRIBUTED IoT NETWORK FRAMEWORK

Designing a framework of a blockchain enabled secure IoT network requires to deal with existing and upcoming challenges, and satisfy various service requirements. The proposed CaBNet considers the following design principles.

- **Adaptability:** To adapt with changing requirements of clients or entities, a framework should have scope to improve accordingly without significant changes of the existing system.
- **Accessibility and Fault Tolerance:** A high accessibility of control and operation system is an essential factor. Besides different failure detections, self-healing and mitigation mechanisms are necessary to be ensured.
- **Reliability:** It is the highest priority while designing a distributed framework. This metric is measured using the factors, performance essential and performance achieved by the system in different environmental conditions.
- **Scalability:** Various objectives and features are adding to the IoT based technology with the growth of the applications. The framework should be able to manage current as well as to be adaptive for future extend of new demands without significant impact on the existing system.
- **Security and Privacy:** Actions in counter to known or unknown attacks and data confidentiality are the important metrics that are needed to be ensured through imposing effective mechanisms in the system.
- **Performance:** While the performance of a network comes into consideration, several aspects are taken into account. Different applications require different metrics to achieve the desired performance.

IV. OVERVIEW OF THE CaBNet

A. IoT AND BLOCKCHAIN SYSTEM

The IoT promises to change the existing industrial production procedures by optimizing manufacturing, refining customer experiences, minimizing costs, and enhancing efficiency in enterprises. Besides, it facilitates industrial services and human with seamless connection by providing big data analytic, edge and cloud computing, and development of applications. In the coming years, it will make a significant impact on existing business models in many sectors, such as healthcare, smart grid, manufacturing, agriculture, transportation, retail a name of few. The challenges of the system are in the industrial control system, process control system, and technologies to cyber-attacks.

The blockchain has great potential in Industry 4.0. Blockchain enabled IIoT allows the enterprises to use TXs of crypto-currencies and accountings with a safer and more resilient alternative to deal with shipping and goods. For example, in logistic, it will facilitate the companies keeping records of shipment over several devices with trust and out of manipulation.

B. CHALLENGES OF IoT NETWROK

Providing security is one of the primary challenges of an IoT network. The security parameters have been highlighted and discussed extensively in [21]. The security solutions has a trade-off between security and accessibility. One more key challenge is the verification of integrity of the devices. Generally, applying encryption in communications and firmware is a comparatively complex process. Because, the design limitation of the IoT devices manufactured which has a lack of robust security goal, usually as a cheap to survive. However, the main challenges of an IoT network are as follows:

- **Trust Management:** To ensure this, it is required involving multiple nodes to provide the same service

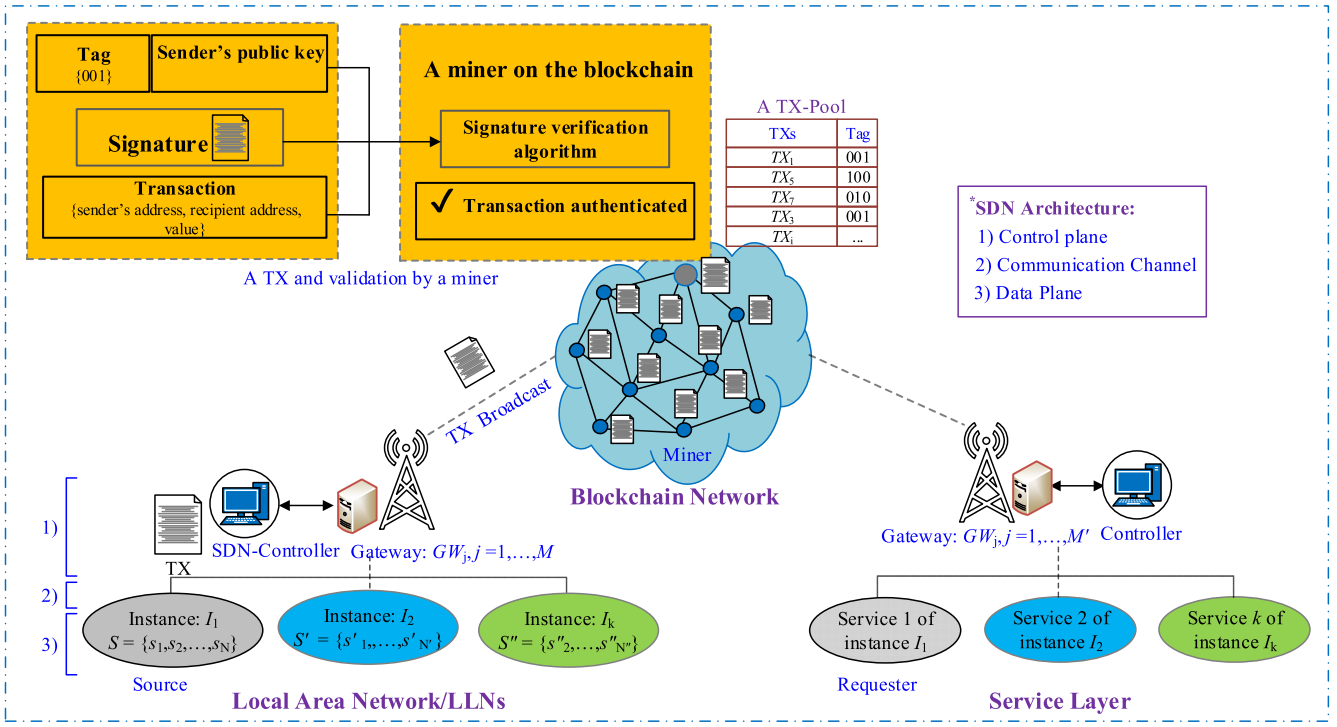

FIGURE 1. Overview framework of the context-aware blockchain-based transaction validation protocol for a secure distributed IoT network (named as "CaBNet").

for redundancy which is a common approach in such applications. The collaboration of the nodes among them to serve a selected purpose is difficult due to the nodes are operated alike in a diverse environment. Measuring reputation of the nodes and share the information to allow them in order to collaborate with most trustworthy counterparts is an effective approach.

- **Secure Communication:** Maintaining secure communication channels among the nodes is important. Due to limited flexibility of the nodes in terms of software customization, a substantial effort is mandatory to use the conventional encryption algorithms in the purpose.
- **Energy Efficiency:** Generally, the IoT applications are implemented where the devices are equipped with on board power batteries. It requires to install the devices with low power consumption, so that the replacement of the batteries are not be frequent. For this, an energy-efficient IoT network design is essential. It includes, the upper layer must play an important role for energy-efficient operations. Although, there are many schemes for energy-efficient operations in WSNs (Wireless Sensor Networks), but those are not appropriate in IoT immediately. As IoT network may contain a multitude of devices, data are sent individually that consumes more energy.
- **Coexistence and Interoperability**: The coexistence of heterogeneous devices with limited spectrum in a closed proximity increases rapidly as increases the connectivity of the IoT. This invokes an imminent challenge in a crowded ISM (industrial, scientific, and medical) band. It is very important to keep less interference between them. This issue can be addressed using software flexibility, cross-technology based communications, and multimode radios.

The proposed CaBNet composed of three layers that are 1) the IoT which contains the sensor devices/LLN called edge or local network, 2) the SDN-GW acts as a middleware between the LLN and the blockchain network, and 3) the distributed blockchain network that consists of miner nodes. The major components of the framework are illustrated in Fig. 1 and discussed in detail subsequently.

C. IoT NETWORK AND ASSUMPTION

An IoT network assumed is comprised of LLNs that access, manage, and manipulate information locally and globally related to different applications (i.e., industrial automation). The standard of the network is defined by IEEE 802.11.4 and Industry 4.0, where the devices are connected via different mediums. The main components of the network are as follows:

1) **Low Power and Lossy Networks (LLNs).** An LLN consists of several to thousands of sensor devices that are installed to collect information and provide services to the clients or entities through a GW/individually. The connections of the devices are usually provided by Wi-Fi, ZigBee, Bluetooth, and so on.
2) **Multiple Instances.** IoT devices and associated data types are varied according to various services. Therefore, the information of different instances are not

Algorithm 1 Routing Protocol

```
start (network in operation)
state (network initialization)
  for each s_i ∈ S do
    Sends (ID, I_k, wI_k, tag_k) Service_k to the GWj
    Updates neighbors list s_i.list = [s_l]
    The GW updates the network topology
  end
state(communications)
  if between (s_i, s_l) or (s_i, GW_j) and s_l, GW_j ∉ [s_l] do
    Collects the rules from the GW
    Sends TX to the GW using the rules
  end
end
```

equally important in terms of QoS. Some services are delay sensitive such as smart healthcare, smart parking a few of them, while some are not. We define the instances $I = \{1,2,3,\ldots, K\}$ of the services of a single or multiple sensors $S = \{s_1, s_2,\ldots, s_N\}$ and weight wI_k corresponding to an I_k along with other information (i.e., *IDs*) that are agreed by a consensus algorithm among the participants joined the network.

D. IoT SDN-GATEWAY (GW)

An SDN-enabled GW plays a role as a middleware in which to connect the LLN and the blockchain network via Internet. The sensors of the instances are registered to the GW using a registration message (REG_MSG) that contains *ID*, I_k, wI_k, and tag_k, of the nodes. On received the messages, the GW lists the *ID*s and the assigned weights according to the various services related to. The subsequent section describes the layers of an SDN architecture in detail. The control and operations of the SDN is given in Algorithm 1.

1) SOFTWARE DEFINED NETWORKING (SDN)

SDN handles largescale and complex mesh network integrated IoT according to the service requirements. It consists of three layers that are 1) the control plane, 2) the communication channel, and 3) the data plane. The layers are to access of information, manage and control the system, and provide necessary security of the network. The layers of the SDN are described subsequently.

a: COMMUNICATION CHANNEL

To communicate between the controller and the SDN-enabled nodes, a common channel is created by using signaling messages (SIGMs) of routing protocols. This mechanism provides communication between the data plane and control plane without any impact on the performance of the network. It also circumvents the obligation of an additional network interface. Besides, several control messages used in this layer are described as follows:

- **RULE_REQ (Rule Request Message):** The communication among nodes which are not listed as neighboring nodes, each node requests for a rule to the controller using this message.
- **RULE_RESP (Rule Request Response Message):** The controller sends this message as a reply to a *RULE_REQ* message that contains the requested rules.
- **LQREQ (Link Quality Request Message):** To measure the level of link quality, nodes send this message to the neighboring nodes.
- **LQREP (Link Quality Request Response Message):** It is used to reply to an *LQREQ* message, so that the requester can measure the link quality between them. The level of link quality between two neighboring nodes is measured based on the expected transmission count (ETX) as in Eq. (1).

$$ETX(s_i, s_j) = \frac{1}{d_{ij}(data) \times d_{ji}(ack)} \tag{1}$$

where $d_{ij}(data)$ and $d_{ji}(ack)$ represent the measured probability that a packet and the acknowledgment is received successfully, respectively.

- **NTUPDT (Network Topology Update Message):** The nodes send their neighborhood nodes' link quality information using this message to the controller. On received the messages, the controller can update the network topology according to the current topology of the network.

b: DATA PLANE

The data plane comprised of two functions that are query for data and request for rules. The given rules are kept in the tables of the nodes and the communications take place according to the rules.

c: CONTROL PLANE

The controller configured at the GW acts as a logical plane. The duty of the controller is to convert the data routing decisions into rules and sending them to the LLN nodes obtaining in the data plane using the SIGM. Along this, it contains the network status and routing mechanism which are defined by the application. The network topology may or may not be included in the routing mechanism to set the rules during communication.

2) ROUTING PROTOCOL

The planes and mechanisms discussed earlier compose of core routing protocol either for single and multihops communication. Although, once the routing protocol is set by the application, the rules are changeable. Someone can modify the protocol as required only by substituting the firmware of the controller. The network performs accordingly.

3) ANOMALY DETECTION

The SDN-GW adopts the Multivariate Correlation Analysis (MCA) algorithm [30] in anomaly detection. MCA is an AI-based feature extraction and analysis technique that distinguishes legitimate and illegitimate data. It is used

to characterize network traffics by using the geometrical associations between the extracted features.

E. BLOCKCHAIN SYSTEM

The blockchain system adopted is ideologically similar to the Bitcoin concept unlike the TX selection for validation process. However, the major components of the blockchain system are described below:

1) **Transaction (TX):** TX is sent between peers. It contains a sender's public key, private key, timestamp, and data. In CaBNet, we adopt adding a tag in the header of a TX according to a service. The data and the control information are hashed through a signature algorithm i.e., secure hash algorithm (SHA256). The priority of a service is defined by a weight which is represented by a tag that is agreed among the participants through a mutual consensus.
2) **TX Validation:** Miner on the blockchain is responsible to validate a TX. For this, a miner selects a TX from its TX-Pool with a priority defined by the rank. The priority of selection for validation is proportional to the rank, it is higher with a higher rank. If there are multiple TXs have the same rank, the priority of the selection will be biased by the time of received. The TX received earlier is verified first. The rank of a TX is calculated in different conditions as follows:

   Condition 1: A TX has weight greater than a threshold weight w_{th} and the number of waiting epochs in the TX-Pool of a miner is equal to 0, the rank of the TX is defined as in Eq. (2).

$$R(TX_i) = \frac{P \times w(TX_i)}{|TXs| \times \left(\sum_{i=1}^{m} w(TX_i)\right)} \tag{2}$$

   where $R(TX_{\text{i}})$ denotes the rank of a TX, P is the percentile of TXs to be selected for validation and added into a new block in a current epoch, and $w(TX_{\text{i}})$ is the weight of a TX according to the assigned tag of a service.

   Condition 2: A TX has weight greater than the w_{th} and the number of waiting epochs in the TX-Pool is greater than 0, the rank of the TX is defined as in Eq. (3). The equation is applicable until its rank is less than or equal to a threshold rank R_{th}. Otherwise, the rank is calculated as in Eq. (5).

$$R(TX_i) = \frac{P \times w(TX_i)}{|TXs| \times \left(\sum_{i=1}^{m} w(TX_i)\right) \times (E_{curr}(TX_i) - E_{in}(TX_i))} \tag{3}$$

   where $E_{\text{in}}(TX_{\text{i}})$ denotes the number of epochs that a TX has been initialized in the TX-Pool of a miner and $E_{\text{curr}}(TX_{\text{i}})$ is the number of current epochs.

   Condition 3: A TX has weight less than or equal to the w_{th} and the number of waiting epochs in the TX-Pool is equal to 0, the rank of the TX is defined as in Eq. (4).

$$R(TX_i) = \alpha \left(\frac{P \times w(TX_i)}{|TXs| \times \left(\sum_{i=1}^{m} w(TX_i)\right)} \right) \tag{4}$$

   where α is an independent weight factor defined by a miner according to the desired QoS of the application and the consensus.

   Condition 4: A TX has weight less than or equal to the w_{th} and the number of waiting epochs in the TX-Pool is greater than 0, the rank of the TX is defined as in Eq. (5).

$$R(TX_i) = \alpha \left(\frac{P \times w(TX_i) \times (E_{curr}(TX_i) - E_{in}(TX_i))}{|TXs| \times \left(\sum_{i=1}^{m} w(TX_i)\right)} \right) \tag{5}$$

   Finally, the rank of a TX is normalized as in Eq. (6).

$$R(TX_i)_{norm} = \frac{R(TX_i)}{Max\ (R(TX_i | i = 1, 2, 3, \ldots, m))} \tag{6}$$

   where $R(TX_{\text{i}})_{\text{norm}}$ denotes the normalized value of the rank of a TX and *Max* is the maximum rank among the TXs in a TX-Pool of a miner.
3) **Block and Blockchain:** A number of validated TXs are added into a new block by a miner. A block is a data packet with a header and a payload. A header contains metadata, such as block ID, hash of the block, hash of the previous block and the timestamp. The payload section contains only the TXs. Once a block is generated, it is broadcasted across the network and is added to the blockchain locally by a miner. A blockchain is an immutable ledger of TXs where the TXs are replicated and recorded as a ledger and distributed among the peers in the network.
4) **Poof of Work (PoW):** Prior to append a block to the blockchain, the recipient miners verify either the newly mined block is valid or not. If valid so it is added to their local blockchain and propagated across the network as well. The miner who added a new block to the blockchain successfully on discovered the nonce will receive the reward according to the application.
5) **Consensus:** It is a mutual agreement among the participants in which TX, validation, block and PoW are executed.
6) **Merkle Tree:** It is one of the fundamental parts of blockchain system and is a data structure that allows for efficient and secure verification of data in order to verify the consistency and content of the data.

   Step 1: A requester sends request for a TX to the blockchain network where the miners are active with high computation and storage of resources.

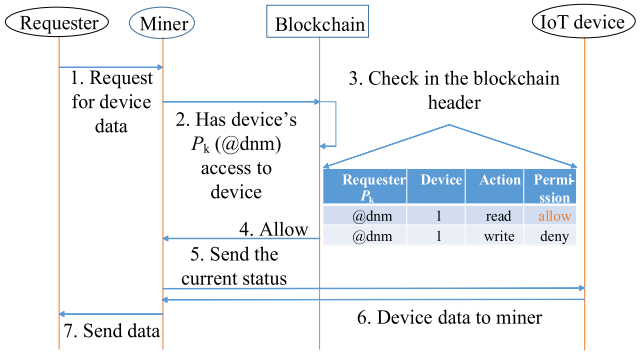

FIGURE 2. Access transaction of CaBNet.

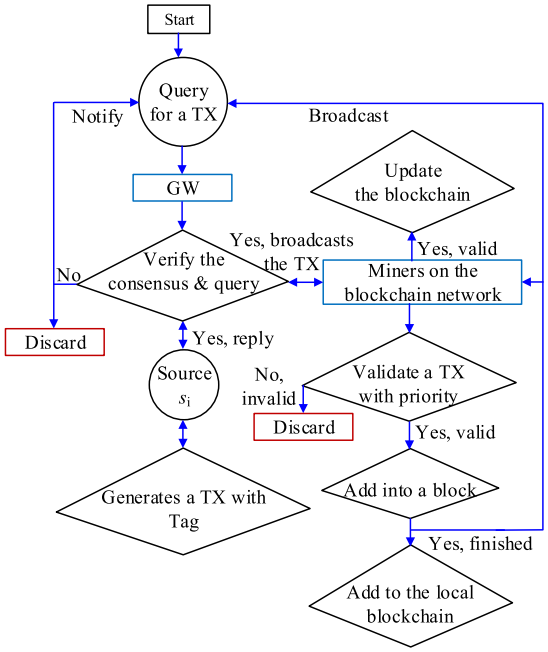

FIGURE 3. Flowchart diagram of CaBNet.

Step 2: A miner checks and verifies whether the TX is authenticated and exists in the blockchain upon received the TX request.

Step 3: The miner checks the requester public key in the blockchain policy header and the permission either request to allow or deny.

Step 4: If the permission is allowed, then the miner make the requested TX available to the requester.

The operations of the CaBNet is illustrated in Fig. 3. The figure shows the necessary operations and logical steps of a TX execution through a validation process by the miners on the blockchain network. The detail of the TX validation and execution is given in Algorithm 2.

V. PERFORMANCE EVALUATION

A network emulator, Common Open Research Emulator (CORE) [31] is used to evaluate the performance of the CaBNet. The emulations run in a system with configuration as shown in Table 1. The blockchain network comprised of 10 nodes as miners and are connected each other.

Algorithm 2 TX-Validation and Execution Using Blockchain

1: **Start** (network in operation)
2: **state** (query for a TX and response)
3: **for** query $q_i(TX_i) \in (Service_K)$ **do**
4: Checks the requester r_j is permitted or not
5: **if** *ID* $(r_j) \in [r_j]$ is permitted **do**
6: Sends the q_i to the GW
7: The GW collects and verify the info of the TX
8: Broadcasts to the blockchain network
9: **else**
10: Discard the q_i
11: **end**
12: **end**
13: **end**
14: **state** (TX-validation and execution)
15: **for** each unconfirmed $TX_i \in TX\text{-}Pool$ of a miner **do**
16: Validates with priority and adds into a block
17: Updates the blockchain
18: The r_i receives the TX and executes
19: **end**
20: **end**

TABLE 1. Setup system.

System	Configuration
Desktop	Intel core i7 @2.8 GHz with 16 GB of RAM
Virtual Machine	VirtualBox
Guest processor	4
Guest memory	8 GB of RAM
Operating system	Windows 10

An LLN of sensor nodes deployed randomly and an SDN-GW are also configured. The miners are responsible for receiving connection request of requesters and LLN nodes via the GW, validating TXs, generating blocks and propagating them to the rest miners. The LLN nodes are connected to the blockchain network via the GW through a registration process. The GW collects TXs from the nodes and sent to the requester using the blockchain network through the series of operations. We assumed the LLN nodes generate TXs with a priority interval of [0,1] corresponding to different services that are sent to the requester using the underneath routing mechanism. The given priority of the generated TXs are agreed and known to all participants (i.e., LLN nodes, GW and miners) by a consensus algorithm.

A. SECURITY AND PRIVACY

Let's assume that an attacker can be any entities in the blockchain system and capable of sniffing communications, generate forged TXs and blocks, modify or remove data in a TX, discard TXs, sign forged TXs to compromise nodes and analyze various TXs prior to legitimate a node. We assume as well that standard secure encryption methods are used among participants [32], so that they are not compromised by any attacker. The CaBNet provides the security regarding the following attack scenarios comes from the blockchain system:

- **Sybil Attack:** An attacker pretends itself as more than one nodes and uses multiple public/private keys as IDs. The CaBNet is resilient counter to this attack as the GW verifies the related information of the initiator of a TX before propagating to the blockchain network. To encounter this, an attacker must need the public/private keys of multiple nodes of valid IDs existing in the network.
- **Modify TXs:** An attacker changes the content of data in a TX. Every generated TX is signed by the initiator prior sending to the blockchain that stored on it. Alerting the data of a TX could be traced by any peer (i.e., GW, miners) through the verification of its signature. An unverified TX is discarded.
- **Malicious Miner:** A legitimate miner continuously receives TXs from nodes. But the miner is not able to change any data in the TXs as the data are signed by the responsible nodes and their private keys are secured.

Besides the conventional attacks on blockchain, Selfish Mining, Race, Majority, and Block-Withhold are also exists [33]. In Selfish Mining, a group of miners increase their revenue unlawfully. A Race attack is performed by injecting two conflicting TXs by an attacker. In Majority attack, majority of the attackers' take control over the network to prevent other miners from completing blocks. The 51% attack where a group of miners control the mining hash rate greater than 50% of the network, is an example of the Majority attack. A Block-Withhold attack is executed when a miner select a valid block not to submit instead discards it. These attacks make the PoW consensus algorithm vulnerable. There are several studies and solution approaches have been proposed. A novel approach [33] regarding the issues can be used in the CaBNet.

The privacy of the CaBNet is intuitive which comes from the public key mechanism similar to other blockchain systems that identifies each participant. In addition, in our framework, each key for each participant is defined by a time bound. Once a participant is reached the expiration time, it regenerates a new key pair.

To analyze the anomaly detection at SDN-GW, the number of attacks flow were varied. The results of dropping packets with respect to attacks is shown in Fig. 4. For this, we used the dataset [34], where the network traffic of different types captured at different locations, such as home network, small office and ISP (Internet Service Provider). Different types of attacks including Denial-of-Service in short DoS and Portscan were considered. The percentage of dropping malicious packets in the proposed model is rapidly increased when the attack flow rate exceeds 250 flows/sec unlike the baseline (the GW without SDN). Fig. 5 shows the Receiver Operating Characteristics (ROC) curve of true positive rate and false positive rate of CaBNet which achieved a higher anomaly detection accuracy.

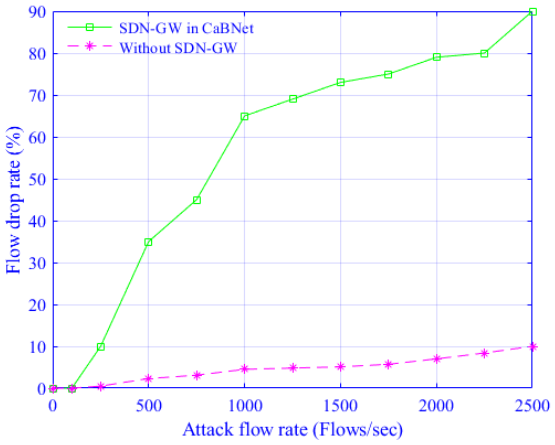

FIGURE 4. Flow drop rate and attack flow rate.

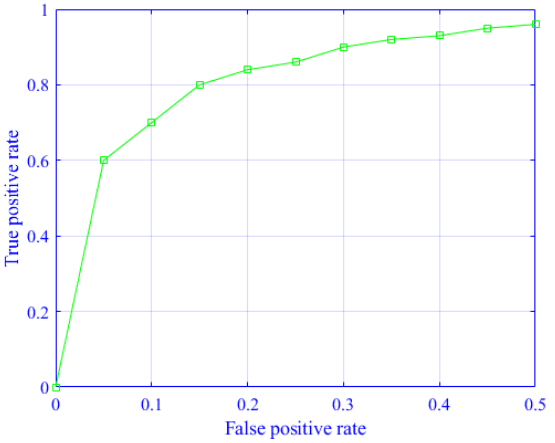

FIGURE 5. ROC curve of detection rate.

B. NETWORK PERFORMANCE

To evaluate the scalability of CaBNet, the number of LLN nodes and their generated TXs were varied. We analyzed the performance in three scenarios. The emulations were conducted over 10 times for each scenario to study the performance of each metric.

We first analyzed the delay of TXs (prioritized and nonprioritized) that are taken by the miners to add into a new block which are randomly requested for various services. We considered, the number of requests of the services are varied according to the nodes, it is increased with increased in the number of LLN nodes (i.e., here 30% different services with given priority). The metric includes the processing of selected TXs, verify data signature, append a TX into a new block, checks the block not expired, and notify other miners on the updates.

Fig. 6 shows an average of maximum delay required a prioritized and nonprioritized TX (randomly selected) by the miners among the (200, 400, 600) TXs generated by the (100, 200, 300) nodes, respectively. The results depict that a prioritized TX obtained less average delay than a nonprioritized TX in the scenarios. It can also be seen that the delay

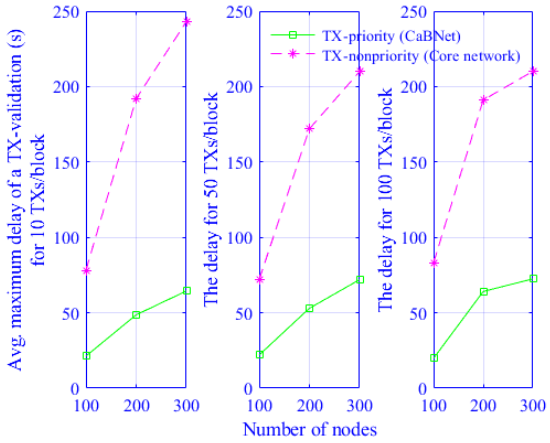

FIGURE 6. An average of maximum required time of added a prioritized and nonprioritized TX into a new block.

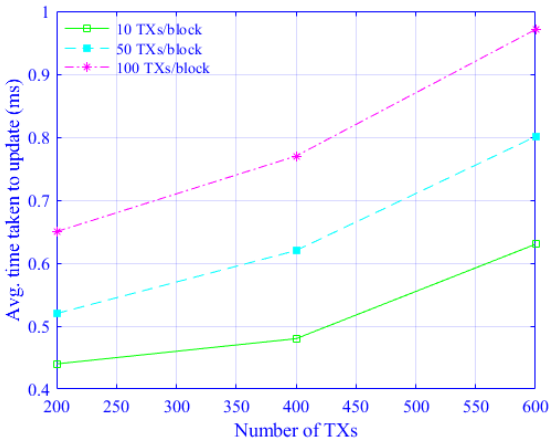

FIGURE 7. Time to update miner's local blockchain with received TXs of CaBNet.

increases with increases in the number of TXs which has a similar impact on the CaBNet and the Core network.

Every TX generated by the nodes is sent to the miners. The integrity and trust of a TX are ensured by them. Once the process is performed by a miner, the miner updates its local blockchain and broadcasts to the rest miners. Fig. 7 shows the time taken to update by a miner. The results depict that the metric increases as TXs increased in a block. Considering a block with (10, 50, 100) TXs respectively, the time increases as TXs increased due to more TXs are processed by the miner.

Time taken by the miner(s) added a new block with a prioritized or nonprioritized TX to the blockchain is also evaluated. It includes receiving request of a connection at the miner, request validation, finding the necessity for a new block and generate, and informing the rest miners as well. Fig. 8 shows an average of maximum delay of a prioritized and nonprioritized TX added to the blockchain successfully. The results state that the delay of a prioritized TX is significantly minimized when compared to a nonprioritized TX. The results also depict that the time increases with increases in the number of TXs and generated blocks due to more TXs and blocks are validated.

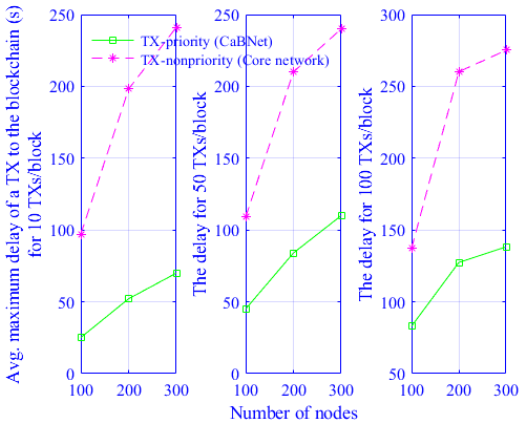

FIGURE 8. An average required time added a prioritized and nonprioritized TX to the blockchain.

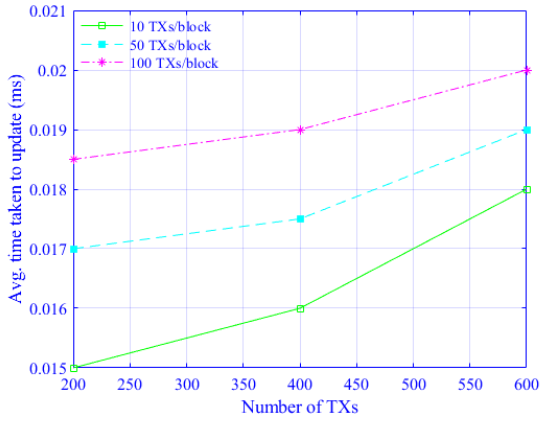

FIGURE 9. Time to update miner's blockchain with received blocks of the TXs of CaBNet.

Time taken by a miner to update a new block by another miner to its blockchain is also evaluated. The average time required to the update is depicted in Fig. 9. The results show that the time differs and varies from (0.015 ∼0.020) ms for the blocks with (10, 50, 100) TXs in the blockchain, respectively.

The LLN nodes are resource constrained, therefore, they only construct the Merkle Tree that contains the information of the blocks (hashes) instead of storing all contents of the blocks in the blockchain. The blocks can be stored elsewhere (i.e., GW). The operations are performed on the TXs. It is estimated that the time varies from (0.105, 0.58, 7.001) ms for a block with (10, 50, 100) TXs, respectively. It is also seen that, the time increased sublinearly as TXs increased within a block.

We also analyzed the impact on the number of services with given priority. For this, the percentile of the services were varied from (0 ∼ 100) % of 600 TXs and a generated block with 100 TXs. Fig. 10 shows, when the number of services with given priority is a less (here 30%), the delay is significantly reduced. It increases with increases in the number of services with priority. Consequently, the average delay of a TX to be added to the blockchain is nearly equal in the system. It states that the lower the services of given

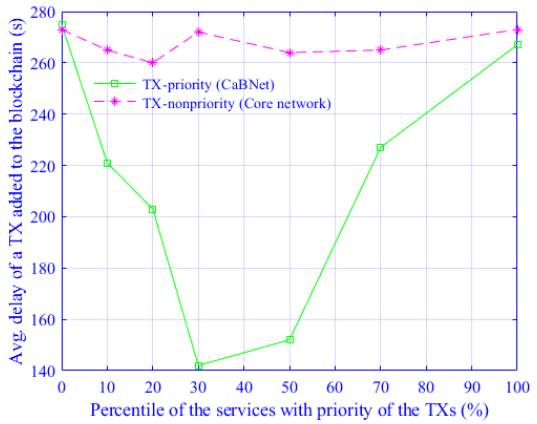

FIGURE 10. An average of maximum required time added a prioritized and nonprioritized TX to the blockchain.

priority, the higher the probability of obtaining less delay of the TXs in CaBNet compared to the Core network.

Limitations. Through this work, we have ideologically designed the CaBNet framework based on the blockchain concept. We assumed that the participants joined the network are agreed upon assigning weights of the TXs through the consensus algorithm where the policy of the assigning weights yet to be designed. Meanwhile, the number of IoT devices, TXs, and the number of miners on the blockchain network considered during the emulation might not be sufficient reflecting the real-time scenarios that may vary in the measured units with unchanged performance of the proposed protocol.

VI. CONCLUSION AND FUTURE WORK

In this paper, a context-aware blockchain-based transaction validation protocol for a secure IoT network is proposed. It provides a delay sensitive time-critical TX validation technique along with the security and privacy solutions. The priority technique adopts a ranking mechanism of a TX to be validated defined by the weight of a service. A higher ranked TX is validated by a miner with a priority in contrast with a lower ranked TX in a TX-Pool. So that the delay of the TX is minimized. Besides, the security and privacy in terms of various vulnerabilities and attacks are taken into consideration that are ensured by the blockchain system and SDN-GW.

The emulations conducted with various parameters, number of IoT devices, transactions generated, and transactions in a block in different scenarios and the performances are evaluated in terms of delay, and security and privacy, in particular. The results show that while the conventional method is not able to provide the QoS of a time-critical TX in terms of the performance metrics, the proposed protocol outperforms. In our future work, the consensus algorithm of the protocol will be included. In addition, we will integrate the artificial intelligence technique into the proposed model to solve problems with uncertain, time-varying, and complex functionalities. To take full advantage of the 5G and beyond network technologies, the proposed model will deepen the analysis and expand to meet the challenges of a smooth deployment for the next generation computing network.

REFERENCES

[1] T. Saarikko, U. H. Westergren, and T. Blomquist, "The Internet of Things: Are you ready for what's coming?" *Bus. Horizons*, vol. 60, no. 5, pp. 667–676, Sep. 2017.

[2] A. S. M. S. Hosen, S. Singh, P. K. Sharma, M. S. Rahman, I.-H. Ra, G. H. Cho, and D. Puthal, "A QoS-aware data collection protocol for LLNs in fog-enabled Internet of Things," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 1, pp. 430–444, Mar. 2020.

[3] Statista. *Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025*. Accessed: Jul. 5, 2019. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[4] J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, and J. Zurek, "On cohabitating networking technologies with common wireless access for home automation system purposes," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 76–83, Oct. 2016.

[5] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann, "Logically centralized?: State distribution trade-offs in software defined networks," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, Helsinki, Finland, Aug. 2012, pp. 1–6.

[6] S. Schmid and J. Suomela, "Exploiting locality in distributed SDN control," in *Proc. 2nd ACM SIGCOMM workshop Hot Topics Softw. Defined Netw. (HotSDN)*, Hong Kong, Aug. 2013, pp. 121–126.

[7] X. Wu, C. Wu, Q. Wu, and B. Wang, "A multipath resource updating approach for distributed controllers in software-defined network," *Sci. China Inf. Sci.*, vol. 59, no. 9, pp. 92301–92326, 2016.

[8] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jun. 10, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] V. Buterin. (2013). *Ethereum, GitHub Repository*. Accessed: Jul. 11, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[10] *BitShares 2.0-Industrial-Grade Decentralized (DPoS) Eco-System on Blockchain*. Accessed: Jul. 11, 2019. [Online]. Available: https://bitshares.org/

[11] Dash. *Dash Crypto Currency-Dash*. Accessed: Jul. 11, 2019. [Online]. Available: https://www.dash.org

[12] Dogecoin. (2013). *An Open Source Digital Currency*. Accessed: Jul. 10, 2019. [Online]. Available: https://dogecoin.com/

[13] Litecoin. (2013). *Litecoin-Open Source P2P Digital Currency*. Accessed: Jul. 11, 2019. [Online]. Available: https://litecoin.org/

[14] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019.

[15] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial Internet of Things technology," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1442–1453, Dec. 2019.

[16] R. A. Memon, J. P. Li, and J. Ahmed, "Simulation model for blockchain systems using queuing theory," *Electronics*, vol. 8, no. 234, pp. 1–19, 2019.

[17] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[18] Z. Meng, Z. Wu, C. Muvianto, and J. Gray, "A data-oriented M2M messaging mechanism for industrial IoT applications," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 236–246, Feb. 2017.

[19] P. Ferrari, E. Sisinni, D. Brandao, and M. Rocha, "Evaluation of communication latency in industrial IoT applications," in *Proc. IEEE Int. Workshop Meas. Netw. (M&N)*, Naples, Italy, Sep. 2017, pp. 1–6.

[20] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[21] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

[22] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "SMChain: A scalable blockchain protocol for secure metering systems in distributed industrial plants," in *Proc. Int. Conf. Internet Things Design Implement.*, Montreal, QC, Canada, Apr. 2019, pp. 249–254.

[23] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART Supply Network*. Cham, Switzerland: Springer, 2019, pp. 21–46.
[24] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–18, 2019.
[25] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2019.
[26] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, Oct. 2019.
[27] S. Singh, P. K. Sharma, and J. H. Park, "SH-SecNet: An enhanced secure network architecture for the diagnosis of security threats in a smart home," *Sustainability*, vol. 9, no. 4, pp. 1–19, 2017.
[28] 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.
[29] 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.
[30] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. Ping Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 447–456, Feb. 2014.
[31] J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, "CORE: A real-time network emulator," in *Proc. MILCOM-IEEE Mil. Commun. Conf.*, San Diego, CA, USA, Nov. 2008, pp. 1–7.
[32] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, pp. 1–18, Apr. 2018.
[33] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Vienna, Austria, Oct. 2016, pp. 1–13.
[34] S. A. Mehidi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*, Menlo Park, CA, USA, Sep. 2011, pp. 161–180.

A. S. M. SANWAR HOSEN received the M.S. and Ph.D. degrees in computer science and engineering (CSE) from Jeonbuk National University (JBNU), Jeonju, South Korea, in 2013 and 2017, respectively. He worked as a Postdoctoral Researcher with the School of Computer, Information, and Communication Engineering, Kunsan National University, Gunsan, South Korea, and with the Division of CSE, JBNU. He is an Assistant Professor (research) with the Division of CSE, JBNU. He has published several articles in journals and international conferences, and serves as a Reviewer of several reputed journals. His research interests are in wireless sensor networks, the Internet of Things, network security, data distribution services, fog-cloud computing, artificial intelligence, blockchain, and green IT.

SAURABH SINGH received the bachelor's degree from Utter Pradesh Technical University, the master's degree in information security from Thapar University, and the Ph.D. degree from Jeonbuk National University, carried out his research in the field of ubiquitous security. He held a postdoctoral position at Kunsan National University, South Korea. He has experience of being a lab leader. He holds a strong academic record. He is working as an Assistant Professor with Dongguk University, Seoul, South Korea. He has published many SCI/SCIE journal articles and conference papers. His research interests include blockchain technology, cloud computing and security, the IoT, deep learning, and cryptography. He is the Reviewer of the IEEE Internet of Things (IoT) Journal, IJCS, IEEE Access, FGCS, *The Journal of Supercomputing*, IJDSN, COMPELECENG, and many other journals. He received the Best Paper Award from KIPS and CUTE Conference, in 2016.

PRADIP KUMAR SHARMA (Member, IEEE) received the Ph.D. degree in computer science and engineering (CSE) from the Seoul National University of Science and Technology, South Korea, in August 2019. He worked as a Postdoctoral Research Fellow of the Department of Multimedia Engineering, Dongguk University, South Korea. He was a Software Engineer at MAQ Software, India, and involved in variety of projects, and proficient in building largescale complex data warehouses, OLAP models, and reporting solutions that meet business objectives and align IT with business. He is an Assistant Professor in cybersecurity with the Department of Computing Science, University of Aberdeen, U.K. He has published many technical research articles in leading journals of the IEEE, Elsevier, Springer, and MDPI. Some of his research findings are published in the most cited journals. He has also been invited to serve as the Technical Programme Committee Member and the Chair of several reputed international conferences such as the IEEE ICC 2019, the IEEE MENACOMM 2019, and 3ICT 2019. He received a Top 1% Reviewer of computer science by Publons Peer Review Awards, in 2018 and 2019, and Clarivate Analytics. His current research interests include cybersecurity, blockchain, edge computing, SDN, SNS, and the IoT security. He has been an Expert Reviewer of the IEEE Transactions, Elsevier, Springer, and MDPI journals and magazines. He has been serving as a guest editor for international journals of certain publishers such as Springer, MDPI, and JIPS. He is currently an Associate Editor of *Human-Centric Computing and Information Sciences* (HCIS) and the *Journal of Information Processing Systems* (JIPS).

UTTAM GHOSH (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical engineering from IIT Kharagpur, India, in 2013. He has a postdoctoral experience at the University of Illinois at Urbana–Champaign, Fordham University, and Tennessee State University. He is working as an Assistant Professor of Practice with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA. He has published fifty articles in reputed international journals including the IEEE Transactions, Elsevier, Springer, IET, Wiley, InderScience, and IETE, and in top international conferences sponsored by the IEEE, ACM, and Springer. His main research interests include cybersecurity, computer networks, wireless networks, information centric networking, and software defined networking. He has served as a Technical Program Committee (TPC) Member of renowned international conferences, including ACM SIGCSE, the IEEE LCN, IEMCON, STPSA, SCS SpringSim, and the IEEE COMPSAC. He is a member of AAAS, ASEE, ACM, and Sigma Xi. He has conducted several sessions and workshops related to cyber-physical systems (CPS), SDN, the IoT, and smart cities, as the Co-Chair of top international conferences including the IEEE GLOBECOM, MASS, SECON 2019, CPSCOM 2019, IEMCON 2019, ICDCS 2017, and so on. He is actively working on editing two edited volumes on *Emerging CPS, Security, Machine/ Machine Learning* (CRC Press), a Chapman Hall Big Data Series. He is contributing as a Guest Editor for special issues of the IEEE Transactions on Network Science and Engineering, *ACM Transactions on Internet Technology* (TOIT), MTAP (Springer), and ITL (Wiley).

JIN WANG (Senior Member, IEEE) received the B.S. and M.S. degrees from the Nanjing University of Posts and Telecommunications, China, in 2002 and 2005, respectively, and the Ph.D. degree from Kyung Hee University, South Korea, in 2010. He is currently a Professor with the Changsha University of Science and Technology. He has published more than 400 international journal articles and conference papers. His research interests mainly include wireless sensor networks, and network performance analysis and optimization. He is a member of the ACM.

IN-HO RA (Member, IEEE) received the M.S. and Ph.D. degrees in computer engineering from Chung-Ang University, Seoul, South Korea, in 1991 and 1995, respectively. From 2007 to 2008, he was a Visiting Scholar with the University of South Florida, Tampa. He is currently a Professor with the School of Computer, Information, and Communication Engineering, Kunsan National University, Gunsan, South Korea. His research interests include wireless *ad-hoc* and sensor networks, cross-layer network protocol, cognitive radios, PS-LTE, and the IoT.

GI HWAN CHO received the B.S. degree in computer science from Chonnam University, Gwangju, South Korea, in 1985, the M.S. degree in computer science from Seoul National University, Seoul, South Korea, in 1987, and the Ph.D. degree in computer science from The University of Newcastle, Newcastle Upon Tyne, U.K., in 1996. He worked with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea, as a Senior Member of Technical Staff, from September 1987 to August 1997, and with the Department of Computer Science, Mokpo National University, Mokpo, South Korea, as a full-time Lecturer, from September 1997 to February 1999. In March 1999, he joined the Division of Computer Science and Engineering, Jeonbuk National University, Jeonju, South Korea, and he is currently serving as a Professor. His current research interests include mobile computing, computer communication, security on wireless networks, wireless sensor networks, and distributed computing systems.