Hindawi
Mobile Information Systems
Volume 2020, Article ID 8831976, 13 pages
https://doi.org/10.1155/2020/8831976

Research Article

Rogue Device Mitigation in the Internet of Things: A Blockchain-Based Access Control Approach

Uzair Javaid,[1] Furqan Jameel,[2] Umair Javaid,[3] Muhammad Toaha Raza Khan,[4] and Riku Jäntti[2]

[1]*Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583*
[2]*Department of Communications and Networking, Aalto University, Espoo 02150, Finland*
[3]*IREC/MIRO and ICTEAM UCLouvain, Avenue Hippocrate 54, Brussels 1200, Belgium*
[4]*Kyungpook National University, Daegu 41566, Republic of Korea*

Correspondence should be addressed to Furqan Jameel; furqan.jameel@aalto.fi

Received 16 July 2020; Revised 12 August 2020; Accepted 9 October 2020; Published 28 October 2020

Academic Editor: Zengpeng Li

Recent technological developments in wireless and sensor networks have led to a paradigm shift in interacting with everyday objects, which nurtured the concept of Internet of Things (IoT). However, low-powered nature of IoT devices generally becomes a hindrance that makes them vulnerable to a wide array of attacks. Among these, the emergence of rogue devices is quickly becoming a major security concern. Rogue devices are malicious in nature which typically execute different kinds of cyberattacks by exploiting the weaknesses of access control schemes in IoT environments. Therefore, access control is one of the crucial aspects of an IoT ecosystem that defines an entry point for a device or a user in the network. This paper investigates this issue and presents an access control scheme by integrating an IoT network with blockchain technology, thereby arguing to replace the traditional centralized IoT-server architecture with a decentralized one. The blockchain is used with smart contracts to establish a secure platform for device registration. Due to this reason, the IoT devices are first required to register themselves and access the network via contracts thereafter. Moreover, the contracts host a device registry, the access control list, to grant or deny access to devices. This allows the proposed scheme to authorize registered devices only and block unregistered ones, which facilitates the mitigation of rogue devices. To demonstrate the feasibility and improvements of the proposed scheme, security analysis along with in-depth performance evaluation are conducted, where the obtained results indicate its applicability. A case study is also formulated with a comparative analysis that confirms the superior performance of the proposed scheme for low-powered IoT systems.

1. Introduction

In recent years, Internet of Things (IoT) has gathered substantial popularity and wide acceptance for low-powered communication among devices [1, 2]. The IoT networks enable connectivity of physical devices via the Internet that can operate, communicate, and actuate autonomously to provide innovative services in a wide array of applications [3]. It is expected that, by the end of the year 2020, almost 50–100 billion devices will be connected to the Internet [4]. These devices would require unconventional and dynamic methodologies to support ultrareliable low-latency communication (URLLC) and enhanced mobile broadband (eMBB) services [5, 6]. Furthermore, there would be a need for novel security mechanisms to ensure the integrity and authenticity of the data.

The interconnection of such a sheer number of devices will inevitably introduce security issues into an IoT-based system as IoT devices are generally resource-constrained in memory, energy, and computational resources, which exacerbate the architectural and security challenges of IoT [7, 8]. To cope with the security issues of IoT networks and prevent future network breaches, several approaches and solutions have been proposed. For instance, some key exchange schemes have been proposed to provide resilience against different kinds of attacks, where key management is

concerned with the generation, storing, and exchange of the keys. Moreover, mechanisms like authentication provide resistance against man-in-the-middle (MITM) and impersonation attacks [9, 10].

With the rise of Bitcoin and cryptocurrency in general, the concept of distributed blockchain databases has received significantly wider attention. This is because a wide range of distributed applications can be built based on the distributed infrastructure of blockchain. One unique variant in this regard is the Ethereum blockchain platform, which includes a Turing-complete programming framework with system state information to realize the so-called smart contracts [11]. Furthermore, the blockchain facilitates a resilient and highly distributed ledger for recording transactions, attributing them to a specific node in a network, and ordering them relative to time. This phenomenon is made possible through a process known as mining, whereby a large number of dedicated high-powered computers running application-specific integrated circuits (ASICs) process the transactions in real time. The miners compete with each other for a small fee in addition to a subsidy in the form of a cryptocurrency or token. Moreover, data is permanently recorded in the blockchain network through a data structure called blocks. Thus, a ledger of past transactions is called the blockchain as it is a chain of blocks that serves to confirm the transactions to the rest of the network [12].

Security protocols in IoT networks are still in a primitive stage and only make use of HTTP, MQTT, and XMPP protocols for routing the messages [13]. With blockchain technology, the issues of key distribution and management are completely solved due to the global unique identifier (GUID) of each IoT device. This would eliminate the handshake procedures and exchange of PKI certificates for communication among IoT devices, thus, leading to a smoother communication experience. Blockchain technology in IoT networks acts as a tool to execute a system of contracts focused on the application of value exchange [14]. Furthermore, there is a multitude of applications that can be run alongside, or in conjunction with, the blockchain-enabled IoT networks, which takes advantage of the large amount of computing power or computational effort generated by the dedicated mining machines. In the next section, we review some of the recent literature in the domain of blockchain-enabled IoT networks.

1.1. Literature Review. Research in IoT has recently received worldwide attention such that [7] highlights various challenges in IoT environments and identifies the following avenues for future research directions: architecture and dependencies, creating knowledge and big data, robustness, scaling, privacy, human-in-the-loop, and security in particular. This is because dealing with security attacks is one of the major problems that are prevalent on the Internet [13]. This is deeply problematic for IoT since its operation depends on the Internet connectivity. Moreover, we can define a blockchain as an online and distributed ledger that primarily consists of a list of blocks. Each block is an ordered record of application relevant data and a hash of the preceding block. This enables a system to achieve transparency in its operation and makes a blockchain highly resistant to data tampering. To achieve synchronization of the ledger, different consensus algorithms are used for sharing control across the blockchain network. This contributes to overall increased robustness. Therefore, many applications have adopted it to provide trust-free and decentralized solutions.

The authors of [14] provide a survey of existing blockchain-enabled IoT solutions for permission-less trading in the network. In another work [15], the authors propose a secure signing mechanism for ensuring the integrity of data. The proposed solution makes use of hash-based signing which is more efficient when compared to the existing approaches. The study in [16] proposes SMACS, which is a smart contract access control service. SMACS offloads the burden of expensive access control validation and management operations to an off-chain infrastructure, while only implementing the lightweight token-based access control on a blockchain. Moreover, healthcare is quickly adopting new technologies like artificial intelligence to automate the different modules in a standard clinical workflow for radiation oncology [17, 18]. However, machine learning models are data demanding meaning that abundant data is required for optimal learning, where well-annotated medical data is scarce [19]. In a typical setting, data is collected at a single/different institute(s) and subsequently shared with others as per collaboration agreement. This traditional approach of data sharing is time consuming as it normally requires a centralized database, which is created and maintained by the host institute. Data sharing using blockchain can address this problem. The authors of [20] perform similar studies for private blockchain networks. More specifically, a practical byzantine fault tolerance protocol is proposed. This is an efficient protocol that allows devices to operate even if 33% of the nodes are honest while the rest 66% of nodes become rogue or malicious. The authors of [21] propose a novel approach called Enigma. It is a decentralized platform for guaranteeing the integrity and security of the collected data. The sensitive information in Enigma is stored in an off-chain database with strong encryption that mitigates the impact of cyberattacks. Similarly, a blockchain-based consent model for health data sharing platforms is also discussed in [22].

For smart home applications, the authors of [23] propose a new IoT authorization stack protocol in which the devices are connected to the cloud for exchanging commands with a mobile user. The proposed solution addresses the security leakage issues in an untrusted cloud communication architecture. In a similar work [24], the authors focus on the centrality of blockchain nodes to manage and monitor the IoT devices. Some interesting proposals for private blockchain networks are also provided in [25, 26], wherein the authors created a threat model for evaluating the security protocols. They demonstrated that the intrusion detection systems based on techniques like anomaly behavior analysis can prove quite useful against cyberattacks in IoT networks. Following the same approach, the authors of [27] point out different vulnerabilities and provided solutions for IoT networks.

To ensure the security and integrity of IoT networks, the authors of [28] provide a proof-of-concept implementation of a distributed ledger technology. This was done on multiple Raspberry Pi devices connected to the network in a realistic communication environment. An unclonable solution (used in key management and generation) for low-powered IoT devices and vehicular networks is proposed by [29–31]. Later, an extension of the same was provided in [32, 33], which eliminated the high-cost process of key generation. Quantum security solution for distributed ledger technologies has also been explored in [34]. They propose a one-time signature for reducing the signature time cost and size by 75% and 76%, respectively. The security issues of blockchain-enabled IoT networks for industry 4.0 have also been considered by many studies [35–37], in which different integration challenges and recommendations were highlighted by the authors.

1.2. Motivation and Contribution. To help solve and address the aforementioned limitations, we propose a blockchain-based access control scheme for IoT that works in conjunction with smart contracts and achieves distributed and trustworthy access control in an IoT system. Blockchain is used to provide a device registration mechanism via its Public Key Infrastructure (PKI) framework as well as for distributing the control within the network, while smart contracts are used to implement the access control functions with Access Control List (ACL). Moreover, a higher computing capability with lower computation cost for establishing the access control methods is achieved by using smart contracts as opposed to [38–40]. In this backdrop, our work employs blockchain technology for providing access control in IoT networks. More specifically, this paper introduces a scheme for decentralized IoT access control. This is established by integrating the traditional device-to-server communication infrastructure with blockchain and smart contracts. To summarize, the blockchain offers a safe and secure device registration mechanism with its PKI, while the smart contracts enforce the access control functions by using an ACL mechanism. Thus, this paper makes the following contributions to the state of the art:

(i) A novel blockchain-based decentralized IoT access control scheme is proposed. The proposed scheme makes use of the registration platform to register or remove a device in the network.

(ii) The ACL mechanism is designed to authorize registered devices only. The integration of ACL mechanism with the proposed scheme mitigates the impact of rogue devices in an IoT network.

(iii) A comprehensive analysis with a state-of-the-art blockchain-based IoT access control scheme is provided. The results demonstrate the feasibility and superior performance of the proposed scheme.

1.3. Paper Organization. The remainder of the paper is organized in the following way. Section 2 describes the IoT-blockchain model while Section 3 explains its operation. Section 4 presents the security analysis of the proposed scheme. Section 5 details its performance evaluation along with its relevant discussion and a comparative analysis. Finally, Section 6 presents the concluding remarks with potential directions for future research.

2. IoT-Blockchain Model

This paper presents a blockchain-based access control scheme for IoT that operates in conjunction with smart contracts. The scheme is based on Ethereum [41], a variant of blockchain technology that allows decentralized applications (DApps) to be built atop blockchain along with their corresponding states, which is composed of objects called accounts that have the following fields [41]:

(i) A 20-byte address (i.e., ID)

(ii) A smart contract code that may be empty

(iii) A balance of Ether used to pay transaction fees

(iv) A nonce so that each transaction is processed only once

Furthermore, a state in Ethereum refers to the current data present in the blockchain, whereas a state transition occurs whenever a transaction occurs. Additionally, there are two types of accounts in Ethereum:

(a) Externally owned account (EOA): these are user accounts managed with PKI

(b) Contract: this is a computer program, and its corresponding account has its code and is controlled by the same

Furthermore, by sharing data across the blockchain and committing transactions, the smart contracts can be executed in a decentralized manner. This adheres to their integrity and enables their transparent execution. Besides, there exists a gas limit for each transaction and process within Ethereum, where gas is an analogous word for "resource," i.e., a certain amount of gas for a function means that its execution has that much of resource to use. Therefore, IoT devices have to use very negligible amounts of gas for their operation. It can be interpreted as a cost factor for the IoT devices but it also ensures security by limiting the devices to generate only as many requests as the amount of gas that they have [42].

2.1. Network Model. As shown in Figure 1, the IoT-blockchain model consists of seven core components. Thus, the details of these components are provided herewith:

(1) *Server*. It represents a device or a set of devices that is responsible for providing different kinds of services to users and devices of the IoT-blockchain network. Moreover, the server is the host of the IoT-blockchain network; i.e., it initiates a blockchain with the first block but instead of being centralized, servers are decentralized here. This way, the servers act as the trusted hosts since they hold the genesis block that is trusted by all users and devices in the network.

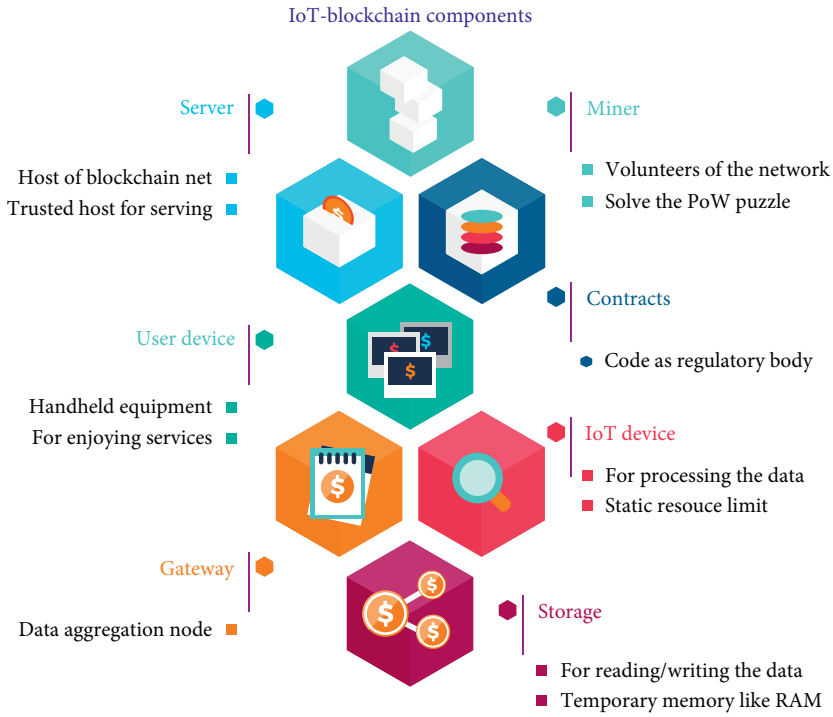

Figure 1: An overview of the IoT-blockchain model and its core components.

Moreover, they may employ permissionless or permissioned consensus protocols to enable interactions between them and the network constituents that include and are not limited to collecting data, processing, querying data from, and/or writing data to storage devices.

(2) *Miner*. It represents the volunteers of the IoT-blockchain network, i.e., miners. They are mainly responsible for solving the PoW puzzles and mine new blocks. Thus, they provide the computing power required by the proposed scheme to operate.

(3) *Smart Contracts*. It represents the computer programs or codes that act as the regulatory bodies in the proposed scheme, i.e., the smart contracts. They enforce the access control functions and host the ACL. Thus, they are responsible for registering and removing devices as well as authorizing them. This way, they can block rogue devices and mitigate their impact.

(4) *User Device*. This represents user setups that include and are not limited to PCs, laptops, and smartphones. A user can conveniently check and enjoy the services provided by the servers in the network using these devices, as well as read data from or write to the storage devices of the network.

(5) *IoT Device*. This represents the things, i.e., devices that are responsible for sensing, processing, and communicating data to the server via gateways. They may also read data from or write to a storage device as well as send control signals to actuators which in turn may operate another device.

(6) *Gateway*. This represents the service agent for IoT devices in the network. The devices can use the gateways for communication; i.e., it provides network connectivity to them via short-range communication technologies and protocols such as Bluetooth, Wi-Fi, and Zigbee. Moreover, a gateway may also provide additional functionalities such as data aggregation and specific security features. Thus, different gateways may be used for different types of devices or a single gateway can also be used for a range of devices, thereby, forming a device cluster.

(7) *Storage*. It represents the reading and/or writing processes of data to storage devices, which may be permanent like read-only memory (ROM) or temporary like random-access memory (RAM). Thus, different data types (e.g., JSON, XML, CSV, etc.) can be written on them such that they can be used by other devices in the network.

2.2. System Assumptions. The proposed scheme uses the following system configurations and assumptions:

(i) The scheme uses a proof-of-work (PoW) consensus algorithm for its operation.

(ii) All peers (servers/miners) have a blockchain account that allows them to claim a deployment instance of a smart contract during system initialization and, subsequently, identify themselves as the trusted hosts.

(iii) An adversary/a group of adversaries cannot compromise the blockchain such that peers are not

resource-constrained and control more than 50% of the total computing power.

(iv) Elliptic Curve Cryptography (ECC) with the Elliptic Curve Digital Signature Algorithm (ECDSA) is used to generate the account addresses (IDs) for both IoT devices and peer nodes.

(v) Gateways act as the agents of IoT devices and are responsible for storing their accounts. It is assumed that gateways are physically accessible as well as secure, which makes them unlikely to be compromised. Thus, they can be trusted as agents.

(vi) All peer nodes are assumed to be synchronized on the same blockchain block.

2.3. Threat Model. We consider a threat model where the objective of an adversary is to compromise the proposed access control scheme by exploiting a security loophole and gain unauthorized access into the system with his/her rogue device(s), which are just plain malicious in nature by definition. Note that the loophole can include endpoint vulnerabilities, malfunctioning hardware, and "bring your own device" (BYOD). Thus, by compromising the system with weak access control setup, the adversary intends to execute different kinds of cyberattacks on the system, which may include impersonation, resource depletion, sinkhole, denial of service (DoS), distributed DoS (DDoS), birthday, and spoofing. This presents serious security implications: if an adversary successfully enters into a system, he/she can target its specific components to steal information or disrupt the network operations, or in rare cases, permanently damage the whole system. Therefore, effects of rogue devices and devices exhibiting rogue behavior must be mitigated.

3. Blockchain-Based IoT Access Control Scheme

The proposed scheme uses ECDSA for generating distinctive IDs for IoT devices and the peer nodes. The smart contracts maintain the ACL and can differentiate between registered and rogue devices. Thus, with the ACL mechanism, each device is required to first register itself with the network using its ID, which is handled through gateways. The registration process will generate a unique ID for each device, which can be used to interact with other devices or peers. These interactions are enabled by the contracts by using ACL. Note that the contracts are hosted by the nodes that deployed them, i.e., peers. Thus, the smart contracts act as the regulatory bodies of the scheme and are responsible for facilitating secure communication between devices and peers. For this purpose, the contracts provide the following ABIs:

deviceAdd: it functions to register a new device using its ID and store it in the ACL. Note that the ID here represents the 20-byte address of the IoT device which is used by this ABI to list the device name in ACL.

deviceDelete: it functions to rescind the access of a device by removing it from the ACL. Similar to deviceAdd ABI, it also requires the 20-byte ID of the device to match against the ACL and remove it thereafter.

sendMessage: this is the enabler of communication with smart contracts. It functions to fetch and return the address of a contract to a device; i.e., if a device wants to send a message, it needs to interact with a contract instance in the network via this ABI.

accessControl: it is the core ABI that is responsible for authorizing and blocking devices with the application of ACL. For this purpose, it first checks if a device is registered in the ACL. Thus, whenever a device calls this ABI to authorize its current access request, it will start the validation process to check the validity of the request according to Algorithm 1, where access$(d_s[n])$ is the access control routine of contracts, request$(d_s[n]$.node$)$ represents a message generated by an IoT device (subject), d_s represents a set of subjects, and ACL is the access control list hosted by the contracts. Thus, this ABI allows the requests of registered devices only and blocks rogue ones, thereby, limiting their impact.

It is worth noting here that only the smart contract creator can add, delete, or update the definitions of these ABIs. Therefore, access control permissions must be carefully considered while designing them.

3.1. Mining Operation. To handle the requests (we refer to them as transactions) generated in the IoT-blockchain network, miners (block producers) need to generate blocks efficiently with the optimal time cost. Therefore, they need to complete the following steps: (i) collect, verify, and combine the transactions into a block and mine it; (ii) broadcast the mined block to reach a consensus in the network and append it to the blockchain as the latest block.

We now formulate the miners in our proposed scheme. Let us assume that there are N peer nodes and M miner nodes in the network, where peer nodes represent both miners and servers. Moreover, the set of peer nodes is represented by $\mathcal{N} = \{n_1, n_2, \ldots, n_N\}$, where the computing power of node n_n, $n = 1, \ldots, N$ is represented by Υ_n, respectively. Note that $\Upsilon = \{\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_n\}$ is used here to represent the set of computing power of the network. Thus, M miners represented by $\mathcal{M} = \{m_1, \ldots, m_m, \ldots, m_M\}$, $\mathcal{M} \subseteq \mathcal{N}$, are selected out of $\mathcal{N}$ nodes.

3.2. Degree of Decentralization. This paper introduces a novel way to measure the degree of decentralization in the proposed scheme by using Gini coefficient (G); it is well studied as a measurement for inequality of wealth or income [43]. Due to its accuracy in evaluating inequality, G has been employed in many fields that include and are not limited to capturing contrast intensity [44], system fairness [45], and resource difference degree [46]. For further details on G, we direct the reader to Appendix A. Thus, we measure the decentralization of our scheme by considering the distribution of computing power among the miners. To formulate

Function: access($d_s[n]$)
Input: request($d_s[n]$.node)
Output: allow, block
(1) **while** Input **do**
(2) **for** n in $d_s, d_s \in S \forall n = 1, \ldots, s$ **do**
(3) **if** $d_s[n]$.node is in ACL **then**
(4) allow
(5) **else**
(6) block

Algorithm 1: Establishing access control policies with smart contracts.

this, G for miners with respect to (w.r.t.) computing power distribution can be calculated by in the following way:

$$G(\Upsilon) = \frac{\sum_{m_i \in \mathcal{M}} \sum_{m_j \in \mathcal{M}} \left| \Upsilon_i - \Upsilon_j \right|}{2 \sum_{m_i \in \mathcal{M}} \sum_{m_j \in \mathcal{M}} \Upsilon_i} = \frac{\sum_{m_i \in \mathcal{M}} \sum_{m_j \in \mathcal{M}} \left| \Upsilon_i - \Upsilon_j \right|}{2M \sum_{m_i \in \mathcal{M}} \Upsilon_i}, \tag{1}$$

The values of G are within the range $[0, 1]$, where 0 denotes full decentralization while 1 denotes the opposite (full centralization), respectively. Using this formulation, we can observe that the more uniform or decentralized the distribution of computing power is, the closer G is to 0. Figure 2 describes the decentralization performance of the proposed IoT-blockchain scheme. Different from [47], where decentralization performance of a blockchain is measured by the number of miners, a more general metric, G, is used here to capture the degree of decentralization w.r.t. the computing power distribution among miners. It can be seen from the figure that as the threshold of G decreases, the Lorenz curve gradually approaches the line of ideal decentralization, thereby, making the blockchain more decentralized. Note that Lorenz curve details are given in Appendix A. This demonstrates that G is an effective metric that can be used to measure the decentralization degree of blockchain-based systems. Similarly, G can also be calculated for other aspects of a blockchain quantitatively.

4. Security Analysis

This section presents the security analyses of the proposed scheme by discussing the following factors.

4.1. Distributed Servers. Traditional IoT systems primarily rely on a centralized cloud server that is responsible for managing IoT devices and handling the majority of the computation and decision operations. Although a cloud server may in reality be replicated for authentication and decision processes, the system can still be considered as a single entity. This presents us with a serious security concern; i.e., the whole system can be potentially compromised if an adversary gains access to the server. Thus, the proposed scheme eliminates this concern by distributing the computation resources among miners. This results in high-security fidelity and enables a system to continue operation even if one or more of its peers cease to operate. Moreover, by distributing the computation in this manner, the resources required by a server can be relaxed. This will likely result in a situation where adversaries will consume mainly their resources to perform any malicious activity or attack.

4.2. Trust-Free System Operation. A typical IoT system operates on trust which is normally established via third parties that work as the middlemen between the devices and the server. These third parties have their associated costs in terms of labor and latency, where centralized IoT systems have to pay as trust a key security requirement for reliable network operation. The proposed scheme eliminates this reliance since it does not require any intermediary to guarantee its operation [48]. Moreover, a PoW distributed consensus protocol is used instead, which allows the network to reach consensus, and, thus, trust-free system operation is realized.

4.3. Rogue Device Mitigation. A conventional IoT system usually lacks a device registration mechanism for effectively handling the devices. By using the ACL mechanism in the proposed scheme, the smart contracts authorize each device whenever they generate a request. Thus, when a device sends a message, it is checked against the ACL and granted access only if it is registered in it. This way, the proposed scheme can establish a defense mechanism against rogue devices and, therefore, mitigate their impact on the IoT-blockchain system.

4.4. Shorter Key Lengths. The authenticity of messages in the proposed scheme is guaranteed via digital signatures by using ECDSA [49]. This ensures data integrity; i.e., data can be sent by registered devices only. For its feasibility, we present a comparison between ECC, Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), and Diffie–Hellman (DH) in Table 1 [49, 50]. We can observe that for an 80-bit strength of a system's security, ECC needs only 160 bits while all of the other algorithms need 1024 bits. Similarly, for a 256-bit strength, ECC needs 521 bits compared to 15360 bits needed by the others. This proves that ECC needs shorter key lengths when compared with the other cryptographic algorithms to achieve similar security strength levels. This helps reduce the overhead in our scheme as smaller key lengths translate into lower computational overhead [51].

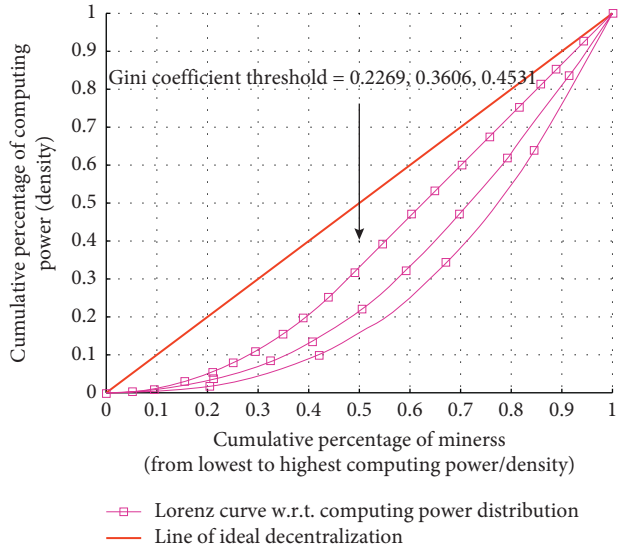

Figure 2: Quantifying the degree of decentralization performance of miners in a blockchain-enabled IoT network. The Gini coefficient here signifies how the distribution of computing power is made among the miners, i.e., whether it is in a centralized or decentralized manner. It can be seen that as the coefficient increases, the performance worsens and is more inclined towards centralization.

Table 1: Security strength comparison of key size combinations for various cryptographic algorithms.

Security	Key size (bits)			Ratio
	Symmetric encryption algorithm	ECC	RSA/DH/DSA	
80	Skipjack	160–223	1024	
112	3DES	224–255	2048	
128	AES-128	256–383	3072	1:6–30
192	AES-192	384–511	7680	
256	AES-256	512–more	15360	

4.5. Blockchain Robustness. The quintessential factor of our scheme is the employment of blockchain technology in it. Therefore, it is of paramount importance to guarantee its security. For this purpose, let us consider a case where an adversary A tries to create a dishonest chain faster than the honest chain. Note that the honest chain is hosted by the honest miners in the proposed scheme and we assume that they always control more than 50% of the total computational resources. Moreover, we say that A wants to catch up with the honest chain (we say i blocks behind) and, therefore, be able to invalidate it with his/her dishonest chain. Thus, the probability that A catches up from i blocks behind the honest chain is analogous to a Gambler's Ruin problem. Let us consider a player who starts to play with unlimited credit at a given deficit. The player potentially plays an infinite number of trials and tries to reach a breakeven point. Then, the probability that A ever reaches breakeven, or in other words, that A ever catches up with the honest chain can be represented as [49]

$$Q_i = \begin{cases} 1 & \text{if } p \le q \\ \left(\frac{q}{p}\right)^i & \text{if } p > q \end{cases}, \tag{2}$$

where q represents the probability that A finds the next block, p represents the probability that an honest miner in the IoT-blockchain network finds the next block, and Q_i is the probability that A will catch up with the honest chain from i blocks behind. This is visually illustrated in Figure 3 that confirms the infeasibility of this attack as long as the honest miners have more than 50% of the total computing power. It can be seen that for values $p = 1, 0.9, 0.8, 0.7, 0.6$, $Q_i$exponentially decreases with the increasing number of blocks of deficit. To elaborate, immediately after just 10 blocks, Q_i reduces to 0. Moreover, for the average value $p = 0.5$, Q_i increases to 1, which signifies again that whoever in the IoT-blockchain network controls more than 50% of the total computational capacity, controls the blockchain. However, given our assumption $p > q$, Q_i exponentially drops with the increasing number of blocks of deficit A has to catch up.

5. Performance Evaluation

For evaluating our scheme, we realized its implementation by designing a smart contract in Solidity which is the programming language for writing smart contracts. Subsequently, simulations were conducted to validate the

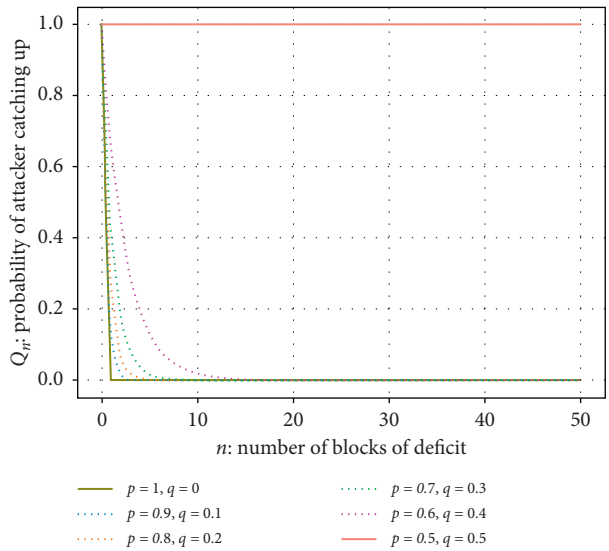

Figure 3: The probability of an adversary (Q_i) trying to reach a breakeven point, i.e., mine an alternate and dishonest chain in a blockchain by competing against an honest chain that has the computing power of at least 51% of honest miners.

interactions and access control functions between subject–object pair nodes.

5.1. Setup. We conducted the simulations using a PC setup with Ubuntu OS on virtual machine client, Oracle VM VirtualBox. Subsequently, the shell scripting environment of Terminal was used for verifying the access control functions. The specifications of the PC were Intel® Core™ i7-7700HQ CPU @ 2.80 GHz (8 CPUs), 16384 MB RAM, NVIDIA GeForce GTX 1060 with 6052 MB memory and 1024 GB HDD + 128 GB SSD of storage. Moreover, the nodes were instantiated using the Ethereum Go client (Geth) according to Algorithm 2. Note that Geth is a command-line interface (CLI) implemented in the Go language for Ethereum development purposes. Thus, separate nodes were used to simulate the subject–object pair interactions with the distributed contracts. Furthermore, the contracts were written and compiled using the Remix integrated development environment (IDE), a browser-based IDE for Solidity, where an outlook of Remix IDE console can be seen in Figure 4. Note that the contracts are deployed at the object side as the blockchain is hosted by the objects.

5.2. Deployment Cost. The cost of performing a task in the Ethereum platform is measured in terms of gas, i.e., for every operation executed in Ethereum, there exists a specified gas cost. Gas is measured in wei and is equal to $1\,\text{wei} = 10^{-18}$ ether. Thus, we can observe that the more complex a task is, the more gas it will require. The gas consumption estimates for the proposed scheme are as follows: the amount required for deploying the contract is 985200 while that for executing it is 21128.

5.3. Experiments. Once the subject–object pair nodes are initialized and the contracts are deployed at the object nodes (we refer to them as server), interaction is now possible with the contract from the subject nodes to simulate IoT-server interactions. Thus, the access control results of the proposed scheme are summarized in Figure 5 as follows: the mining of the contract instance for its address by an object node can be seen in Figure 5(a), whereas the functions used in the proposed scheme are demonstrated in Figure 5(b). It can be seen that a subject node with address 0x c7d9 2270 5023 924b 2073 16bc 7fec f794 f608 020a is first registered in the ACL by the contract and then authorized for a message it sends as well as it is subsequently removed and unauthorized. Finally, Figure 5(c) shows the interactions between a subject–object pair node. This demonstrates and confirms the functions of the proposed scheme.

5.4. Comparative Analysis. This paper compares its scheme with the state-of-the-art scheme [39] that presents a similar contract-based access control mechanism for IoT. A summary of the comparison results is documented in Table 2. The authors in [39] design their scheme with three smart contracts that include multiple access control contracts (ACC), judge contract (JC), and register contract (RC). The operation of their scheme is defined in the following way:

(i) ACC is responsible for enforcing one access control method at a time for a subject–object pair. It also checks and keeps into account the behavior exhibited by a subject.

(ii) JC is responsible for subject behavior management based on the reports of ACC. It also provides functions (e.g., register, update, and delete) to manage the subjects.

(iii) RC offers a storage hub for the scheme; i.e., it is responsible for storing ACC and JC contracts together with the methods associated with them (access control and subject behavior monitoring).

```
while simulation do
  for i in d_o, d_o ∈ O ∀ i = 1, ..., o do
    genesis (.json) ⟵ define
    d_o[i] ⟵ create node
    for j ⟵ 1, i do
      d_o^i[j].node ⟵ deploy contract
  for n in d_s, d_s ∈ S ∀ n = 1, ..., s do
    genesis (.json) ⟵ define
    d_s[n] ⟵ create node
  while d_o &d_s do
    contract ⟵(message())⟵ d_s[n].node
    d_o^i[j].node ⟵ contract
    if request (d_s[n].node) then
      Algorithm 1 ⟵ call
```

Algorithm 2: Initializing the subject–object pair nodes.

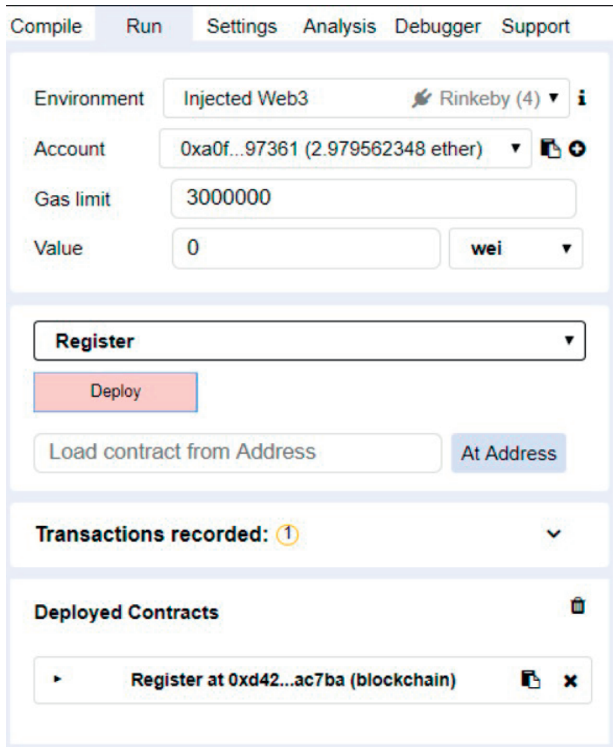

Figure 4: The user interface console of Remix, which is an IDE that is predominantly used in Ethereum to design and compile a smart contract. It offers different settings for analysing and debugging a contract as well as study the execution costs associated with it. The account field represents the address of the contract while the gas limit represents its execution limit among other parameters.

Moreover, [39] does not particularly emphasize on rogue device mitigation, which limits its application and feasibility. It also fails to explain the decentralization degree of miners in a blockchain-enabled IoT network.

In contrast, the proposed scheme establishes the same access control methods by using only one contract with a significantly lesser cost of execution. It manages the malicious behavior of devices via an access control list, which blocks and mitigates the impact of rogue devices. This way, the scheme ensures network reliability by only allowing registered devices to communicate. Furthermore, it discusses the decentralization degree of miners in an

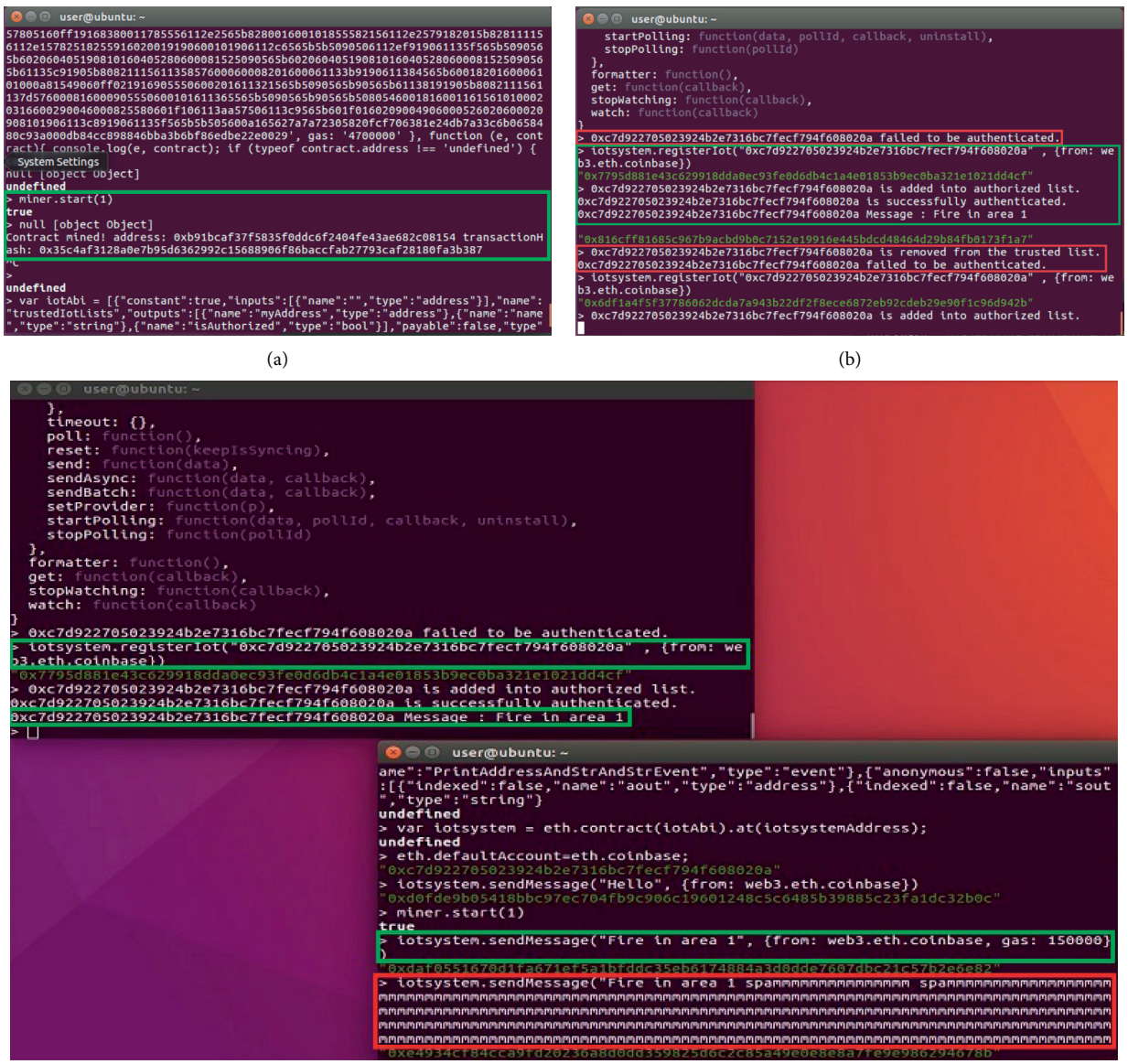

Figure 5: Illustrating the proposed blockchain-based decentralized IoT access control scheme through its implementation in Geth client of Ethereum. Note that the green-colored frames represent a successful operation while the red-colored ones represent a failed operation. (a) Deploying a contract instance on a server (object) node in Geth client. (b) Testing the access control functions on a IoT device node. (c) Demonstrating the interactions between a subject–object pair via a smart contract with a set of message requests.

Table 2: A comparison summary of the proposed scheme with [39].

Attributes	[39]	Proposed	Improvement (%)
No. of contracts	3	1	66
Deploying cost (gas)	5484074	985200	82
Execution cost (gas)	90000	21128	76
Platform	Ethereum	Ethereum	—
Data access	Contract-based	Contract-based	—

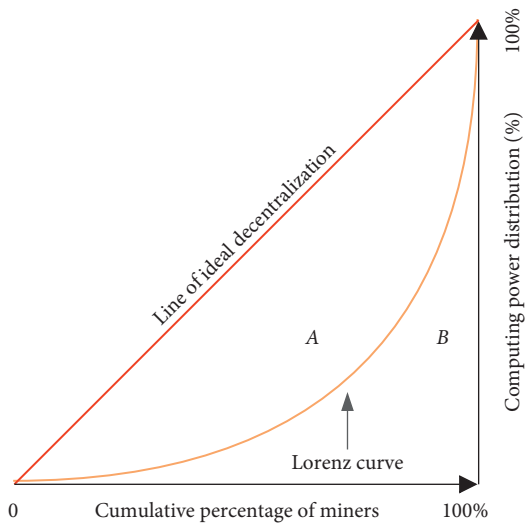

Figure 6: An illustration of a Lorenz curve-based Gini coefficient for quantifying the degree of decentralization of miners in a blockchain. The x-axis represents the increasing number of miners while the y-axis represents the increasing computing power. The Lorenz curve here represents how well the computing power is divided among miners. The line of ideal decentralization is realized when all of the miners have an equal share of computing resources.

IoT-blockchain model using the Gini coefficient. Thus, it can be seen from Table 2 that our scheme outperforms [39] by offering superior performance with low execution cost.

6. Conclusion

This paper investigated the shortcomings of providing access control to devices in a traditional IoT-server communication-based model and presented a blockchain-based access control scheme to mitigate the impact of rogue devices in IoT environments. The proposed scheme uses blockchain in conjunction with smart contracts to provide a secure registration platform for IoT devices. It is also able to distinguish between registered and rogue devices via the application of access control list. To demonstrate the feasibility of the proposed scheme, a security analysis was presented. Additionally, a performance evaluation along with a comparative analysis was also performed for providing access control in a blockchain-based IoT network, which confirms the improvement of the scheme in achieving decentralized IoT access control.

It is noteworthy here that although the results provided in this paper demonstrate the feasibility of the proposed scheme, it can be improved and extended in a number of ways.

Future studies can focus on integrating machine/deep learning techniques to further mitigate the impact of rogue devices in IoT networks. For instance, neural networks can be trained on real data to better identify the attributes of rogue devices and facilitate in providing safeguarding measures together with decentralized access control. The obtained results can also be improved by adopting data sharing and power-domain nonorthogonal multiple access techniques for applications in 5G and beyond. The proposed scheme can be used with resource allocation in cyberphysical systems. For instance, a device can be considered as a subject, which is registered with the network, that requires resource assignment for application-specific purposes, e.g., edge computation offloading. Transaction fees in traditional blockchain platforms remain an open issue that needs to be addressed. Therefore, the proposed implementation can be extended to such platforms where transaction fees are not required. The applicability and feasibility of the proposed scheme can be studied under different consensus protocols of blockchain technology, which will subsequently help identify the applicability of such protocols for providing decentralized and trust-free access control in IoT.

These interesting yet challenging approaches to access control are some of the potential future research avenues that will eventually be discussed and addressed in future studies.

Appendix

A Gini Coefficient

The Gini index or Gini coefficient is a statistical measure of distribution which was first introduced in 1912 by the Italian statistician Corrado Gini [43]. It is primarily used as a gauge of economic inequality and measuring income or wealth distribution among a population. The index ranges from 0 to 1 (or 0–100%), with 0 representing perfect equality and 1 representing perfect inequality. Moreover, there are two commonly accepted definitions of the Gini coefficient.

The first definition is based on Lorenz curve which plots the proportion of the total income of population (y-axis) against the cumulative share of income earned by the population (x-axis). Therefore, the Gini index can be defined as a ratio of the areas area(A)/area$(A + B)$ [45, 46] (an illustration for reference is presented in Figure 6). Using this

argument, we can deduce from the figure that the Gini index can be interpreted as the degree of deviation from the line of ideal decentralization.

The second definition is defined as "half of the relative mean absolute difference," which is mathematically equivalent to the definition of Lorenz curve [52]. The mean absolute difference can be calculated by the average absolute difference of all pairs of people in a population, while the relative mean absolute difference is simply the mean absolute difference divided by the relative average. Therefore, the expression of Gini coefficient can be given as [44, 52]

$$\mathcal{G} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\left|x_i - x_j\right|}{2\sum_{i=1}^{n}\sum_{j=1}^{n}x_i} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\left|x_i - x_j\right|}{2n\sum_{i=1}^{n}x_i}, \tag{A.1}$$

where x_i is the wealth or income of person i while n is the total number of persons. Thus, this paper uses this definition to calculate the Gini coefficient for measuring the degree of decentralization in a blockchain-enabled IoT network.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

References

[1] M. N. Aman, K. C. Chua, and B. Sikdar, "Hardware primitives-based security protocols for the internet of things," in *Cryptographic Security Solutions for the Internet of Things*, M. T. Banday, Ed., pp. 117–141, IGI Global, Hershey, PA, USA, 2019.

[2] M. Rehan and M. Rehmani, *Blockchain-enabled Fog and Edge Computing: Concepts, Architectures and Applications: Concepts, Architectures and Applications*, CRC Press, Boca Raton, FL, USA, 2020.

[3] F. Jameel, M. A. Javed, S. Zeadally, and R. Jantti, "Efficient mining cluster selection for Blockchain-based cellular V2X communications," 2020, http://arxiv.org/abs/2007.01052.

[4] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Privacy of big data in the internet of things era," 2014, http://arxiv.org/abs/1412.8339.

[5] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: opportunities and challenges," in *Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, Waikoloa, HI, USA, December 2019.

[6] F. Jameel and S. A. Hassan, *Wireless-Powered Backscatter Communications for Internet of Things*, Piscataway, NJ, USA, 2020.

[7] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[8] F. Jameel, U. Javaid, B. Sikdar, I. Khan, G. Mastorakis, and C. X. Mavromoustakis, "Optimizing Blockchain networks with artificial intelligence: towards efficient and reliable IoT applications," in *Convergence Of Artificial Intelligence And the Internet of Things*, pp. 299–321, Springer, Berlin, Germany, 2020.

[9] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, p. 1, 2020.

[10] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: design challenges and opportunities," in *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 417–423, San Jose, CA, USA, November 2014.

[11] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering*, vol. 3, pp. 648–651, Hangzhou, China, March 2012.

[12] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 441–510 457, 2019.

[13] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems," in *Proceedings of the 17th International Conference on VLSI Design Proceedings*, pp. 605–611, Mumbai, India, January 2004.

[14] A. Sedrati, M. A. Abdelraheem, and S. Raza, "Blockchain and IoT: mind the gap," in *Interoperability, Safety And Security in IoT*, pp. 113–122, Springer, Berlin, Germany, 2017.

[15] A. Malik, S. Gautam, S. Abidin, and B. Bhushan, "Blockchain technology-future of IoT: including structure, limitations and various possible attacks," vol. 1, pp. 1100–1104, in *Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, IEEE, Kannur, India, July 2019.

[16] B. Liu, S. Sun, and P. Szalachowski, "Smacs: smart contract access control service," in *Proceedings of the 2020 50th Annual IEEE/IFIP International Conference On Dependable Systems And Networks (DSN)*, pp. 221–232, Valencia, Spain, 2020.

[17] U. Javaid, D. Dasnoy, and J. A. Lee, "Multi-organ segmentation of chest ct images in radiation oncology: comparison of standard and dilated unet," in *International Conference on Advanced Concepts for intelligent Vision Systems*, pp. 188–199, Springer, Berlin, Germany, 2018.

[18] U. Javaid, K. Souris, D. Dasnoy, S. Huang, and J. A. Lee, "Mitigating inherent noise in Monte Carlo dose distributions using dilated U-Net," *Medical Physics*, vol. 46, no. 12, pp. 5790–5798, 2019.

[19] U. Javaid, D. Dasnoy, and J. A. Lee, "Semantic segmentation of computed tomography for radiotherapy with deep learning: compensating insufficient annotation quality using contour augmentation," in *Medical Imaging 2019: Image Processing*, vol. 10949, p. 109492P, SPIE Press, Washington, DC, USA, 2019.

[20] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-pbft: an eigentrust-based practical byzantine fault tolerance consensus algorithm," *China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[21] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: decentralized computation platform with guaranteed privacy," 2015, http://arxiv.org/abs/1506.03471.

[22] V. Jaiman and V. Urovi, "A consent model for Blockchain-based health data sharing platforms," *IEEE Access*, vol. 8, pp. 143734–143745, 2020.

[23] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Future Generation Computer Systems*, vol. 86, pp. 740–749, 2018.

[24] M. von Maltitz, S. Smarzly, H. Kinkelin, and G. Carle, "A management framework for secure multiparty computation in dynamic environments," in *Proceedings of the NOMS 2018-*

2018 IEEE/IFIP Network Operations And Management Symposium, pp. 1–7, IEEE, Taipei, Taiwan, April 2018.

[25] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," *Sensors*, vol. 19, no. 4, p. 856, 2019.

[26] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self∗ Systems (FAS∗ W)*, pp. 242–247, IEEE, Augsburg, Germany, September 2016.

[27] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[28] L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[29] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, 2018.

[30] U. Javaid, M. N. Aman, and B. Sikdar, "BlockPro: blockchain based data provenance and integrity for secure IoT environments," in *Proceedings of the 1st Workshop On Blockchain-Enabled Networked Sensor Systems*, pp. 13–18, ACM, New York, NY, USA, 2018.

[31] U. Javaid, M. N. Aman, and B. Sikdar, "Drivman: driving trust management and data sharing in vanets with blockchain and smart contracts," in *Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, Kuala Lumpur, Malaysia, May 2019.

[32] S. S. Arslan, R. Jurdak, J. Jelitto, and B. Krishnamachari, "Advancements in distributed ledger technology for internet of things," *Internet of Things*, vol. 9, Article ID 100114, 2020.

[33] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, Article ID 100057, 2020.

[34] F. Shahid, A. Khan, and G. Jeon, "Post-quantum distributed ledger for internet of things," *Computers & Electrical Engineering*, vol. 83, Article ID 106581, 2020.

[35] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: a review," *Internet of Things*, vol. 10, Article ID 100081, 2019.

[36] H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," *Advances in Computers, Role of Blockchain Technology in IoT Applications*, vol. 115, pp. 73–113, 2019.

[37] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jäntti, "Reinforcement learning in blockchain-enabled IIoT networks: a survey of recent advances and open challenges," *Sustainability*, vol. 12, no. 12, p. 5161, 2020.

[38] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[39] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[40] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: the case study of a smart home," in *Proceedings of 2017 IEEE Interence Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, March 2017.

[41] V. Buterin, "Ethereum: a next-generation smart contract and decentralized application platform," 2014, https://github.com/ethereum/wiki/wiki/White-Paper.

[42] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating loT device based DDoS attacks using blockchain," in *Proceedings Of the 1st Workshop On Cryptocurrencies And Blockchains for Distributed Systems, ser. CryBlock'18*, pp. 71–76, ACM, New York, NY, USA, 2018.

[43] C. Gini, "Variability and mutability," *Journal of the Royal Statistical Society*, vol. 76, pp. 619–622, 1913.

[44] Z. Lin, F. Wen, Y. Ding, and Y. Xue, "Data-driven coherency identification for generators based on spectral clustering," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 3, pp. 1275–1285, 2018.

[45] L. Dai, Y. Jia, L. Liang, and Z. Chang, "Metric and control of system fairness in heterogeneous networks," in *Proceedings of the 2017 23rd Asia-Pacific Conference on Communication (APCC)*, pp. 1–5, Perth, Australia, December 2017.

[46] D. Wu, G. Zeng, L. Meng, W. Zhou, and L. Li, "Gini coefficient-based task allocation for multi-robot systems with limited energy resources," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 155–168, 2018.

[47] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile Blockchain meets edge computing: challenges and applications," 2017, http://arxiv.org/abs/1711.05938.

[48] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain -the gateway to trust-free cryptographic transactions," in *Proceedings of the Twenty-Fourth European Conf. On Information Systems (ECIS)*, pp. 1–14, Springer Publishing Company, Istanbul, Turkey, 2016.

[49] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, p. 1, 2020.

[50] K. Maletsky, "Rsa vs ECC comparison for embedded systems," 2015, http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8951-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-WhitePaper.pdf.

[51] M. N. Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto, "Token-based security for the internet of things with dynamic energy-quality tradeoff," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2843–2859, 2018.

[52] A. Sen, *On Economic inequality*, Oxford University Press, Oxford, UK, 1977.