# A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things

Mohammad Wazid

Ashok Kumar Das

Sachin Shetty
*Old Dominion University*, sshetty@odu.edu

Minho Jo

Original Publication Citation

Wazid, M., Das, A. K., Shetty, S., & Jo, M. (2020). A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things [Article]. *IEEE Access, 8*, 88700-88716. https://doi.org/10.1109/access.2020.2992467

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 23, 2020, accepted April 30, 2020, date of publication May 6, 2020, date of current version May 21, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2992467*

# A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things

**MOHAMMAD WAZID**[1], **(Senior Member, IEEE),**
**ASHOK KUMAR DAS**[2], **(Senior Member, IEEE), SACHIN SHETTY**[3], **(Senior Member, IEEE),**
**AND MINHO JO**[4], **(Senior Member, IEEE)**
[1]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India
[2]Center for Security, Theory, and Algorithmic Research, International Institute of Information Technology, Hyderabad, Hyderabad 500032, India
[3]Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[4]Department of Computer and Information Science, Korea University, Sejong City 30019, South Korea

Corresponding author: Minho Jo (minhojo@korea.ac.kr)

This work was supported in part by the Ripple Centre of Excellence Scheme, Center of Excellence (CoE) in Blockchain, International Institute of Information Technology Hyderabad, India, under Grant International Institute of Information Technology/Research and Development Office/Internal Projects/001/2019, in part by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD [R&E]) under Agreement FA8750-15-2-0120, and in part by the National Research Foundation of the Korean Government under Grant NRF-2019R1I1A3A01057514.

**ABSTRACT** The Internet of Intelligent Things (IoIT) communication environment can be utilized in various types of applications (for example, intelligent battlefields, smart healthcare systems, the industrial internet, home automation, and many more). Communications that happen in such environments can have different types of security and privacy issues, which can be resolved through the utilization of blockchain. In this paper, we propose a tutorial that aims in desiging a generalized blockchain-based secure authentication key management scheme for the IoIT environment. Moreover, some issues with using blockchain for a communication environment are discussed as future research directions. The details of different types of blockchain are also provided. Some of the widely-accepted consensus algorithms are then discussed. Next, we discuss different types of applications in blockchain-based IoIT communication environments. The details of the associated system models are provided, such as, the network and attack models for the blockchain-based IoIT communication environment, which are helpful in designing a security protocol for such an environment. A practical demonstration of the proposed generalized scheme is provided in order to measure the impact of the scheme on the performance of the essential parameters. Finally, some of the future research challenges in the blockchain-based IoIT communication environment are highlighted, which will also be helpful to the researchers.

**INDEX TERMS** Blockchain, Internet of Intelligent Things (IoIT), IoT, security and privacy.

## I. INTRODUCTION

The Internet of Things (IoT) is a specific type of computing and communication environment that consists of different types of computing devices, electromechanical devices, people, or animals that have uniquely associated identities (for example, Internet Protocol addresses through which these devices and objects become capable of transferring data over a network without human involvement [1], [2]. On the basis of its applications and uses, Blockchain of Things (BCoT) has different types of applications as shown in Fig. 1. Some of the potential applicatons of IoT involve ‘‘Internet of Medical Things (IoMT)’’/‘‘Internet of Healthcare Things (IoHT)’’, ‘‘Internet of Energy (IoE)’’, ‘‘Internet of Drones (IoD)’’, ‘‘Internet of Vehicles (IoV)’’ and ‘‘Industrial Internet of Things (IoIT)’’ [3]–[11].

The IoT communication environment produces a huge amount of data. Hence, we need a powerful procedure to handle and process that data, and to make useful conclusions from this process. Such procedures can be effectively

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

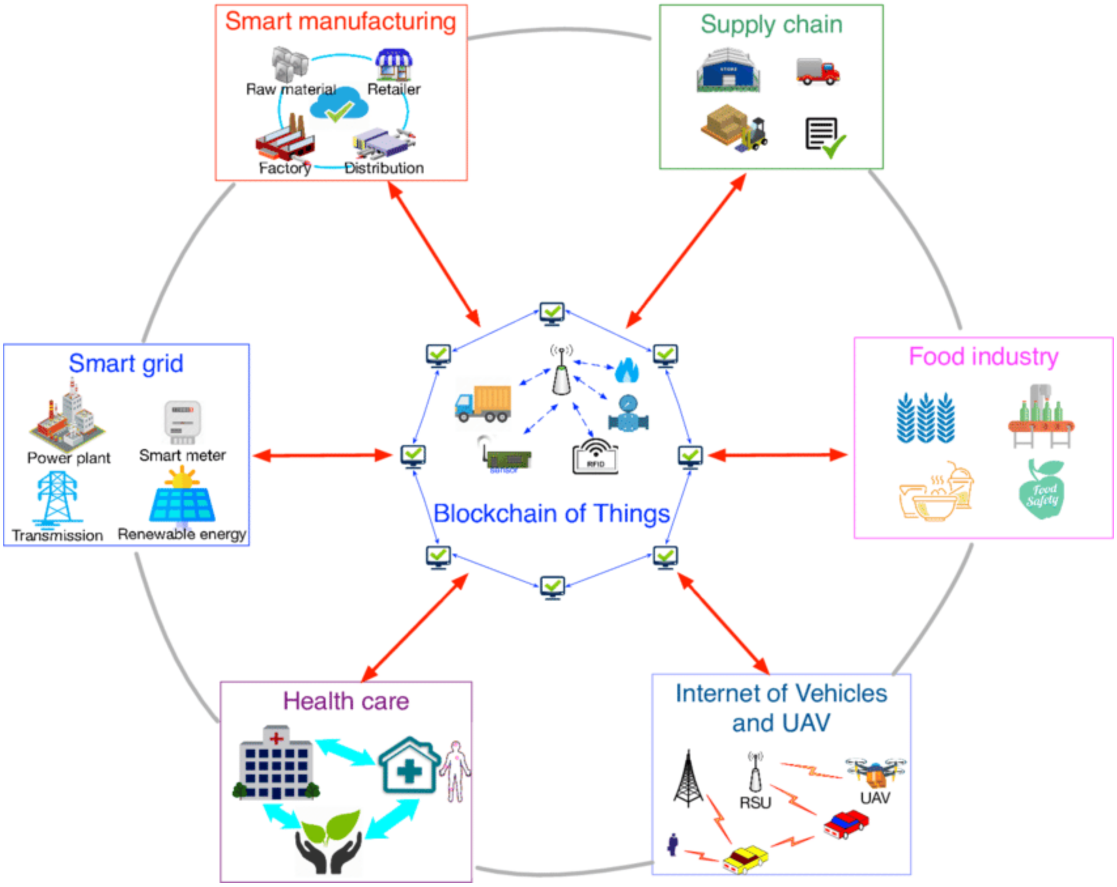


**FIGURE 1.** Potential applications of Blockchain of Things (BCoT) [12].

conducted through the use of artificial intelligence (AI). The conjoining of AI and the IoT creates an intelligent computing and communication environment called the Internet of Intelligent Things (IoIT) [13]. However, the communications that use the IoIT are vulnerable to various types of attack, and need some strong protection mechanisms. Then, the question that arises is: Can we use blockchain to secure communications in the IoIT? And it is obvious that the answer is yes. Blockchain is also called a distributed ledger technology that creates a history for any type of digital asset (e.g., cryptocurrencies). That history is unalterable and transparent to the involved parties through the deployment of decentralization and cryptographic hashing mechanisms. A blockchain contains a time-stamped series of immutable records of data, commanded by a cluster of systems (i.e., cloud servers). There is no single authority that owns these clusters. The data stored and exchanged via blockchain are secured and bound together through cryptography, and there is no central authority. It is a kind of shared and immutable ledger, and therefore, the information in the blockchain is available only to the involved parties. Blockchain is a simple method of passing information from node A to node B in a safer and fully automatic way. A node (or party) can commence a transaction through block creation. Furthermore, the created block is verified by other nodes (i.e., the parties, or the miner nodes) distributed around the network. For this purpose, the nodes utilize a method called a consensus algorithm (i.e., a proof of work [PoW]). If all the other miner nodes commit to the addition of a block, then verification happens successfully; the block is added to the chain and reflected in the distributed ledger across the network. It is not just the creation of a unique record, but also the creation of a unique history. Tampering with a single record would require tampering with an entire blockchain that exists over millions of sites (nodes), which is virtually impossible. Bitcoin uses a blockchain scheme for financial transactions. However, it can also be used for other goals (i.e., secure data exchange among authenticated communicating parties [14]–[18]). The main advantage of using blockchain is to improve data security. Data security (both stored data and data in transit) is one of the essential requirements of all organizations around the globe. Such issues can be resolved through the deployment of a blockchain mechanism, which seems to be a strong mechanism for the security of cloud Internet of Things (IoT)-based organizations.

Following are the impacts of blockchain on data security [14], [17], [19].

- **Overall protection:** The blockchain methods ensure data encryption that resists a data-modification attack. The cryptographic signature corresponding to a document can be saved in the blockchain. This assures users that the file is not modified without demanding that the entire file be saved in the blockchain. Since blockchain is decentralized in nature, the file's signatures can be cross-verified by all the nodes in the network. If an adversary attempts to update a file, then signature verification will fail. The blockchain methods provide reliable and independent verification of data in an undeniable manner. The blockchain records are not stored in any central location; thus, blockchain does not have a single point of failure and cannot be compromised by a single system. The distributed and decentralized ledger of the blockchain network updates continuously in a synchronized manner. With traditional networks, hackers can get all the data from a single system (the repository, i.e., the server) and can try to compromise it, which is impossible in blockchain networks.

- **Decentralized mechanisms:** Blockchain does not depend on any central authority because it is decentralized in nature. Because of the use of the digital ledger, every node (site) maintains a complete copy of the data. The system becomes more unbiased and secure because there is no central point of control. Blockchain uses different types of consensus mechanisms (e.g., PoW, practical byzantine fault tolerance) to validate the transactions. Therefore, it does not depend on any central authority for conducting secure transactions, and data are saved on multiple nodes. Therefore, it is highly secure, even if one or more systems fail.

However, there are some issues with using blockchain for a communication environment, as follows.

- **Effect on the communication environment:** The blockchain-based IoIT environment relies on encryption techniques to provide security when establishing consensus over a distributed network. If a party wants to add something to the chain, that party has to prove he/she has permission to add a block to the chain. The procedure executes a complex algorithm, and in turn, demands excessive use of computing power. For instance, in the bitcoin network over the last year, it is said that the computing power needed for execution of networking tasks devoured the same amount of energy as was needed by 159 countries. Therefore, it is important to consider the energy requirement factor in the deployment of blockchain in an IoIT environment [20], [21].
- **Cost factor:** Apart from the above implementation cost is another challenge for the blockchain-based IoIT. Blockchain schemes are not that efficient in terms of execution of transactions and the related energy requirements. For example, the bitcoin scheme executes three to five transactions per second and consumes a lot of energy in that work. If we compare its performance with other platforms, such as Visa, it seems worse because Visa performs about 1,667 transactions per second. Therefore, to fulfil the requirements of a blockchain-based IoIT environment, we must accept the very high implementation costs. We cannot invest a large share of the budget of a country to secure some infrastructure of computing. Only a few countries have the budget to support such kinds of communication schemes. We need to invent efficient methods that can be deployed in the blockchain-based IoIT. Therefore, this is another issue for the people working in the same domain [20]–[23].
- **Loads from blockchain technology:** Blockchain is deployed with a distributed ledger and through cryptographic algorithms. Blockchain transactions require extra time and resources to process a transaction. The main objective of the blockchain-based IoIT environment is secure information exchange, which can be achieved through deployment of the blockchain mechanism. But transactions in a blockchain may require extra hours to finalize. Quick information exchange is a primary requirement in some domains (for example, battlefields, healthcare, and rescue operations). If the processing and exchange of information consumes extra time, then the intended recipient will not get the information within the required time. The concerned authority will not be able to make a decision within the desired reaction time. These issues can be sorted out by the use of lightweight cryptographic operations, because they need low computation, communications, and storage costs to process the transactions [24], [25].

### *A. BLOCKCHAIN AND VARIOUS CONSENSUS ALGORITHMS*

In this section, we discuss overview of various blockchain technologies and consensus algorithms.

#### 1) TYPES OF BLOCKCHAIN

In the following, we discuss different types of blockchain.

- **Public blockchain:** It is a non-restrictive, permissionless distributed ledger based system. Anybody having access to the Internet can register and sign in the blockchain platform. A user (called as a node), who is a part of public blockchain, is authorized to access the records, verify transactions or conduct mining for the incoming block. One of the main uses of public blockchains is to exchange cryptocurrencies (for example, bitcoin and litecoin blockchains). Most of time public blockchain is secure if the users follow security guidelines. However, sometimes it may be risky in case if the users do not follow the security guidelines. Some of the famous examples include bitcoin, Ethereum, and litecoin [26]–[29].
- **Private blockchain:** It is a restrictive or permission blockchain that works only for a closed network. Most of the time they are used within an organization or enterprises where we have only selected participants. Some of the important properties, such as security, authorizations and accessibility, are the control of a controlling organization. Therefore, private blockchains are like the public

blockchains, but they have a small or restrictive network. Private blockchain can be deployed to perform some of the specific operation (for instance, voting, supply chain management and asset ownership). Some examples of private blockchains include multichain and hyperledger projects (i.e., fabric, and sawtooth) [26], [29]–[31].

- **Consortium Blockchain:** It is a semi-decentralized type in which more than one organization manages the network of blockchain. It is different than the private blockchain, which is managed by only a single organisation. In such type of blockchain, more than one organisation acts as the authority to do mining or exchanging the information. These blockchains are used in various sectors like banking or other government organizations. The examples of such type of blockchain include energy web foundation and R3 [26], [29], [32], [33].
- **Hybrid Blockchain:** It is a combination of the private and public blockchain platforms. The features of both blockchains are applied in this case (for example, users can have "private permission-based system" as well as "public permission-less system"). In the hybrid platform, users can control who acquires access to which data stored in the blockchain. Only some of the selected records of the blockchain are permitted to go public and rest of them are made confidential in the private network. It is flexible system in which users can easily join a private blockchain with multiple public blockchains. The transaction in a private network of a hybrid blockchain is usually verified within that specific network. However, users can also release this in the public blockchain for the verification. The public blockchains do the increment in the hashing and also require more number of verifications. This further improves the security and transparency of the blockchain network. "Dragonchain" is an example of hybrid blockchain [26], [29], [34], [35].

### 2) CONSENSUS ALGORITHMS

A consensus algorithm plays an important role in the mining of the blocks for a blockchain. Consensus algorithms play a decision-making process for a group (i.e., miner nodes), in which each individual member of the group constructs and supports the decision which works best for the rest of them. It is a kind of a resolution which is supported by each individual to draw some conclusion. The consensus model can have following objectives [29], [36]–[39]:

- **Coming to an agreement:** The consensus process gathers all the agreements from the group members.
- **Collaboration:** Every one in the group wishes a better agreement which results in the groups' interests as a whole.
- **Co-operation:** All group members work like a team and put their personal interests aside.
- **Equal rights:** Every single participant (miner) has same weightage in voting process which means every miner's vote is important.
- **Participation:** Every miner has to participate in the voting process. None of them should ignore the participation.
- **Activity:** Every miner has to be equally active. Thus, everybody has the responsibility in the group.

Some of the important consensus algorithms are discussed below [29], [36], [40].

- **Proof-of-Work (PoW):** It is an original consensus algorithm of blockchain. It is used to confirm transactions and produce new blocks to the chain. According to the mechanism of PoW, miners compete among each other to complete the transactions and they also get rewards. Furthermore, it is the measurement of denial-of-service (DoS) attack and other service abuses which include spam on a network by involving the service requester in the process. The major drawback of PoW is that it consumes lot of computational power. It executes through solving of computationally intensive puzzles for the validation of transactions and creation of new blocks. "Bitcoin" and "ethereum" cryptocurrency platforms use PoW consensus algorithms for their mining work.
- **Proof-of-Stake (PoS):** The concept of PoS states that a person can mine or validate block transactions according to the coins he/she holds. This means that the more cryptocurrency coins (i.e., bitcoin) owned by a miner, the more mining power he/she has. PoS was invented to overcome the problems with PoW and aimed for distributed consensus. The cryptocurrency platforms such as "PIVX" and "NavCoin" apply PoS for their mining works.
- **Delegated Proof-of-Stake (DPoS):** It is an another form of PoS algorithm in which the miners (validators) are known as delegates. The determination of block production helps to perform the transaction within a second. DPoS algorithm was designed to assure all levels of protection against the regulatory issues. Cryptocurrency platform such as "lisk" uses DPoS consensus algorithm for its mining work.
- **Leased Proof-of-Stake (LPoS):** It is another improved version of PoS consensus algorithm. According to the mechanism of LPoS, the user is capable to lease waves from his/her wallet to various contractors, who can pay a percentage to him/her as a reward. If a node gets more leased amount, it has high chance for being chosen as the miner to produce the next block for the blockchain.
- **Proof of Elapsed Time (PoET):** This consensus algorithm uses some specific tactics to prevent the high resource utilization along with the high energy consumption. It carries permission blockchain network through a fair lottery system.
- **Practical Byzantine Fault Tolerance (PBFT):** It is one of the best consensus algorithm for the enterprise consortiums in which the members are partially trusted. The only drawback of PBFT is its exponentially increasing messages count with the addition of nodes (replicas) in the set. This algorithm protects against "Byzantine

**TABLE 1.** Summary of consensus algorithms in blockchain.

| Algorithm | Characteristics |
|---|---|
| Proof-of-Work (PoW) | According to the mechanism of PoW, miners compete among each other to complete the transactions and they also get rewarded. Furthermore, it is the measurement of denial-of-service (DoS) attack and other service abuses which include spams on a network by involving the service requester in the process. It requires a lot of computational power. |
| Proof-of-Stake (PoS) | The concept of PoS states that a person can mine or validate block transactions according to the coins he/she holds. This means that the more cryptocurrency coins (i.e., bitcoin) owned by a miner, the more mining power he/she has. |
| Delegated Proof-of-Stake (DPoS) | It is a another form of PoS algorithm in which the miners (validators) are known as delegates. The determination of block production helps to perform the transaction within a second. |
| Leased Proof-of-Stake (LPoS) | A user is capable to lease waves from his/her wallet to various contractors which can pay a percentage to him/her as a reward. If a node gets more leased amount then it has high chances for being chosen as the miner. |
| Proof of Elapsed Time (PoET) | It uses some specific tactics to prevent the high resource utilization along with the high energy consumption. It carries permission blockchain network through a fair lottery system. |
| Practical Byzantine Fault Tolerance (PBFT) | It is one of the best consensus algorithm for the enterprise consortiums in which the members are partially trusted. The only drawback of PBFT is its exponentially increasing message count with the addition of nodes (replicas) in the set. |
| Simplified Byzantine Fault Tolerance (SBFT) | In this algorithm, a block first gathers all the transactions and then batch them into another block. |
| Delegated Byzantine Fault Tolerance (DBFT) | It was introduced to overcome the Byzantine generals problem. It was implemented with perfect conclusion that all transactions are 100% final after getting the first confirmation. |
| Directed Acyclic Graphs (DAG) | It is not a consensus mechanism rather a form of data structure. DAG is convenient for the handling of some particular issues such as data processing, routing and compression. |
| Proof-of-Activity (PoA) | This mechanism mixes the two commonly used consensus algorithms PoW and PoS. The mixing of these two algorithms provides a more secure secure. |
| Proof-of-Importance (PoI) | This algorithm proves the utility of nodes in a network and allows them to create a block. It offers a constituent streamlined technique of maintaining a secure ledger of transactions as compared to other traditional methods. |
| Proof-of-Capacity (PoC) | It allows the mining devices in the network to use their computational power and available hard drive space to decide the mining rights instead of using the other mining device's computing power. |
| Proof-of-Burn (PoB) | It avows the miners to sent few coins to an "eater address". The miner who burns the coins receives a reward and can mine a new block. |
| Proof-of-Weight (PoWeight) | It solves the biased nature of PoS algorithm with the help of "weighted factors". |

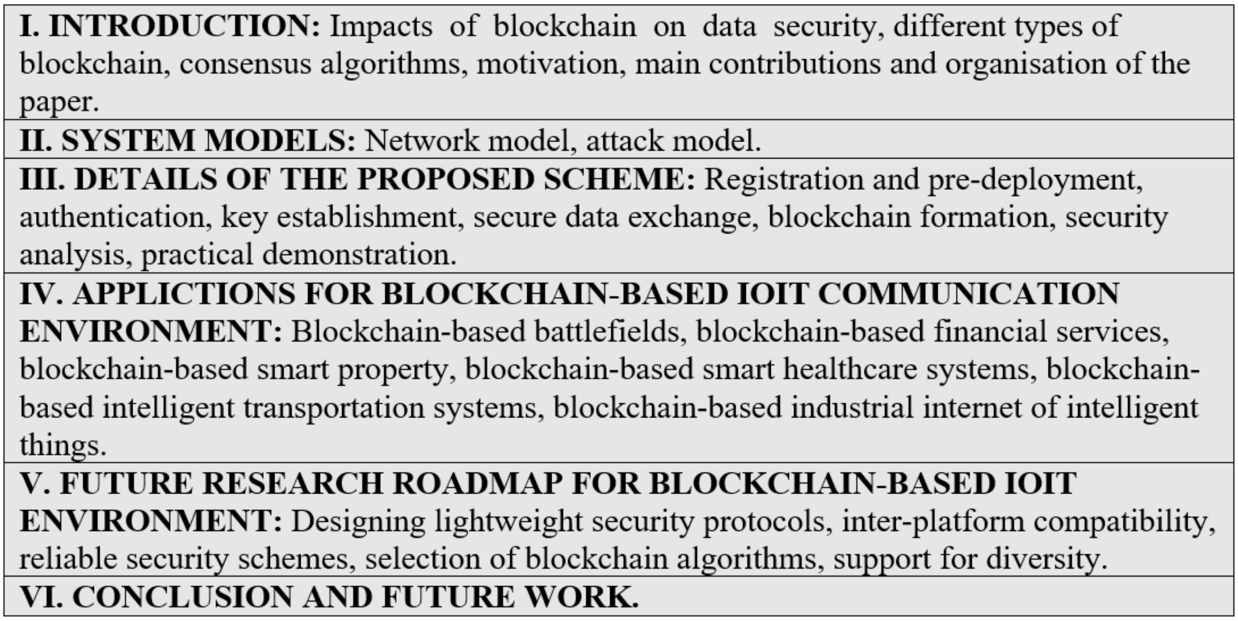
faults" and goes for the optimization aspects of "Byzantine Fault Tolerance (BFT)".

- **Simplified Byzantine Fault Tolerance (SBFT):** In this algorithm, a block first gathers all the transactions and then batch them into another block. Finally, it validates them together.
- **Delegated Byzantine Fault Tolerance (DBFT):** This consensus algorithm was introduced to overcome the Byzantine generals problem. It was developed by "NEO team" with perfect conclusion that all transactions are 100% final after obtaining the first confirmation.
- **Directed Acyclic Graphs (DAG):** It is not a consensus mechanism rather a form of data structure. A blockchain is chain of blocks contains data (in blocks). However, DAG is a graph which stores data topologically. DAG is convenient for handling of some particular issues, such as data processing, routing and compression.
- **Proof-of-Activity (PoA):** This mechanism mixes two commonly used consensus algorithms "Proof of Work (PoW)" and "Proof of Stake (PoS)". The mixing of these two algorithms provides a more secure solution which is secured against different types of attacks.
- **Proof-of-Importance (PoI):** This algorithm proves the utility of nodes in a network and allows them to create a block by a process named as "New Economy Movement (NEM)". It offers a constituent streamlined technique for maintaining a secure ledger of transactions as compared to other traditional methods.
- **Proof-of-Capacity (PoC):** This consensus algorithm allows the mining devices in the network to use their computational power and available hard drive space to decide the mining rights, instead of using the other mining device's computing power (as in PoW algorithm).
- **Proof-of-Burn (PoB):** It avows the miners to sent few coins to an "eater address". The miner, who burns the coins, receives a reward and can mine a new block. However, the coins which are sent to the "eater address" can not be reverted back.
- **Proof-of-Weight (PoWeight):** It is an upgraded version of PoS algorithm. In PoS, the more coins a node owns, the greater are his/her chances to mine a block that results in a bit biased system. However, PoWeight algorithm tries to solve such biased nature of PoS algorithm with the help of "weighted factors".

Finally, various consensus algorithms used in blockchain and their characteristics are summarized in Table 1.

### B. MOTIVATION

The IoIT environment can be used in a wide variety of applications, such as battlefield, smart healthcare, home



**I. INTRODUCTION:** Impacts of blockchain on data security, different types of blockchain, consensus algorithms, motivation, main contributions and organisation of the paper.

**II. SYSTEM MODELS:** Network model, attack model.

**III. DETAILS OF THE PROPOSED SCHEME:** Registration and pre-deployment, authentication, key establishment, secure data exchange, blockchain formation, security analysis, practical demonstration.

**IV. APPLICTIONS FOR BLOCKCHAIN-BASED IOIT COMMUNICATION ENVIRONMENT:** Blockchain-based battlefields, blockchain-based financial services, blockchain-based smart property, blockchain-based smart healthcare systems, blockchain-based intelligent transportation systems, blockchain-based industrial internet of intelligent things.

**V. FUTURE RESEARCH ROADMAP FOR BLOCKCHAIN-BASED IOIT ENVIRONMENT:** Designing lightweight security protocols, inter-platform compatibility, reliable security schemes, selection of blockchain algorithms, support for diversity.

**VI. CONCLUSION AND FUTURE WORK.**

**FIGURE 2.** A pictorial representation of the organisation of the paper.

automation, and many more. However, it suffers from different types of security and privacy related issues owing to various types of attacks, such as ‘‘replay’’, ‘‘man-in-the-middle (MITM)’’, ‘‘impersonation’’, ‘‘credential information guessing’’, ‘‘session key leakage’’, ‘‘data disclosure’’, and ‘‘data modification’’. Hence, we need secure protocols to protect such communication environment from passive and active adversaries. The blockchain mechanism has great potential, and it can be utilized for securing the communications that happen in an IoIT environment because it provides ‘‘immutability’’, ‘‘transparency’’ and ‘‘decentralization’’. In this tutorial work, we propose a generalized blockchain-based secure communication scheme, mainly from the authentication key management perspective point of view, for IoIT environments.

### C. MAIN CONTRIBUTIONS

The contributions of this paper are listed below.

- The impact of blockchain on the existing communication environments is discussed.
- The details of different types of blockchain are provided. Some of the famous consensus algorithms are also discussed.
- We propose a blockchain-based, secure communication scheme for the Internet of Intelligent Things (IoIT).
- The different applications of blockchain-based IoIT communication environments are discussed.
- Network and attack models for blockchain-based IoIT communication environments are described, which are helpful in designing a security protocol for such communication environments.
- A practical demonstration of the proposed scheme is conducted in order to measure the impact of the proposed scheme on the performance of essential parameters.
- Finally, future research challenges in blockchain-based IoIT communication environments are highlighted, which will be helpful to future researchers.

### D. ORGANISATION OF THE PAPER

The remainder of the paper is arranged as follows. The details of the system models required to design a blockchain-based secure communication scheme for the Internet of Intelligent Things are provided in Section II. The details of the proposed scheme are explained in Section III. The various applications of blockchain-based IoIT communication environments are in Section IV. Future research challenges of blockchain-based IoIT environments are discussed in Section V. Finally, the work is concluded in Section VI. For the better readability of the paper, a pictorial representation of the organisation of the paper is also provided in Fig. 2.

## II. SYSTEM MODELS

The overall workings and requirements of a blockchain-based IoIT environment can be explained with the help of the following models.

### A. NETWORK MODEL

The generic architecture of a blockchain-based Internet of Intelligent Things environment is provided in Fig. 3. The architecture consists of smart and intelligent devices, such as drones, robots, autonomous vehicles, wearable devices and weapons for soldiers, wearable and implantable medical devices for patients, and smart home appliances. These devices not only monitor their surroundings but are also able to make required decisions using their knowledge base.

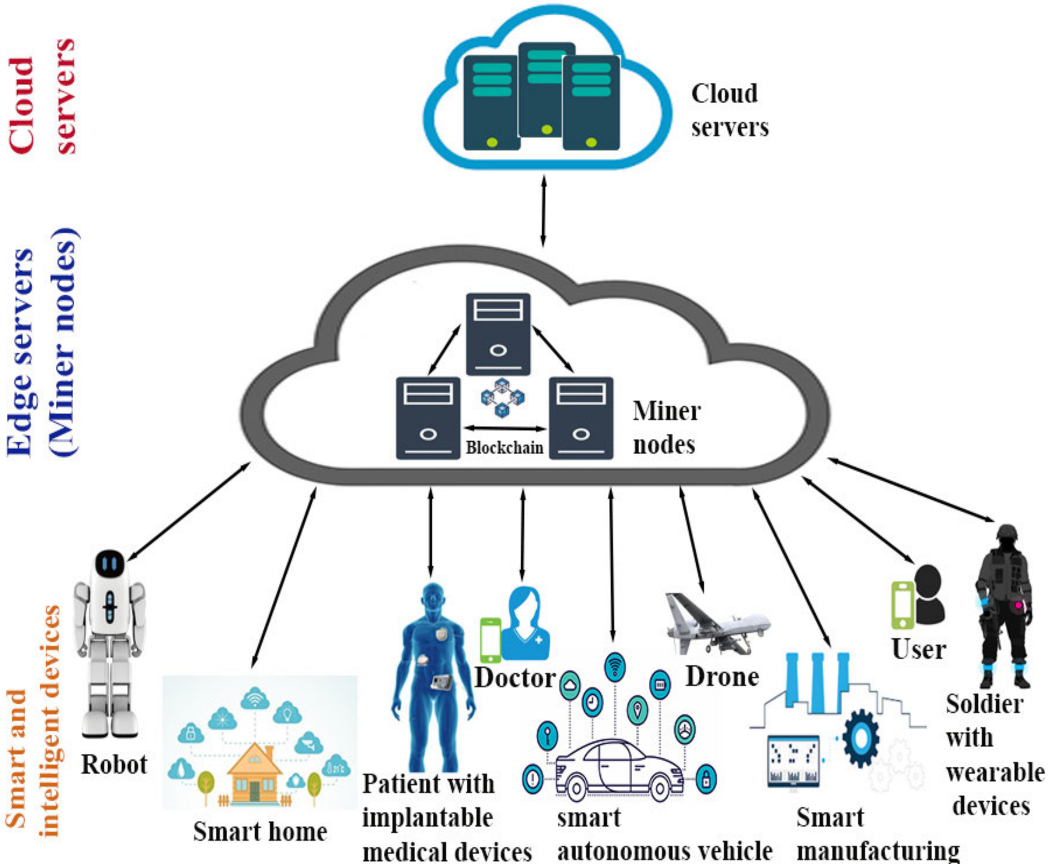

Cloud servers
Cloud servers
Edge servers (Miner nodes)
Miner nodes
Blockchain
Smart and intelligent devices
Robot
Smart home
Patient with implantable medical devices
Doctor
smart autonomous vehicle
Drone
Smart manufacturing
User
Soldier with wearable devices

**FIGURE 3.** Generic architecture of the blockchain-based Internet of Intelligent Things environment (adapted from [1], [41], [42]).

For example, drones can monitor the activities of the enemy and can retaliate according to the situation. A recommendation system in healthcare can suggest the required medicine to the patient in the absence of a doctor. All these devices come under the category of end devices. However, we also have other devices, such as resource-rich edge servers, also called miner nodes because they do the task of blockchain mining. At the same time, we have cloud servers in which data not frequently required can be stored. This kind of communication environment is very helpful in facilitating the daily routines people. However, there are some security- and privacy- related problems from different types of attacks, such as replay, MITM, impersonation of entities, privileged insider, secret guessing, data disclosure, and data modification. Therefore, the blockchain mechanism can be utilized to make the communication environment more secure and robust against these possible attacks. For this purpose, edge nodes (servers) can be utilized. When a smart device has some data, that device can securely send these data to the edge server with the help of an established session key. The edge node also acts as a miner node, receives the data from the smart device, prepares a block from them, and publishes it to the other miner nodes. For block mining purposes, any method, like PoW, can be utilized. If the addition of the block is done by another miner node, that block can be added to the blockchain's distributed ledger, and it is accessible to all miner nodes. If a user is interested in accessing the data of a particular device, the request will go the corresponding miner node. The miner node has access to all blocks in the blockchain (i.e., the distributed ledger), and can then securely provide the data to an authorized user using an established session key. Therefore, the deployment of blockchain mechanism in the IoIT environment is highly recommended.

### B. ATTACK MODEL

The widely accepted Dolev-Yao (DY) threat model [43] can be followed for designing security protocols for IoIT environments. According to this model, two communicating nodes (end-point entities) communicate over an unsecured/open/public channel. Moreover, the end-point entities (e.g., wearable devices, smart home devices) are not, in general, trusted. Therefore, the exchanged messages of the parties might be leaked, modified, or deleted because the channel is unsecured. Furthermore, Canetti and Krawczyk's adversary model (known as the CK-adversary model) [44] can be followed. This model is a current de facto standard model used for designing secure authentication and key

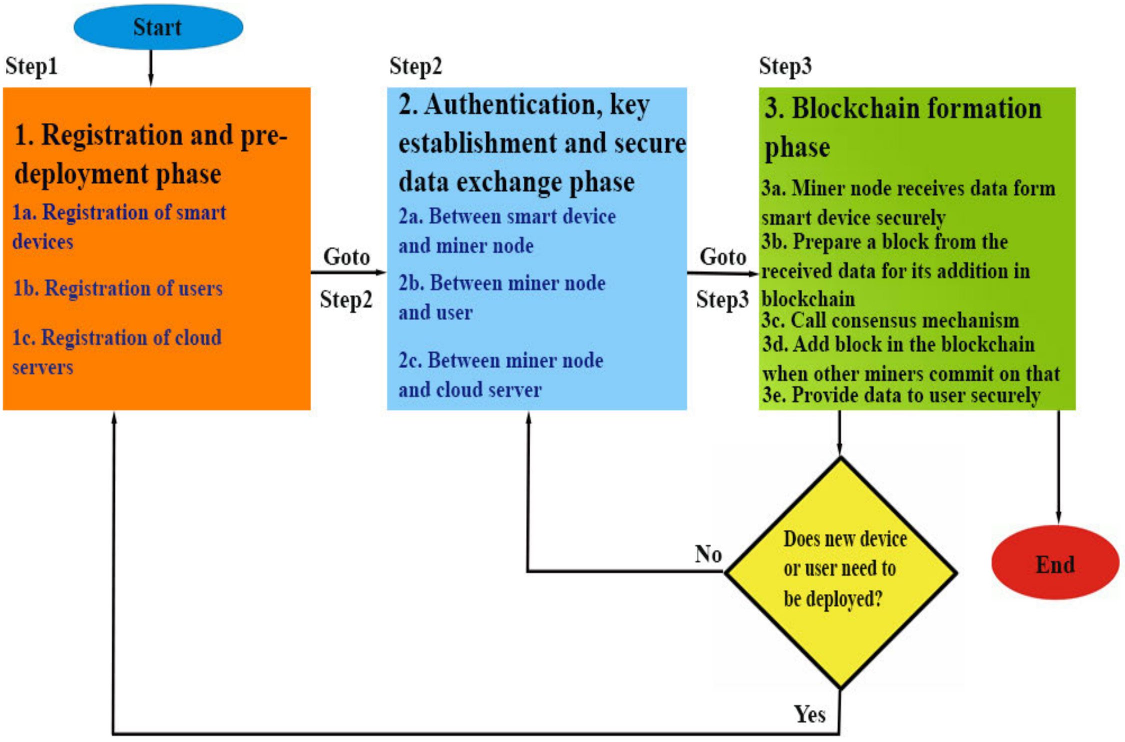

Start
Step1
1. Registration and pre-deployment phase
1a. Registration of smart devices
1b. Registration of users
1c. Registration of cloud servers
Goto Step2
Step2
2. Authentication, key establishment and secure data exchange phase
2a. Between smart device and miner node
2b. Between miner node and user
2c. Between miner node and cloud server
Goto Step3
Step3
3. Blockchain formation phase
3a. Miner node receives data form smart device securely
3b. Prepare a block from the received data for its addition in blockchain
3c. Call consensus mechanism
3d. Add block in the blockchain when other miners commit on that
3e. Provide data to user securely
Does new device or user need to be deployed?
No
Yes
End

**FIGURE 4.** Flow chart of secure communication mechanism for IoIT environment.

agreement schemes. In the CK-adversary model, the attacker (A) can have all the abilities of the DY model; additionally, A can compromise secret credentials, since the session states (session keys) correspond to an established session. Apart from that, A can physical capture smart devices (for instance, the memory unit of a drone, an implantable medical device, a wearable device, the onboard unit of a smart autonomous vehicle) and tries to extract the stored secret information (i.e., the credentials) from these devices by executing a power analysis attack [45]. After that the extracted information can be used for other unauthorized tasks (for instance, computation of a session key, smart-device impersonation, launching the privileged-insider attack, the replay attack, or the MITM attack, and password guessing). Finally, the edge servers (blockchain-miner nodes) are considered fully trusted entities in the network, and they will not be compromised. However, cloud servers are treated as semi-trusted entities in the network.

## III. A GENERALIZED BLOCKCHAIN BASED SCHEME

To explain the overall working of the proposed generalized blockchain based scheme in the Internet of Intelligent Things (IoIT) communication environment.

**TABLE 2.** Notation used in the proposed scheme.

| Notation | Meaning |
|---|---|
| $SD_p$ | $p^{th}$ smart device |
| $U_q$ | $q^{th}$ user |
| $CS_r$ | $r^{th}$ cloud server |
| $MN_i$ | $i^{th}$ miner node |
| $BLK_x$ | $x^{th}$ block in a blockchain |
| $BC$ | Constructed blockchain |
| $KCM$ | Established secret session key between cloud server and miner node |
| $KSM$ | Established secret session key between smart device and miner node |
| $KUM$ | Established secret session key between user and miner node |
| $H(BLK_x)$ | Hash of $x^{th}$ block |

We divide all the activities related the proposed scheme into several phases: (i) registration and pre-deployment; (ii) authentication, key establishment, and secure data exchange; and (iii) blockchain formation similar to the scheme presented in [46]. The details of notations used in the proposed scheme are provided in Table 2. We can further expand the different phases of the proposed scheme as follows. In addition, a flow chart of the proposed scheme is provided in Fig. 4, which represents the summary of all activities conducted in blockchain-based IoIT environment.

### A. REGISTRATION AND PRE-DEPLOYMENT

For registration and pre-deployment, one can follow the steps available in schemes outlined in [1] and [42]. In this phase, a miner node (edge server-trusted node) registers the smart devices. After successful registration, the corresponding secret credentials are stored in memory, and the smart devices are deployed in the specified area. Details of the

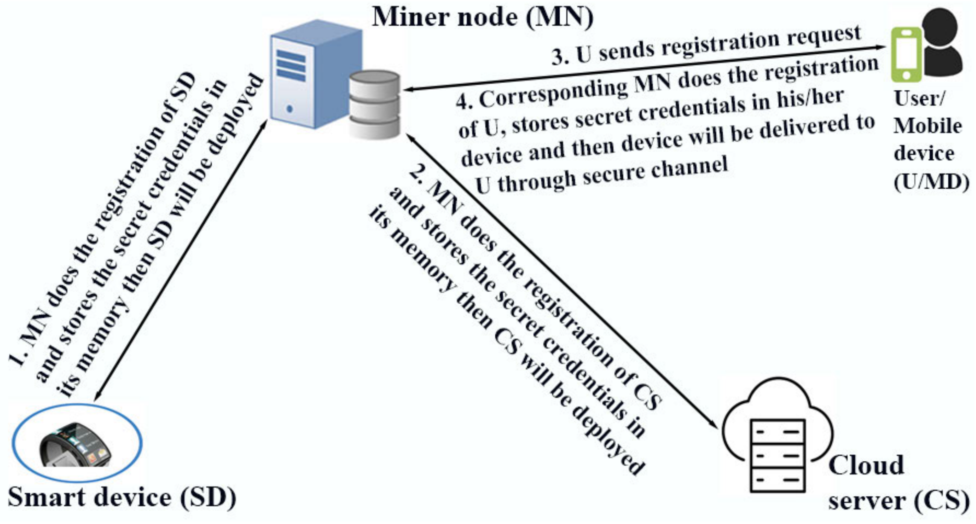

Miner node (MN)
3. U sends registration request
4. Corresponding MN does the registration of U, stores secret credentials in his/her device and then device will be delivered to U through secure channel
User/ Mobile device (U/MD)
1. MN does the registration of SD and stores the secret credentials in its memory then SD will be deployed
2. MN does the registration of CS and stores the secret credentials in its memory then CS will be deployed
Smart device (SD)
Cloud server (CS)

**FIGURE 5.** Registration and pre-deployment phase of the proposed scheme. CS = cloud server; MN = miner node; SD = smart device; U = user; MD = Mobile device of U (i.e., smartphone).

activities related to this phase are provided in Fig. 5. This phase is executed through the following steps.

- **RG1:** Miner node registers smart devices, stores the secret credentials in memory, then the devices are deployed in the specified area.
- **RG2:** The miner node registers the cloud server and stores the secret credentials in memory; then, the cloud server is deployed in the specified area.
- **RG3:** There are some users who want to securely access the data in the smart devices. For this purpose, first of all, they have to register with the corresponding miner node (trusted node-edge server). The user sends a registration request to the miner node through a secure channel. Then, the miner node computes secret credentials for the user and stores them in the smart card or smart phone. Furthermore, the smart card is delivered to the user through a secure channel. Again note that, for registration purposes, it is mandatory to use random identities, pseudo-identities, secret keys for the users and smart devices, and a registration timestamp. This will protect against device/user impersonation attacks and helps in the device- or user-revocation process.

### B. AUTHENTICATION, KEY ESTABLISHMENT AND SECURE DATA EXCHANGE

In this phase, all parties mutually authenticate each other; after that, they establish a secret session key for secure communications. The details of the activities are provided in Fig. 6. The activities can be conducted using the following steps.

- **AKSD1:** The smart device (SD) sends an authentication request to the corresponding miner node (MN). Then, the *MN* computes the authentication reply message and sends it to the *SD*. The *SD* verifies the authenticity of the message and, if successful, both the *SD* and the *MN* establish their secret session key (KSM) to secure their communications. Furthermore, the *SD* encrypts the data with the *KSM* and sends them to the *MN*. Then, the *MN* calls the blockchain formation phase [III-C], which is explained in the next part of this section.
- **AKSD2:** The cloud server (CS) sends an authentication request to the corresponding *MN*. The *MN* computes an authentication reply message and sends it to the *CS*. After receiving the authentication reply message, the *CS* verifies the authenticity of the message, and if successful, both the *CS* and the *MN* establish their secret session key (KCM) to secure their communications. Furthermore, the *MN* encrypts the data with the *KCM* and sends them to the *CS*. The *CS* decrypts the received data with the *KCM* and stores them in memory. Data not frequently required can be stored in the *CS* securely.
- **AKSD3:** A user (U) is authenticated in the specified system and sends a computed login request to the corresponding miner node. The *MN* computes the authentication reply message and sends it to the user. After receiving this message, the user verifies the authenticity of the received message, and if successful, both user and *MN* establish their secret session key (KUM) to secure communications. Furthermore, the *MN* fetches the requested data from the corresponding block of the blockchain (per the blockchain formation phase [III-C]), encrypts it with the *KUM*, and sends it to the user. Again, the mobile device of the user decrypts the data with the *KUM*. It is important to note that all messages should be computed and exchanged with the use of a freshly generated timestamp and random nonce values, and all should be covered inside random identities to

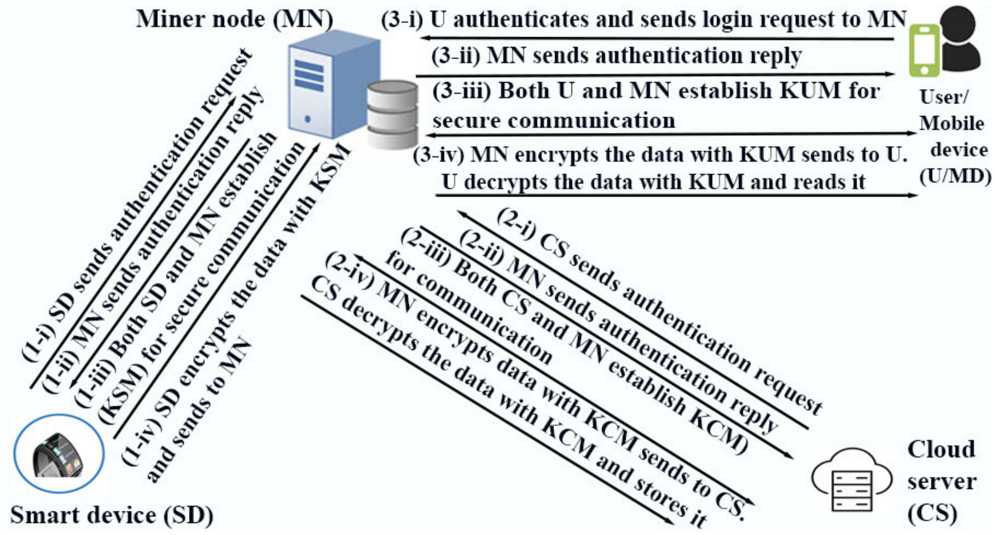

Miner node (MN)
(3-i) U authenticates and sends login request to MN
(3-ii) MN sends authentication reply
(3-iii) Both U and MN establish KUM for secure communication
(3-iv) MN encrypts the data with KUM sends to U. U decrypts the data with KUM and reads it
User/ Mobile device (U/MD)
(1-i) SD sends authentication request
(1-ii) MN sends authentication reply
(1-iii) Both SD and MN establish (KSM) for secure communication
(1-iv) SD encrypts the data with KSM and sends to MN
(2-i) CS sends authentication request
(2-ii) MN sends authentication reply
(2-iii) Both CS and MN establish KCM) for communication
(2-iv) MN encrypts data with KCM sends to CS. CS decrypts the data with KCM and stores it
Smart device (SD)
Cloud server (CS)

**FIGURE 6.** Authentication, key establishment and secure data exchange phase of proposed scheme. CS = cloud server; KCM = key: cloud server-miner node; KSM = key: smart device-miner node; KUM = key: user-miner node; MN = miner node; SD = smart device; U = user; MD = Mobile device of U (i.e., smartphone).

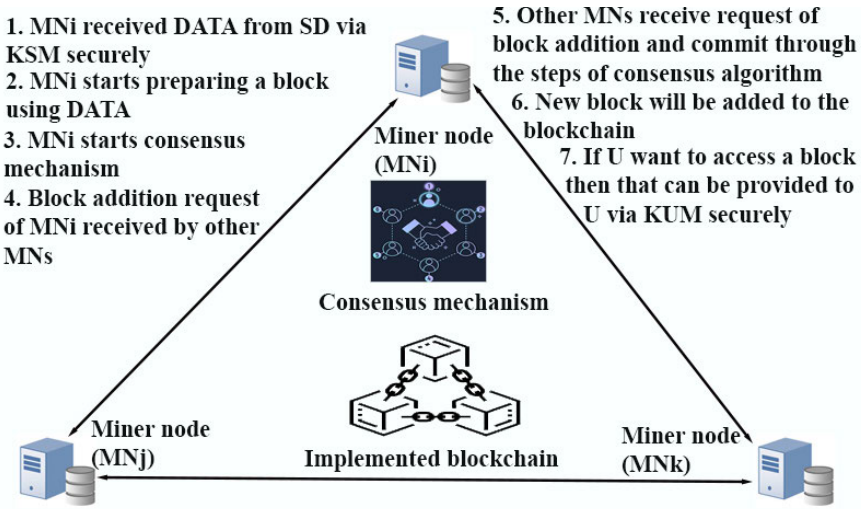

1. MNi received DATA from SD via KSM securely
2. MNi starts preparing a block using DATA
3. MNi starts consensus mechanism
4. Block addition request of MNi received by other MNs
5. Other MNs receive request of block addition and commit through the steps of consensus algorithm
6. New block will be added to the blockchain
7. If U want to access a block then that can be provided to U via KUM securely
Miner node (MNi)
Consensus mechanism
Implemented blockchain
Miner node (MNj)
Miner node (MNk)

**FIGURE 7.** Blockchain implementation phase of the proposed scheme. KSM = key: smart device-miner node; KUM = key: user-miner node; MN = miner node; SD = smart device; U = user.

protect against replay, MITM, impersonation, and illegal session key computation attacks. Each session should be established by using a freshly computed session key.

### C. BLOCKCHAIN FORMATION

After securely receiving the data from the $SD$ with secure session key $KSM$, the corresponding miner node ($MN_i$) starts the formation of the block to be added to the blockchain. A summary of all the steps is provided in Fig. 7. The details of this phase are provided below.

- **BKF1:** Miner node $MN_i$ securely receives the data from its corresponding $SD$ via the established $KSM$. Then, $MN_i$ starts preparation of a block by placing information like timestamp $TS$, ransom nonce $RN$, the hash of this block, $H(BLK_i)$, the hash of the previous block, $H(BLK_{i-1})$, transaction details, etc. After that, $MN_i$ puts its signature on the block using any signature-generation and verification algorithm, i.e., an elliptic curve digital signature algorithm.
- **BKF2:** After that, $MN_i$ starts a consensus mechanism using a consensus algorithm, i.e., practical byzantine fault tolerance. The block-addition request from $MN_i$ is received by other miner nodes, e.g., $MN_j$ and $MN_k$. First of all, these miner nodes verify the signature of this block, and if verified successfully, proves the genuineness of the block.
- **BKF3:** Then, all miner nodes follow the steps of the consensus algorithm, and if all conditions are verified,

other miner nodes commit to addition of this block. The new block is added to the distributed ledger of the blockchain.

- **BKF4:** If an authenticated user wants to access the data of a particular block, the request goes to the corresponding $MN$, and that $MN$ fetches the data from the specified block, providing it to the user securely through the established $KUM$.

The details of the steps of blockchain-based secure communication mechanism for IoIT environment are also explained in Algorithm 1.

**Algorithm 1** Consensus Mechanism for Providing Security in IoIT Environment

**Input:** $m$ is number of smart devices and $n$ is number of users
**Output:** Blockchain of data for $m$ smart devices

```
1:  for all smart devices $SD_p$, $p = 1, 2, \ldots, m$, users $U_q$, $q = 1, 2, \ldots, n$, cloud servers $CS_r$ in IoIT environment, and miner node $MN_i$ do do
2:      Resister all $SD_p$, $U_q$ and $CS_r$.
3:      Perform mutual authentication and key establishment among $SD_p$, $U_q$ and $CS_r$.
4:      Prepare block ($BLK_x$) from the securely received data of $SD_p$.
5:      Call mining procedure for addition of $BLK_x$ using the PoW with other $MN$s.
6:      if other $MN$s commit on addition of $BLK_x$ then
7:          Add $BLK_x$ in blockchain
8:      else
9:          Abort addition of $BLK_x$
10:     end if
11:     Repeat the steps 4–10.
12: end for
```

## D. SECURITY ANALYSIS

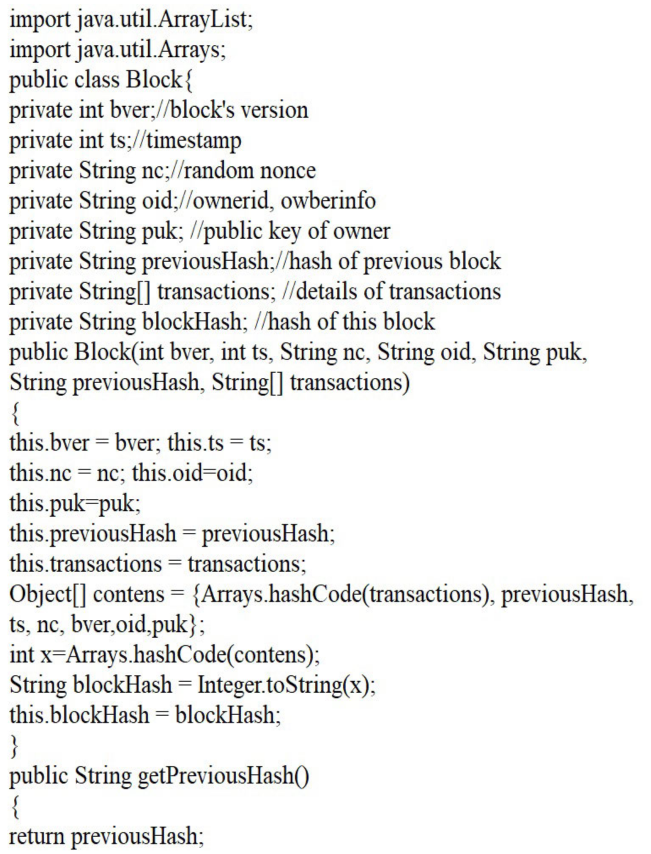
The proposed scheme utilizes the blockchain mechanism. Details of the blockchain-based secure communication scheme for Internet of Intelligent Things environments are provided above. It is resilient against various kinds of attacks, such as replay attacks, man-in-the-middle, impersonation, privileged insider, illegal session key computation, data modification, data leakage, and smart device physical capture. The use of random nonce and timestamps in all exchanged messages protects them against replay and MITM attacks. The secret keys are not installed directly in memory of any smart device. Consideration for, and inclusion of, these parameters protects against various types of attacks, like impersonation, privileged insider, password guessing, illegal session key computation, and smart device physical capture. The utilization of blockchain methods (i.e., signature generation and verification procedures) provides data integrity and authenticity. Furthermore, it maintains transparency and immutability.

**TABLE 3.** Simulation parameters used in the proposed scheme.

| Parameter | Value |
|---|---|
| Platform used | Windows 10 64-bit OS |
| Processor | Intel Core i5-8250U,<br>1.60 -1.80 GHz |
| RAM | 8 GB |
| Programming platform | Eclipse IDE<br>2019-12 with Java |
| Number of smart devices | 5 (case 1),<br>10 (case 2), 15 (case 3) |
| Number of users | 2 (case 1),<br>4 (case 2), 6 (case 3) |
| Number of miner nodes | 4 in all cases |
| Level of difficulty in consensus (mining) | 4 |
| Fields of a block | block-version, timestamp,<br>random nonce, transaction details,<br>owner (miner) identity,<br>owner's public key,<br>hash of previous block,<br>hash of current block,<br>block signature |
| Size of a block | 2560 bits |

## E. PRACTICAL DEMONSTRATION

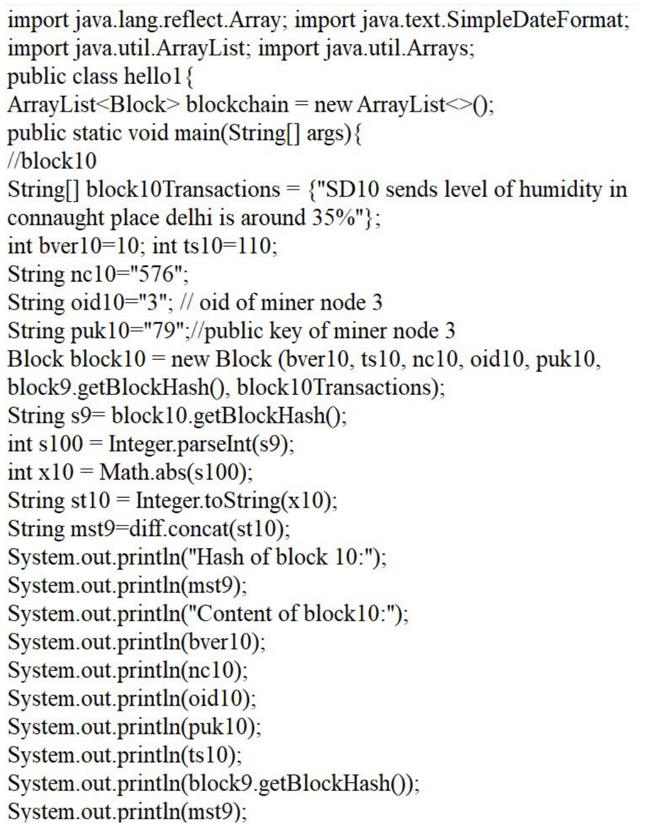
A practical demonstration of the proposed scheme using the blockchain mechanism was performed as follows [7] with the parameters listed in Table 3. Three different cases were considered in the simulations, which were conducted in the Windows 10, 64-bit OS installed on an Intel Core i5-8250U with a 1.60-1.80 GHz processor and 8 GB RAM. The programming platform was the Eclipse IDE 2019-12 with Java. The smart devices considered numbered 5 (case 1), 10 (case 2) and 15 (case 3), with 2, 4, and 6 users, respectively, along with four miner nodes (*MNs*). Mobility affects the performance of a blockchain system operating in a vehicular ad hoc network (VANET). The mobility of nodes causes a distinctive challenge to the blockchain operations due to the dynamicity and continuous change in the connectivity of the nodes. More specifically, mobility makes a proof-of-work (PoW) mechanism difficult. This is happens when the nodes move, they can only have a limited duration of time for a "rendezvous" to exchange a new block for the verification. As the information provided in [47], it is easy to discover that a slow moving VANET can accommodate exchange of a larger number of blocks as it holds a rendezvous for a longer time. However, in the proposed generalized scheme we only consider the static nodes. Therefore, we can neglect the effect of mobility on the blockchain operations. The level of difficulty in consensus (mining) was 4. The level of difficulty is a value for how difficult it is to find (mine) a hash below a given target for the PoW consensus protocol. Finding (mining) a hash is called solving a puzzle sometimes. The target values were present by the system. PoW is also used for implementation of Bitcoin and Litecoin blockchain frameworks. Hence, a similar approach was followed in the proposed framework. The different fields used in a block are as follows.



```
import java.util.ArrayList;
import java.util.Arrays;
public class Block{
private int bver;//block's version
private int ts;//timestamp
private String nc;//random nonce
private String oid;//ownerid, owberinfo
private String puk; //public key of owner
private String previousHash;//hash of previous block
private String[] transactions; //details of transactions
private String blockHash; //hash of this block
public Block(int bver, int ts, String nc, String oid, String puk,
String previousHash, String[] transactions)
{
this.bver = bver; this.ts = ts;
this.nc = nc; this.oid=oid;
this.puk=puk;
this.previousHash = previousHash;
this.transactions = transactions;
Object[] contens = {Arrays.hashCode(transactions), previousHash,
ts, nc, bver,oid,puk};
int x=Arrays.hashCode(contens);
String blockHash = Integer.toString(x);
this.blockHash = blockHash;
}
public String getPreviousHash()
{
return previousHash;
```

**FIGURE 8.** Snippets of code: structure of a block.

- **Block-version** It depicts the version, i.e., identity, of a block. The size of this field is assumed to be 32 bits.
- **Timestamp** It is the timestamp value for a particular block. The size of this field is assumed to be 32 bits.
- **Random nonce** It is a value for a particular block. The size of this field is assumed to be 160 bits.
- **Transaction details** It includes information about the ongoing transactions, for example, which entity is sending which information and for what purpose. The size of this field is assumed to be 1024 bits.
- **Owner (miner) identity** It depicts the identity of the owner (or miner) node. The size of this field is assumed to be 160 bits.
- **Owner's public key** It contains information about the public key of the owner (miner) node. The size of this field is assumed to be 320 bits in the elliptic curve cryptography (ECC) algorithm.
- **Hash of previous block** It contains the hash value. The size of this field is assumed to be 256 bits in the SHA256 algorithm.
- **Hash of current block** It contains the hash value. The size of this field is assumed to be 256 bits in the SHA256 algorithm.
- **Block signature** It contains signature information for a particular block. The size of this field is assumed to be 320 bits in the ECC algorithm.



```
import java.lang.reflect.Array; import java.text.SimpleDateFormat;
import java.util.ArrayList; import java.util.Arrays;
public class hello1{
ArrayList<Block> blockchain = new ArrayList<>();
public static void main(String[] args){
//block10
String[] block10Transactions = {"SD10 sends level of humidity in
connaught place delhi is around 35%"};
int bver10=10; int ts10=110;
String nc10="576";
String oid10="3"; // oid of miner node 3
String puk10="79";//public key of miner node 3
Block block10 = new Block (bver10, ts10, nc10, oid10, puk10,
block9.getBlockHash(), block10Transactions);
String s9= block10.getBlockHash();
int s100 = Integer.parseInt(s9);
int x10 = Math.abs(s100);
String st10 = Integer.toString(x10);
String mst9=diff.concat(st10);
System.out.println("Hash of block 10:");
System.out.println(mst9);
System.out.println("Content of block10:");
System.out.println(bver10);
System.out.println(nc10);
System.out.println(oid10);
System.out.println(puk10);
System.out.println(ts10);
System.out.println(block9.getBlockHash());
System.out.println(mst9);
```

**FIGURE 9.** Snippets of code: data inside a block.

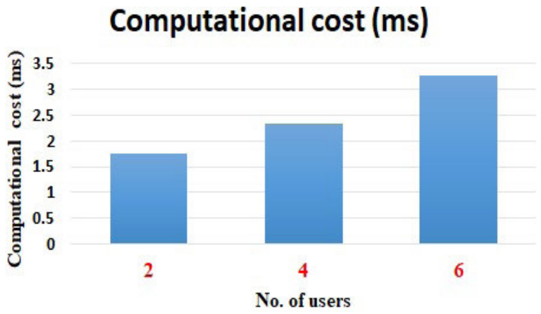


**FIGURE 10.** Results obtained: impact of the number of users.

Some snippets of code are provided in Fig. 8 for the structure of a block, and in Fig. 9 for data inside a block.

The following results were obtained during the simulations.

### 1) IMPACT OF NUMBER OF USERS

The impact of increasing the number of users on the creation and addition of blocks (blockchain mining) is computed as the computation cost (in ms). The values for computation cost were 1.76, 2.34, and 3.28 for 2, 4, and 6 users, respectively. These results are illustrated in Fig. 10. It is important to note that the computation cost increases with the number of users because incrementing the number of users causes the creation and addition (mining) of more blocks in the blockchain.

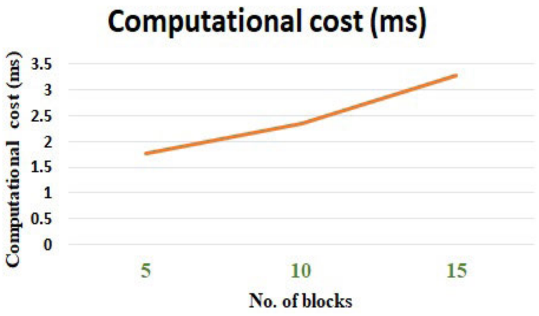


**FIGURE 11.** Results obtained: Impact of the number of blocks.

### 2) IMPACT OF NUMBER OF BLOCKS

The impact of increasing the number of blocks in the blockchain is analyzed in terms of computation cost. The values of the computation cost (in ms) were 1.76, 2.34, and 3.28 for 5, 10, and 15 blocks, respectively. These results are illustrated in Fig. 11. It is important to note that the computation cost increases with more blocks, because incrementing number of blocks causes the creation and addition (mining) of more blocks in the blockchain.

## IV. APPLICTIONS FOR BLOCKCHAIN-BASED IoIT COMMUNICATION ENVIRONMENT

Blockchain-based IoIT environments can be utilized in various types of applications. The information on some of the potential applications is provided below [20]–[25].

### A. BLOCKCHAIN-BASED BATTLEFIELDS

The Internet of Intelligent Battlefield Things is a scenario of battlefield environments that consist of smart devices, such as drones (unmanned aerial vehicles), robots, and wearable devices and weapons for soldiers. These devices monitor their surroundings and send the corresponding data to the base station (control system). These devices also have an inbuilt artificial intelligence component, and on the basis of this component, devices can act automatically (for example, target tracking and retaliation through drones). However, such kinds of communication environments suffer from various types of security and privacy issues. Various attacks are possible such as the replay, MITM, impersonation, privileged insider, password- or other secrets-guessing, illegal session-key computation, data leakage, and data modification. The blockchain ledger can provide security to different types of Internet of Things environments. With billions of connected devices, security experts worry about making sure this distributed information is secure. Therefore, the blockchain mechanism can be utilized to secure communications that take place for the Internet of Intelligent Battlefield Things, and also in other types of environments, such as smart homes and smart grids [48].

### B. BLOCKCHAIN-BASED FINANCIAL SERVICES

Traditional systems are cumbersome, have errors, and unfortunately, are slow. We need the involvement of intermediaries to facilitate the activities and to resolve conflicts. This causes further stress and requires extra time and money. However, if we use a blockchain, things will be much cheaper, more transparent, more effective, and robust. Small financial services firms are growing in number, promoting systems for innovations (for example, smart contracts and smart bonds). This system is much better, because it automatically pays bondholders their money upon completion of preprogramed terms. They are self-executing and self-maintaining in nature. This environment can work more intelligently with the use of smart devices, for example, smart sensing devices. It also provides more security for all communications by making use of the blockchain mechanism. Hence, this is one of the emerging applications of the blockchain-based IoIT environment.

### C. BLOCKCHAIN-BASED SMART PROPERTY

There are different types of property, such as houses, cars, patents, property titles, company shares, etc. Scenarios can be deployed with smart and intelligent devices, such as smart sensing devices and devices with a physical uncloneable function (PUF), which facilitates the overall functioning of the environment. The registration of these properties can be stored in the distributed ledger of a blockchain, along with contractual details (i.e., who is allowed ownership of this property). Furthermore, smart keys can be deployed to provide access to authorized parties. The maintained distributed ledger stores and allows the exchange of smart keys when a contract is verified. The ledger is also a system for recording and managing property rights, and it enables smart contracts to be duplicated if the smart key is lost or stolen. Making a property smart reduces mediation fees and the risk of fraud. Simultaneously, it increases the trust and efficiency of the system. Therefore, this can be another important application of blockchain-based IoIT environments.

### D. BLOCKCHAIN-BASED SMART HEALTHCARE SYSTEMS

The smart and intelligent healthcare system is another potential application of the IoIT. Such communication environments consist of smart healthcare devices (e.g., implantable medical devices, wearable health devices). They also have various types of users (i.e., relatives of patients, doctors, and nursing staff). In order to recommend medicine, health staff members require the health data of the patient, which should be transmitted and received in a secure way. In this communication environment, a recommendation system can also be deployed that can act in a doctor's absence.

However, a smart, or intelligent, healthcare system can have various types of security and privacy issues. It is vulnerable to the attacks listed earlier. In such environments, personal health records could be encrypted and stored in the blockchain, along with a private key that provides access only to authorized personnel. Moreover, the records of surgery could be stored in a blockchain and automatically sent to insurance companies as proof of delivery. Apart from that, the ledger can be used for general healthcare management, for example, for the supervision of drugs, adherence to compliance regulations, recording results from testing, and management of healthcare supplies. Therefore, the blockchain procedure will be helpful in securing the communications that take place in an intelligent healthcare system.

### E. BLOCKCHAIN-BASED INTELLIGENT TRANSPORTATION SYSTEMS

A smart, or intelligent, transportation system consists of autonomous vehicles (e.g., the autonomous car), roadside units, and cloud/fog servers. These devices can communicate with each other using the Internet. It is an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in navigating a complex route. The intelligent units of the system have a responsibility to make decisions with speed, consistency, and accuracy. Such kinds of communication environments provide a comfortable and safe journey to passengers. However, they are also vulnerable to the different types of attacks listed earlier. The use of blockchain technology in an intelligent transportation system makes communications stronger and more reliable against outside and inside network threats.

### F. BLOCKCHAIN-BASED INDUSTRIAL INTERNET OF INTELLIGENT THINGS

The Industrial Internet of Intelligent Things is a combination of connected machines and devices in industry, for example, power generation, oil, gas, and other manufacturing/production systems. Unplanned downtime and system failures in an industrial plant can threaten the lives of the people working inside, which can be avoided through the deployment of an Industrial IoIT environment. A system embedded with smart monitoring and sensing devices can help create a safe and reliable working environment. The IoIT environment consists of smart IoT devices, gateway nodes, and various types of servers. The resource-rich devices, such as servers, can execute machine learning algorithms and make predictions about some phenomena (e.g., chances of a fire inside a plant). However, the communications that happen in such kinds of communication environments are vulnerable to different types of attacks (e.g., hacking of control systems in a plant). Therefore, we can make use of the distributed ledger in a blockchain to make communications more secure and reliable against intruders.

## V. FUTURE RESEARCH ROADMAP FOR BLOCKCHAIN-BASED IoIT ENVIRONMENT

As discussed earlier, the blockchain-based Internet of Intelligent Things communication environment can be utilized in a wide variety of applications. Moreover, deployment of the blockchain mechanism makes it more strong and robust against the existing forms of attack. However, like other kinds of communication environments, it also has some challenges that need to be addressed by research in the future. The roadmap for the blockchain-based IoIT environment is provided below [2], [29], [49].

### A. DESIGNING LIGHTWEIGHT SECURITY PROTOCOLS

Security protocols can be categorized into various types, such as key management, user authentication and key agreement, access control/user access control, and intrusion detection and prevention. All these protocols use cryptographic methods for message generation and exchange. Some of these cryptographic methods utilize heavy algorithms that require very high computation, communications, and storage capabilities. But some of the devices in blockchain-based IoIT environments, such as sensing devices, are resource-constrained in nature and do not have high computation, communications, and storage capabilities. Therefore, we cannot use security schemes having high requirements in computation, communications, and storage capacities. Moreover, deployment of the blockchain procedure also creates extra burdens on the system when it requires such capabilities. Hence, we should be selective when going for the design of security protocols for blockchain-based IoIT environments or for other resource-restricted computing environments. The use of lightweight cryptographic operations will be helpful to researchers who resolve this problem.

### B. INTER-PLATFORM COMPATIBILITY

In a blockchain-based IoIT environment, we have different types of devices and users. They use different types of platforms, tools, and technologies to communicate among themselves. In such situations, there may be an issue of compatibility among the devices operating on different platforms. Hence, we should design a security protocol in such a way that it is strong enough to prevent attacks and does not have any compatibility issues. Therefore, designing such security protocols can be an important research problem for the future.

### C. RELIABLE SECURITY SCHEMES

Different types of security schemes in the literature do not combat some types of attack. Furthermore, some schemes work for a particular attack and do not work for others. Therefore, it is important to design a security scheme so that it detects and prevents different types of attack at the same time. Hence, designing a reliable blockchain-based security scheme can be a challenging problem for future researchers.

### D. SELECTION OF BLOCKCHAIN ALGORITHMS

In a blockchain-based IoIT environment, we have different types of devices, and some of them are resource-constrained (e.g., sensing devices). Moreover, this type of environment is vulnerable to the various types of attacks listed earlier, which can be prevented through the blockchain mechanism. However, selection of a blockchain algorithm is very tricky. For example, which consensus algorithm should we use, and on which node (device)? It is always preferable to use algorithms like Merkle root, which are efficient compared to the other existing algorithms. Therefore, selection of a blockchain's algorithm for securing the environment can also be another interesting problem for researchers.

### E. SUPPORT FOR DIVERSITY

Blockchain-based IoIT environments consist of different types of devices: smart and intelligent devices (e.g., drones, smart autonomous vehicles), laptop systems, desktop systems, personal digital assistants, mobile handheld devices, other low-powered sensing devices, and RFID tags. Furthermore, these devices operate under the existing specifications of communication protocols. Apart from that, these devices have different types of computation strengths, storage capacities, communication strengths, underlying operating systems, and other software. Hence, the security scheme for blockchain-based IoIT environments should be designed in such a way that they can support and protect all types of devices and associated mechanisms.

## VI. CONCLUSION AND FUTURE WORK

Blockchain technology has great potential, and can be useful in securing a communication environment. A blockchain-based IoIT environment can also be secured through deployment of the blockchain mechanism. The system models (i.e., network and attack models for blockchain-based IoIT environments) that will be helpful in designing a security protocol were presented. After that, we provided details of the proposed blockchain-based secure communication scheme for Internet of Intelligent Things environments. The provided security analysis depicts the scheme's resilience against possible attacks. A practical demonstration of the proposed scheme was provided in order to measure the impact of the proposed scheme. The details of different types of blockchain are provided. Some of the famous consensus algorithms are also discussed. The details of various types of applications of blockchain-based IoIT environments were provided, and some future research challenges in this domain were highlighted.

It is worth noticing that in this tutorial paper, we proposed a generalized blockchain based security scheme, which was particularly focused on the authentication and key management issues. In future, we aim to provide the mathematical details related to all the steps of the proposed generalized scheme. For this purpose, a concrete formal security analysis under the standard oracle model and also the formal security verification using automated software validation tools are needed. Next, a detailed performance analysis with respect to computation cost, communication cost and storage cost is essential.

## ACKNOWLEDGMENT

The authors thank the anonymous reviewers and an associate editor for their valuable feedback on the article which helped us to improve its quality and presentation.

## REFERENCES

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[2] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[3] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[4] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[5] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.

[6] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[7] M. Fan and X. Zhang, "Consortium blockchain based data aggregation and regulation mechanism for smart grid," *IEEE Access*, vol. 7, pp. 35929–35940, 2019.

[8] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.

[9] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[10] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[11] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in Internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[12] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[13] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano, "Internet of intelligent things: Bringing artificial intelligence into things and communication networks," in *Inter-Cooperative Collective Intelligence: Techniques and Applications*, F. Xhafa and N. Bessis, Eds. Berlin, Germany: Springer, 2014, pp. 1–37.

[14] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[15] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, May 2018.

[16] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Portfolio, 2018.

[17] A. Rosic. *What is Blockchain Technology? A Step-By-Step Guide for Beginners*. Accessed: Dec. 2019. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/

[18] T. Maksymyuk, J. Gazda, L. Han, and M. Jo, "Blockchain-based intelligent network management for 5G and beyond," in *Proc. 3rd Int. Conf. Adv. Inf. Commun. Technol. (AICT)*, Lviv, Ukraine, Jul. 2019, pp. 36–39.

[19] S. Palavesh. *Here's How You Can Secure Your Data With Blockchain*. Accessed: Dec. 2019. [Online]. Available: https://www.entrepreneur.com/article/318477

[20] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[21] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[22] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.

[23] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.

[24] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.

[26] D. Team. *Types of Blockchains-Decide Which One is Better for Your Investment Needs*. Accessed: Apr. 2020. [Online]. Available: https://data-flair.training/ blogs/ types-of-blockchain/

[27] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 46–56, Jul. 2018.

[28] L. Van Der Horst, K.-K.-R. Choo, and N.-A. Le-Khac, "Process memory investigation of the bitcoin clients electrum and bitcoin core," *IEEE Access*, vol. 5, pp. 22385–22398, 2017.

[29] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K.-R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, Oct. 2019.

[30] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *Proc. IEEE 26th Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst. (MASCOTS)*, Milwaukee, WI, USA, Sep. 2018, pp. 264–276.

[31] A. Mohite and A. Acharya, "Blockchain for government fund tracking using hyperledger," in *Proc. Int. Conf. Comput. Techn., Electron. Mech. Syst. (CTEMS)*, Belgaum, India, Dec. 2018, pp. 231–234.

[32] K. Huang, X. Zhang, Y. Mu, X. Wang, G. Yang, X. Du, F. Rezaeibagha, Q. Xia, and M. Guizani, "Building redactable consortium blockchain for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3670–3679, Jun. 2019.

[33] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[34] X. Han, Y. Yuan, and F.-Y. Wang, "A fair blockchain based on proof of credit," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 5, pp. 922–931, Oct. 2019.

[35] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "ZkCrowd: A hybrid blockchain-based crowdsourcing platform," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4196–4205, Jun. 2020.

[36] H. Anwar. *Consensus Algorithms: The Root of the Blockchain Technology*. Accessed: Apr. 2020. [Online]. Available: https://101blockchains.com/consensus-algorithms-blockchain/

[37] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[38] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles," *IEEE Access*, vol. 7, pp. 139703–139711, 2019.

[39] S. Li, S. Zhao, P. Yang, P. Andriotis, L. Xu, and Q. Sun, "Distributed consensus algorithm for events detection in cyber-physical systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2299–2308, Apr. 2019.

[40] Z. Hary. *What is Blockchain Consensus Algorithms*. Accessed: Apr. 2020. [Online]. Available: https://www.bitdeal.net/blockchain-consensus-algorithms

[41] Alibaba Cloud. *What is Edge Computing?* Accessed: Dec. 2019. [Online]. Available: https://www.alibabacloud.com/knowledge/what-is-edge-computing

[42] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," *Sensors*, vol. 19, no. 24, p. 5539, 2019.

[43] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[44] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Advances in Cryptology*, L. R. Knudsen, Ed. Amsterdam, The Netherlands: Springer, 2002, pp. 337–351.

[45] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[46] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020.

[47] S. Kim, "Impacts of mobility on performance of blockchain in VANET," *IEEE Access*, vol. 7, pp. 68646–68655, 2019.

[48] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure Internet-of-battlefield things (IoBT) architecture," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Los Angeles, CA, USA, Oct. 2018, pp. 593–598.

[49] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

**MOHAMMAD WAZID** (Senior Member, IEEE) received the M.Tech. degree in computer network engineering from Graphic Era deemed to be University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He is currently working as an Associate Professor at the Department of Computer Science and Engineering, Graphic Era deemed to be University, Dehradun, where he is also the Head of the Cybersecurity and the IoT Research Group. Prior to this, he was working as an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. He was also a Postdoctoral Researcher at the Cyber Security and Networks Lab, Innopolis University, Innopolis, Russia. His current research interests include information security, remote user authentication, the Internet of Things (IoT), cloud/fog/edge computing, and blockchain. He has published more than 70 articles in international journals and conferences in the above areas. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON SMART GRID, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), the *IEEE Consumer Electronics Magazine*, IEEE ACCESS, *Future Generation Computer Systems* (Elsevier), *Computers & Electrical Engineering* (Elsevier), *Computer Methods and Programs in Biomedicine* (Elsevier), *Security and Communication Networks* (Wiley), and *Journal of Network and Computer Applications* (Elsevier). He has also served as a program committee member of many international conferences. He was a recipient of the University Gold Medal and the Young Scientist Award from UCOST, Department of Science and Technology, Government of Uttarakhand, India. He received the Dr. A. P. J. Abdul Kalam Award for his innovative research works and the *ICT Express* (Elsevier) Journal "Best Reviewer" Award for the year of 2019.

**ASHOK KUMAR DAS** (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, network security, blockchain, security in the Internet of Things (IoT), cloud/fog computing and industrial wireless sensor networks, and intrusion detection. He has authored over 220 articles in international journals and conferences in the above areas, including over 190 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of *KSII Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *IET Communications*. He is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and the IoT in e-healthcare and of *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for the 5G Enabled IoT, and has served as a program committee member in many international conferences. He also severed as one of the technical program committee chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019.

**SACHIN SHETTY** (Senior Member, IEEE) received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, USA. He is currently an Associate Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored and coauthored over 125 research articles in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served on the Technical Program Committee of ACM CCS, the IEEE INFOCOM, the IEEE ICDCN, and the IEEE ICCCN.

**MINHO JO** (Senior Member, IEEE) received the B.A. degree from the Department of Industrial Engineering, Chosun University, South Korea, in 1984, and the Ph.D. degree from the Department of Industrial and Systems Engineering, Lehigh University, USA, in 1994. He is currently a Professor at the Department of Computer Convergence Software, Korea University, Sejong City, South Korea. He is also the Director of the IoT and AI Lab, Korea University. He is one of the founders of the Samsung Electronics LCD Division. He has published over 100 articles in reputable peer-reviewed journals/magazines and for international conferences. His current research interests include the IoT, blockchain, artificial intelligence and deep learning, big data, network security, HetNets, cloud/edge computing, wireless energy harvesting, autonomous vehicles, and LTE-unlicensed. He was a recipient of the 2018 IET Best Paper Premium Award. He received the Headong Outstanding Scholar Prize, in 2011. He was the Vice President of the Institute of Electronics and Information Engineers (IEIE) and is currently the Vice President of the Korean Society for Internet Information (KSII). He is the Founder and Editor-in-Chief of *KSII Transactions on Internet and Information Systems* (SCI/JCR and SCOPUS indexed) and is the Founder of *IEIE Transactions on Smart Processing & Computing* (SCOPUS indexed). He is currently an Associate Editor of IEEE ACCESS, an Editor of the IEEE WIRELESS COMMUNICATIONS, and of the IEEE INTERNET OF THINGS JOURNAL. He is also an Associate Editor of *Electronics*, *Security and Communication Networks*, and *Wireless Communications and Mobile Computing*.