Hindawi
Security and Communication Networks
Volume 2021, Article ID 7142048, 21 pages
https://doi.org/10.1155/2021/7142048

Research Article

Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey

Sanjeev Kumar Dwivedi, Priyadarshini Roy, Chinky Karda, Shalini Agrawal, and Ruhul Amin

Computer Science & Engineering, DR SPM International Institute of Information Technology, Chhattisgarh, India

Correspondence should be addressed to Ruhul Amin; amin_ruhul@live.com

Received 30 April 2021; Accepted 7 August 2021; Published 27 August 2021

Academic Editor: omar cheikhrouhou

Industry 4.0 connects the latest technologies such as cloud computing, Internet of things (IoT), machine learning and artificial intelligence (ML/AI), and blockchain to provide more automation in the industrial process and also bridges the gap between the physical and digital worlds through the cyber-physical system. The inherent feature of IoT devices creates the industry to smart industry (referred to as industrial IoT, i.e., IIoT) through its data-driven decision policies. However, several challenges such as decentralization, security and privacy vulnerability, single point of failure (SPOF), and trust issues exist in the IoT system. Blockchain is one of the promising technologies that can bring about opportunities for addressing the challenges of IoT systems. In this article, we have investigated the integration of IoT with blockchain technology and provided an in-depth study of the blockchain-enabled IoT and IIoT systems. The state-of-the-art research is categorized into data storage and management technique, big data and cloud computing technique (finance and data auditing), and industrial sectors (supply chain, energy, and healthcare sector). The insightful discussion based on the different categories is also presented in the paper. In particular, first, we introduce the IoT and IIoT and then discuss the need for smart contracts in IoT and IIoT systems. Next, we concentrate on the convergence of blockchain and IoT with state-of-the-art research. In addition, this article also provides the open and future research directions towards this era with the highlighted observations.

1. Introduction

Internet of things (IoT) consists of devices and machines equipped with networking capability which can collect data from their environment via various sensors, share them with other devices over the Internet, and carry out analysis (or act) on received data automatically without requiring human intervention [1, 2]. For example, an IoT-based smart home system can use sensors to detect when the electrical appliances need to be turned on (or off) and do so automatically, thereby conserving energy and making life easier for people. IoT has a huge range from sensors and smart consumer devices like smart television, wearable electronics to human and animal implants (e.g., medical implants or identification), and tracking chips for animals [3]. IoT has a very wide range of applications starting from home consumer products, health, agriculture, energy, and transport to any sector that can benefit from integrating IoT. The number of IoT devices is increasing at an explosive rate, but many challenges [4] exist with the same. IoT devices usually have limited processing capabilities and are vulnerable to security attacks [5]. Hence, security is an important aspect while designing the IoT-based system.

The attacks in the IoT-based system are broadly classified into four major categories [6]. The first category is known as the physical attack in which the attacker is physically very close to the network and tries to launch the malicious functionality in the system. Tampering to the IoT device, jamming the radio frequency signals, side-channel attack, and malicious code injection are the common forms of physical attacks. To counter the physical attack, researchers use the physical unclonable function (PUF) [7] for the authentication of IoT devices. In those systems, authentication is mainly dependent on the challenge-response mechanism. The beauty of using the PUF is that it is impossible to clone the exact microstructure of the device. The network attack is the second category of attack in which the attackers try to manipulate the IoT network. The attacker can launch this attack without being close to the network. Traffic analysis attacks, RFID spoofing, Sybil attack, and man-in-the-middle attack are based on the network attack. The use of a secure hash function and authentication technique can prevent this attack [8]. The third and fourth categories of attacks are known as software attacks and data attacks, respectively. In the software attack, the attacker launches the attack by considering the advantages of software present in the IoT system. In contrast, a data attack involves data inconsistency and unauthorized access to the data. The blockchain-enabled privacy-preserving technique efficiently prevents the data attacks [9].

Industrial IoT (IIoT) refers to using IoT technology in industries in order to boost productivity and efficiency in manufacturing and industrial processes [10]. IoT helps industries by improving data collection, machine-to-machine coordination, monitoring and maintenance of hardware, quality control, supply chain traceability, energy management, and overall cost reduction. Connecting everything to the Internet [11] offers a great advantage; sensors can collect and harvest data and then send them to the servers equipped with high processing capabilities for further analysis and make decisions based on which they can then be enacted by other IoT devices [12]. For example, a watering system for crops can use moisture sensors to collect data about soil moisture, send them to a server to figure out when and how much watering is needed, and automatically water the crops. It can even receive information about weather from the Internet and make decision based on it. The blockchain is one of the promising technologies that can solve various issues (trust, adversary attack, etc.) existing in the IoT and IIoT-based systems [13]. Blockchain technology involving smart contracts has a wide range of applications in the IoT and IIoT [14]. IoT is more consumer-oriented (i.e., focuses on smart appliances which would be beneficial to the end-users), for example, a smartwatch that records the pulse rate.

Blockchain is a decentralized peer-to-peer system and distributed immutable ledger [15]. It is a chain of blocks, where block is a piece of information that is made up of transaction, and it contains a timestamp, as well as hash of the previous block which is used to create the hash of the recent block [16]. The blockchain technology is poised to innovate and transform a wide range of applications. It is a database or digital ledger of transactions. In traditional databases, centralized server is used to store the data where centralized authority (as a trusted one) deletes or updates the data, whereas, under the blockchain mechanism, data are shared across a network of multiple computers (or nodes) which run special software to ensure that all data remain identical [17]. As the information is stored across various computers (or nodes) and all the information (blocks) is linked with the previous one, it is difficult for the adversary to change (or delete) the information from a blockchain-based system and, simultaneously, the blockchain helps to securely store and validate sensitive information that maintains the trust in the decentralized network [18].

Smart contracts are an important feature of blockchain technology. The Ethereum system uses the smart contracts for creating the immutable ledger of records. Smart contracts are just like contracts in the real world [19]. The only difference is that they are completely digital, which means that there is an agreement between two or more people in the form of computer code. It is a computer program that is stored inside a blockchain that computers (or the nodes) execute, and, after execution, the ledger gets updated [20]. Smart contracts are self-executing codes when predetermined terms and conditions are met and verified. As they are stored on a blockchain, they inherit some interesting properties; for example, they are immutable and distributed [21]. Figure 1 illustrates the integration of blockchain with the IoT-based system, where data owners send the collected data from IoT devices to blockchain for storage, and data users get the data from blockchain under the required access control mechanism.

A lot of personal information is stored by the devices gathered from different IoT devices [11], which needs to be secure and can only be accessed by the owner and approved and verified stakeholders. The blockchain is one of the probable solutions that can assure integrity and security of data and, with smart contracts, the owner can control sharing of his data on his terms. Major advantages of blockchain technology in IIoT are the decentralization, immutable records, and nonrepudiation of stored information [22]. The general working mechanism of smart contracts with the IIoT-based system is depicted in Figure 2. The smart contract executes the data provided by the IIoT devices and stores them to the blockchain.

1.1. Background Study of the Smart Contracts.

1.1. Background Study of the Smart Contracts. Nick Szabo introduced the smart contracts concept in 1994. According to Nick Szabo, smart contracts are "a computerized transaction protocol which executes the term of contracts." As long as the blockchain is concerned, smart contracts are a piece of code or scripts (or programs) that store inside the blockchain [23]. The scripts are written in a high-level language. Generally, smart contracts scripts are "IF ...this THEN...this" based statement. Smart contracts always execute in a secure environment. The closed environment provides the correctness of execution and integrity of code and data. These contracts also interact with other contracts and other smart contract-based systems. Smart contracts mechanisms for the blockchain-based system are generally based on a deterministic state machine model. The flow of smart contracts cannot be nondeterministic. The reason is that the nondeterministic model achieves the different output (or states) for the same inputs, and if the system behaves in a nondeterministic way, consensus cannot be achieved. All the nodes in a network agree on contracts in the smart contract-based system, either in permissionless or in permissioned blockchain. These contracts define a set of rules stored on all the nodes in the blockchain network. In

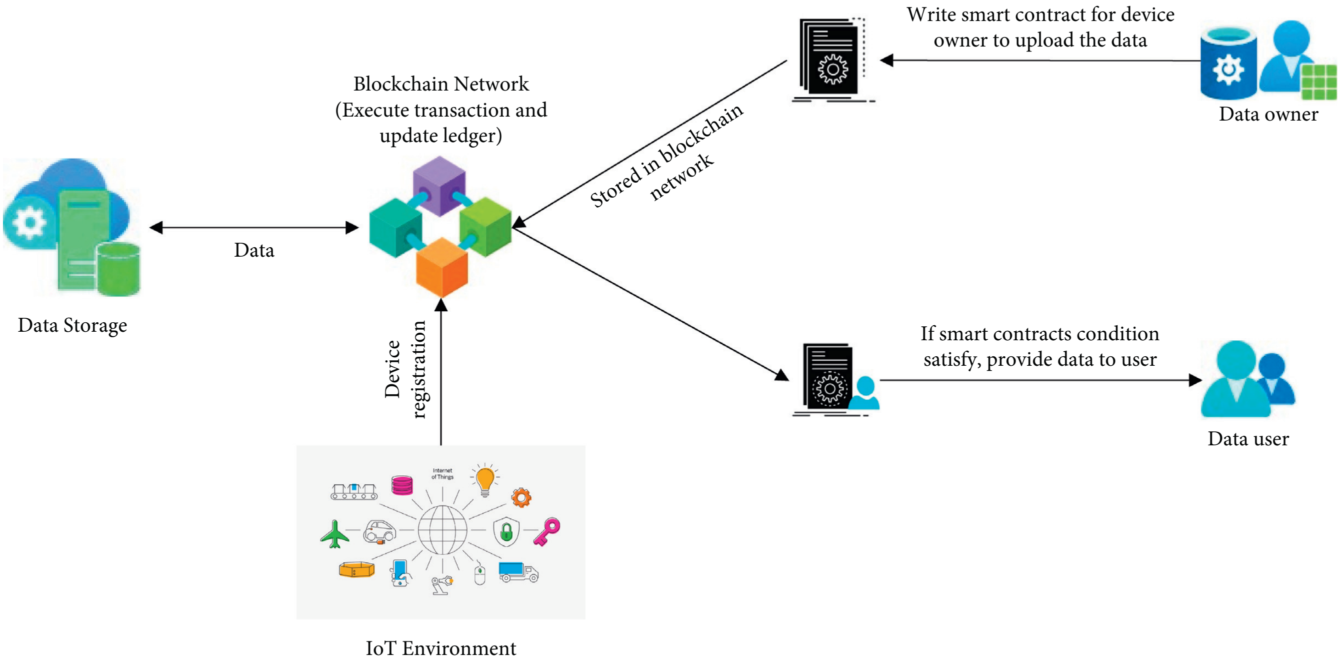
Write smart contract for device owner to upload the data
Data owner
Blockchain Network (Execute transaction and update ledger)
Stored in blockchain network
Data
Data Storage
Device registration
If smart contracts condition satisfy, provide data to user
Data user
Internet of Things
IoT Environment

Figure 1: Integration of blockchain, smart contract, and IoT-based system.

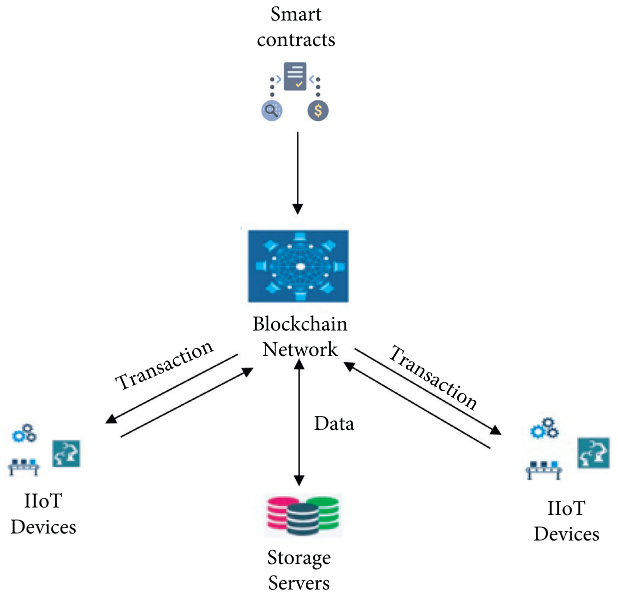

Figure 2: Integration of blockchain, smart contract, and IIoT-based system.

turn, blockchain nodes execute these scripts to perform certain activities or transactions in a network [24]. The systematic architecture of state machine-based smart contract is illustrated in Figure 3. In this directed graph, vertices represent the state, and edges represent the transition from one state to another. The set of actions (Authentication, NoAction, Violation, Permission, etc.) are used for transition from one state to another. For example, if the machine is in state 0 and the action is Authentication, the machine automatically moves from state 0 to state 1, and if it is in state 1 and the action is Violation, the machine automatically moves to state 2, and so on.

The smart contracts are not developed well initially due to the lack of relevant digital systems and theoretical techniques. At that time, there are hardly any digital assets available which are directly manipulated by the contracts. The limitation on computational law is the second big challenge associated with the contracts. The computational law requires the very efficient execution of code, but fast processors' unavailability limits this process. Lastly, the lack of a creditable environment stagnates the development of smart contracts [25]. In the last few years, decentralized blockchain platforms provided a secure and trusted environment for the execution of smart contracts. The technology is changing very rapidly; simultaneously, the attackers are too smart as well. Concerning smart contracts, the attackers try to inject the vulnerabilities in the smart contracts. In 2018, the MAIAN tool was used by Nikolic et al. [26] to perform the security analysis in the smart contracts. They collected the 1million smart contracts for this, and the result revealed that the 34200 smart contracts are vulnerable, where, on average, each contract takes 10 seconds. Nowadays, many formal verification tools are available, which can check the smart contracts and find out the bugs and errors associated with the same. To check the vulnerability in smart contracts code, many researchers and coders use the Oyente tool. This tool generally captures time-stamp dependence, transaction ordering dependence, and reentrancy. Whenever the smart contracts are checked using the Oyente tool, the program variables are replaced by the symbolic variables. Different paths are examined and generate the control flow graph of the contract byte code [27].

The benefits of smart contracts include the faster and more accurate execution, cost reduction, and trust. Due to

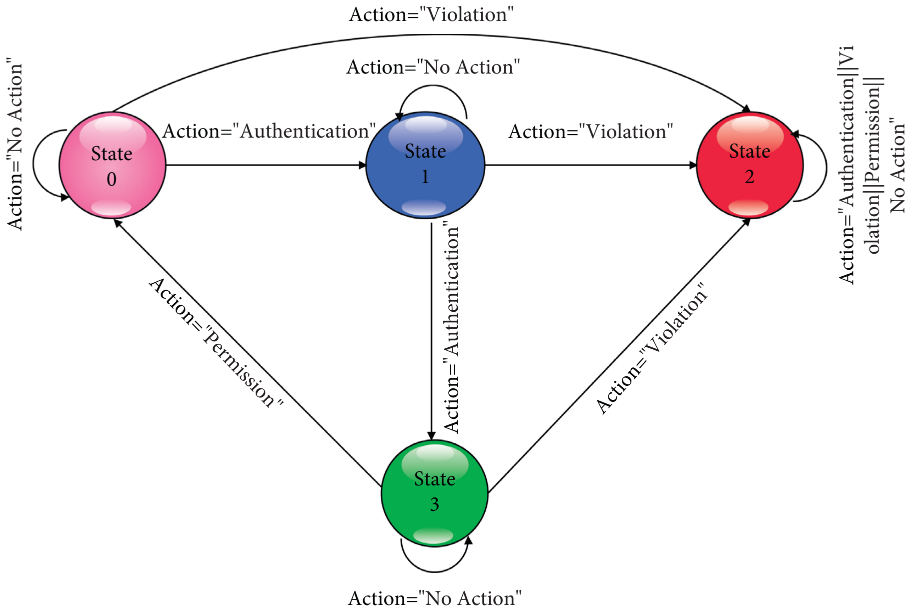

Figure 3: A pictorial representation of smart contracts as a state machine model.

their unique features, many applications use the smart contracts according to their needs and requirements. The diverse scope of the smart contracts includes the following:

(1) In the present time, the costly and risky settlement process hinders the efficiency of transactions processed in the trade settlement system. Due to the involvement of a number of sequential practices, the settlement process is time-consuming and ineffective. For example, on average, more than 20 days are required to settle a leveraged loan. In this context, smart contracts can play a significant role where the transactions are not executed until the predefined conditions are met. They also reduce the risk and decrease the operational cost and settlement time [28].

(2) Similar to the trade settlement, the current mortgage lending relies on outdated processes and frameworks. The loan approvement requires a lot of paperwork and involves many intermediaries (many bank employees and third parties). Each financial document is manually shared with multiple departments, which needs to be signed and tracked by the authorities [29]. Therefore, this whole process requires a lot of human effort and sometimes it is vulnerable because of human mistakes. With the integration of smart contracts, the entire process can be digitized and automated.

(3) The land registry process involves the real-estate agents who examine the land documents such as buyer and seller agreement records and construction data. The involvement of the third party and its manual process lead to the alteration of land documents and, consequentially, fraud. A lot of extra money is also paid to the third party for the settlement of land. Smart contracts-enabled blockchain systems can solve the aforementioned problem, where the blockchain token contains the relevant information of property such as buyer and seller ID and legal description [30].

(4) The insurance industry faces various challenges such as high operational costs and slow claim processing. To further speed up the transaction, the insurance sector can integrate the smart contracts and blockchain, where only a few seconds are required to settle the claims and transfer the funds from one party to another [31]. The IIoT devices play a crucial role for the insurance industry, where the smart sensors are placed on the vehicle (or home) and transfer the real-time data to authorities. After verifying the user's credentials, the smart contracts are automatically triggered to settle the claim.

1.2. *Importance of Smart Contracts in IIoT.*

The smart contract executes automatically, independently, and in a transparent manner (based on the agreement policies) and transfers the ownership of the assets between the two parties without the involvement of a trusted third party (TTP). The detachment of TTP in the smart (digital) contracts saves the extra money and time that are associated with the physical contracts [32]. The key advantage of smart contracts includes the automation, transparency, accuracy, enhanced security, and trust, and the very brief description of the same is discussed below.

The smart contract system creates an environment of trust as the information and logic of the smart contracts are visible to all the participants of the network (based on the permissioned and permissionless network model). In the industrial IoT system, the participants are distributed across the globe, and it is necessary for the industrial sectors to provide full transparency in the system [33]. The smart contracts-based IIoT system is the best option for achieving this. The industrial sectors generally used a third party that maintains a level of trust and imposes security in the system. Due to the TTP, extra costs occurred in the industrial sectors. The smart contract not only removes the TTP but also provides trust in the global trustless environment. The adoption of smart contracts in the industrial sector provides more automation for the contracts. Also. once a contract is deployed over the blockchain network (under the assumption of the majority of consensus), no one can change it. Smart contracts provide more efficiency and speed in the system. By using smart contracts, processed transactions per unit of time are more than the traditional contracts [34]. The IIoT sector (such as healthcare) generates a large volume of data; therefore, to process them, smart contracts are the best-suited option for IIoT sectors.

1.3. Contributions of the Paper. The objective of this paper is to illustrate how blockchain technology solves the issues associated with the IoT and IIoT system. The primary contributions of this paper are summarized as follows:

(1) A very brief introduction of IoT and IIoT is first provided in the paper. Meanwhile, the various research challenges associated with the IoT and IIoT are also outlined in the paper.

(2) This paper highlights the importance of smart contracts in the IIoT sector.

(3) We classify the existing solutions into the three major categories, data storage and management technique, industrial sector, and big data, cloud computing, and network security management technique, and discuss each of them.

(4) We provide a state-of-the-art comparison of different categories of the presented solutions in a tabular form, concerning the technology used, possible solutions, and the implementation remarks.

(5) Based on our comprehensive survey, this paper provides the open research issues and our observations that can be useful for the development of blockchain-based IoT and IIoT systems.

1.4. Organization of the Paper. The paper is organized as follows: Section 1 introduces our paper by describing the IoT and IIoT systems, as well as the need for blockchain in those systems. Section 2 discusses the adoption of blockchain technology in different application areas including the healthcare, supply chain system, and IoT. The state-of-the-art researches based on the different categories are presented in Section 3. Sections 4 and 5 elaborate the open research issues, as well as our observations from the state-of-the-art research. Finally Section 6 provides the conclusion of the paper with future research.

2. Adoption of Blockchain Technology in Application Domains

The blockchain technology is applicable in different domains ranging from health sector and supply chain management system to IoT, smart and autonomous vehicles, and so forth. This technology is applicable to handling the various challenges that are faced by the traditional system; for example, the functionality of the system depends on the trusted third party, as well as many more.

2.1. Health Sector. Due to the continuously increasing world population, the health sector becomes one of the most important social-economic problems. The numbers of hospitals and resources in the hospitals are very limited and, in some areas, there are no hospitals. Currently, wearable health devices play an important role in remote patient's treatment. These devices continuously measure the patient and collect the health data for the required treatment. The advantage of this technique is that the healthcare team and the doctors access the data remotely at any time. But the privacy and security of these wearable devices are a challenging task. Incorporating the blockchain technology in the health sector potentially overcomes few of the challenges that are faced by this sector. In the continuation of it, the authors in [35] proposed a new model for monitoring remote patients using the patient agent-based blockchain system. The health-related data are collected by the wearable sensors and transmitted to the patient agent that further breaks the data into small blocks before storing them in the blockchain network. Meanwhile Xia et al. [36] suggested a blockchain-based secure data-sharing scheme for the private health-data management system. The suggested protocol used identity-based authentication and key-agreement protocol. To manage the individual health records and support the secure sharing of patient's data across the different hospitals, insurance companies, and medical centers, the blockchain-based solutions have been proposed by the authors [37]. This model guarantees the security and privacy of health data. Furthermore, an attribute-based signature scheme to manage the decentralized health records based on the blockchain mechanism gas been proposed by Sun et al. [38]. This scheme verifies the authenticity of the health data and also preserves the privacy of the health-data owner. Griggs et al. [39] suggested that the smart contracts enabled the permissioned blockchain platform to monitor the remote patients. The medical sensors collect the data and send them to the smart contracts for further analysis. The PBFT consensus mechanism is used by this system for the block validation. The patient-centric approach for sharing medical information among the different hospitals and research institutions is proposed by the authors in [40]. The privacy of the patient's medical data is ensured by the system.

2.2. Supply Chain Management. In the supply chain management system, a product consists of multiple parts that are provided by the different manufacturers. In the entire process, if any manufacturer or any other entity submits the low-quality parts (or forged parts), then it is quite expensive to detect the low-quality parts. The integration of blockchain with IoT solves the above-mentioned issue. The unique ID of every part is attached with the timestamp and stored in the blockchain network, which is traceable at any time. In [41], the authors adopted the blockchain mechanism for the authentication of every part that is provided by the owner. Meanwhile, in [42], the authors integrate the blockchain with the IoT to trace the products. They used the Ethereum platform for it. The suggested method achieves the data provenance in the supply chain management system. The authors in [43] showed that the integration of IoT with the blockchain mechanism helps to reduce the cost and risk and fasten the supply chain process. Moreover, to improve the quality and its services, machine learning and the blockchain mechanism are combined in [44]. To provide the traceability system for an agrifood supply chain, the authors in [45] used the radio-frequency identification (RFID) with the blockchain mechanism. The system provides transparency and product traceability. The double marginalization and information asymmetry are the problems associated with the supply chain system. To solve this kind of problems, Nakasumi [46] proposed a solution based on the homomorphic encryption method for the security and privacy of the user's data. In [47], the authors proposed the blockchain-based secured information-sharing scheme for the supply chain system. The two-phase validation protocol (transaction and block validation) was designed by the authors to enhance the security of the proposed system. To show transparency in the supply chain system, smart contracts were designed and the Ethereum blockchain platform was used for its evaluation.

2.3. Internet of Things (IoT). Generally, IoT devices are data-centric devices where data are sent and uploaded by a huge number of devices. Both the device and data can be targeted by the attackers. The attacker sends the falsified data to the network. In the IoT-based system, data can be personal and sensitive. Therefore, the integrity and privacy of data are the top priority for these systems. Blockchain is believed to solve this issue. The characteristics of blockchain attracted the attention of researchers. In the continuation of this, Gu et al. [48] suggested the malware detection system based on the consortium blockchain which is further based on the statistical analysis method. In order to reduce the false-positive rate, they adopted the multiple marking function and fuzzy comparison method. Further, a blockchain technology-based firmware update methodology was proposed by the authors in [49] for the protection of embedded devices in the IoT system. To manage the IoT devices, the authors in [22] suggested the blockchain technology-based access control system. Their system consists of a wireless sensor network, agent node, smart contracts, management hub, managers, and blockchain network. The system is scalable and preserves transparency. The authors in [50] suggested the cloud blockchain for the IoT system to manage the resource allocation scheme. But the disadvantage of this scheme is that the smart contracts for resource allocation are not investigated. The IoT is also applicable in the 5G era, where millions of devices are connected with each other. To solve the privacy issue in the 5G environment, Fan et al. [51] proposed the blockchain-based data-sharing and privacy-preserving scheme.

3. State-of-the-Art Research

With growing innovations and implementation of IoT in different fields such as industries, health [52], supply chain [47], and VANET [53], the huge volume of data is generated from the above application areas, and it is continuously growing. The state-of-the-art research is broadly classified into four major categories: data storage and management technique (discussed in Subsection 3.1), industrial sectors (discussed in Subsection 3.2), big data, cloud computing technique, and network security management technique (discussed in Subsection 3.3), and the various techniques adopted in the healthcare sector (discussed in Subsection 3.4), which are shown in Figure 4.

3.1. Data Storage and Management Techniques. The management and storage of these data for ensuring security, integrity, traceability, and immutability as well as the trusted exchange of data are of utmost importance in current times [13]. These requirements of IIoT-based systems are easily met by blockchain technology. Blockchain technology can be expensive due to the involvement of multiple agents (or nodes), and it requires high processing and computational power. Kurt Peker et al. [54] explored the cost of storing the collected data in blockchain for low computation power in terms of storage and processing. Their work presented that overwriting new data is more cost-efficient than appending new data. They also demonstrate that storing the data in one variable within a smart contract is more cost-efficient than storing the same in an array, but the difference is insignificant. This work provides an idea about how one can reduce cost without compromising data storage in the blockchain.

A huge amount of data generated by the IoT devices is generally stored in a centralized cloud system, but it requires trust in the central authority, and there can exist a single-point-of-failure (SPOF) problem that affects the functionality of the whole network. Moreover, the data exchange between the two parties (or nodes) takes place through the third party. As a result, all the nodes must trust the third party. Manzoor et al. [55] proposed a framework with a distributed cloud server and blockchain-enabled smart contact to ensure security and integrity of data, and a proxy reencryption technique is used while exchanging the data. The distributed cloud solves the problem of centralized cloud and SPOF. The smart contract enables the dynamic data exchange between the owner and the receiver with some preagreed policies and rules to ensure fair, secure, and trusted exchange. These contracts are mined into blockchain for immutability and traceability. However, they utilized the elliptic curve cryptography- (ECC-) based implementation, and the communication and computation costs are high in their method. In addition to this, the authors also did not present any security validation of the framework.

Pan et al. [56] proposed a framework called EdgeChain for improving the scalability of the centralized cloud by deploying edge computing. They used a permissioned blockchain that ensured only authorized nodes are part of

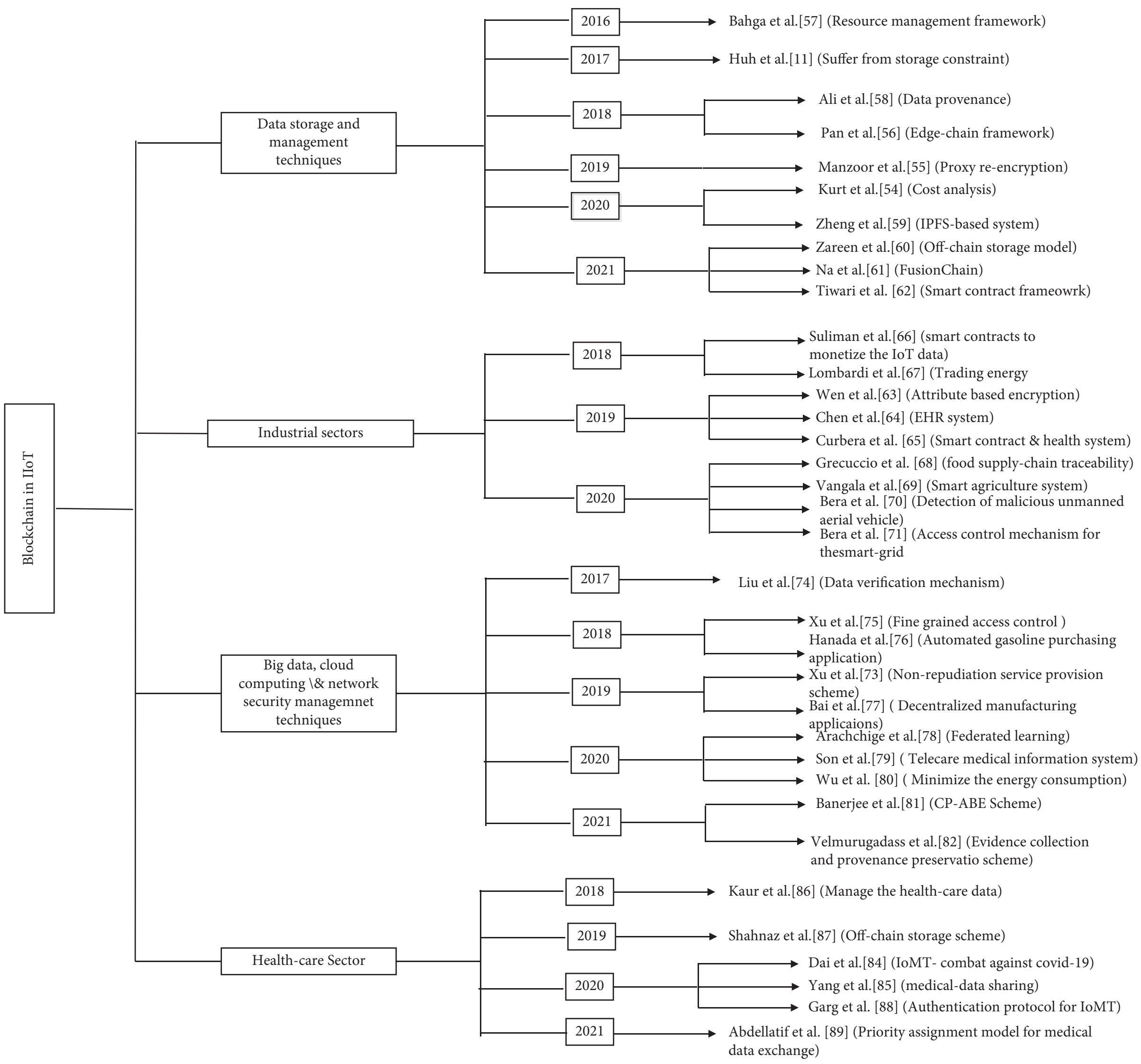
Blockchain in IIoT
Data storage and management techniques
2016
Bahga et al.[57] (Resource management framework)
2017
Huh et al.[11] (Suffer from storage constraint)
2018
Ali et al.[58] (Data provenance)
Pan et al.[56] (Edge-chain framework)
2019
Manzoor et al.[55] (Proxy re-encryption)
2020
Kurt et al.[54] (Cost analysis)
Zheng et al.[59] (IPFS-based system)
2021
Zareen et al.[60] (Off-chain storage model)
Na et al.[61] (FusionChain)
Tiwari et al. [62] (Smart contract frameowrk)
Industrial sectors
2018
Suliman et al.[66] (smart contracts to monetize the IoT data)
Lombardi et al.[67] (Trading energy
2019
Wen et al.[63] (Attribute based encryption)
Chen et al.[64] (EHR system)
Curbera et al. [65] (Smart contract & health system)
2020
Grecuccio et al. [68] (food supply-chain traceability)
Vangala et al.[69] (Smart agriculture system)
Bera et al. [70] (Detection of malicious unmanned aerial vehicle)
Bera et al. [71] (Access control mechanism for thesmart-grid
Big data, cloud computing \& network security managemnet techniques
2017
Liu et al.[74] (Data verification mechanism)
2018
Xu et al.[75] (Fine grained access control)
Hanada et al.[76] (Automated gasoline purchasing application)
2019
Xu et al.[73] (Non-repudiation service provision scheme)
Bai et al.[77] (Decentralized manufacturing applicaions)
2020
Arachchige et al.[78] (Federated learning)
Son et al.[79] (Telecare medical information system)
Wu et al. [80] (Minimize the energy consumption)
2021
Banerjee et al.[81] (CP-ABE Scheme)
Velmurugadass et al.[82] (Evidence collection and provenance preservatio scheme)
Health-care Sector
2018
Kaur et al.[86] (Manage the health-care data)
2019
Shahnaz et al.[87] (Off-chain storage scheme)
2020
Dai et al.[84] (IoMT- combat against covid-19)
Yang et al.[85] (medical-data sharing)
Garg et al. [88] (Authentication protocol for IoMT)
2021
Abdellatif et al. [89] (Priority assignment model for medical data exchange)

Figure 4: Classification of the state-of-the-art research.

the network. The credit-based resource management scheme (resource obtaining depending on rules, priorities, and past behavior), along with the smart contracts for monitoring, controlling, and regulating IoT devices behaviors with defined rules, is used. It also keeps track of resource pool and resource sharing. However, they utilized the centralized cloud server. As a result, the functionality of the system depends on the centralized cloud server, and they did not pay much attention to ensuring fair and trusted exchange of resources. This framework is expensive as edge computing has a complex infrastructure, which raises the question of maintenance. The efficient and frequent computing-resource trading for edge-assisted IoT is still an open issue.

The authors in [58] focused on data provenance as it would confirm the authentication of data and enable their reuse. There is a private blockchain with different types of smart contracts, which guarantees provenance receipt to actual data in the cloud. The device registration contract (unique address), device provenance contract (authenticating device), data provenance contract (data are hashed and stored in blockchain along with a timestamp and public key), and traffic provenance contract (checking for valid data range, sampling interval, size of data for each sample, data rate, and the destination address) are used by them. All this interacts with a centralized cloud server that stores the actual data, whereas the blockchain stores only the device metadata. Furthermore, their work also did not pay much attention to fair and trusted data and the exchange between the owner and requester as well as the centralized cloud server.

The work of Bahga and Madisetti [57] was more inclined towards IIoT resource management. They proposed a framework called BPIIoT to provide trustworthy centralized cloud resources securely. The framework consisted of a public blockchain in which each IoT device would have an account and wallet for easy data exchange. The smart contract (with the rules and policies) eliminates third-party involvement. It also interacts with the centralized cloud where the actual data is stored. The blockchain keeps track of the inventories, manufacturing information of the product, and machine maintenance. Once a smart contract is employed and a transaction is made, it is mined into the blockchain; therefore, it becomes immutable and traceable. The proposed work utilized the centralized cloud and has employed public blockchain.

Huh et al. [11] worked on synchronization and communication of IoT devices when thousands of them are connected to a network, thereby ensuring scalability. They proposed building an IoT system using blockchain. All the devices will be configured on the blockchain and smart contracts will be used for monitoring the behavior of the IoT devices. Meter contract would record the performance data of the IoT device and send them to the blockchain, whereas policy contract states about the working of the devices and key management technique are used to keep public key and signatures of the devices for device authentication. The devices do not have large storage to store data, and, for doing this, they utilized the third party which would compromise the security of the system. For both large storage and security, the cost will be very high and infeasible for small devices. Tables 1 and 2 show the brief overview of different data storage and management techniques used for IIoT-based system.

Zareen et al. [60] suggested the off-chain storage mechanism (i.e., IPFS) with the blockchain. The model utilizes the off-chain storage model for storing the IoT data and node credentials. Moreover, the blockchain is used to storing the hash that the IPFS provides. A prototype for the service model has been proposed between the consumers and service providers to share the services. Additionally, the secure hash algorithm (SHA-256) does the service verification. In case of dispute between the consumers and service providers, a smart contract is designed to resolve it. Similarly, Na and Park [61] proposed a protocol named FusionChain, which utilizes the IPFS to solve the storage issue faced by blockchain technology. Their mechanism adopts the practical byzantine fault tolerance consensus mechanism, which does not have high computational power for adding a new block in the blockchain nodes. Moreover, public key infrastructure-based encryption schemes are used for ensuring the security and privacy of IoT data. Their experimental results show that the computational power required for creating a blockchain is lower than those of the traditional platforms such as bitcoin and Ethereum. The paper in [59] proposed an IIoT data management framework based on the blockchain and IPFS. The authors have suggested the proof-of-concept-based implementation to achieve better security for IIoT data that further utilize the IOTA protocol and IPFS. The data-handling unit, IPFS, IOTA Tangle, and IIoT data consumers are the central unit of their system. In this paper, the authors only provide the theoretical analysis of the suggested protocol. The authors in [62] suggested a decentralized architecture to incorporate the challenges faced by the smart cities, which is further based on the combination of IoT, smart contract, blockchain, and IPFS. The simulation of the proposed prototype is done using the Ganache CLI *v*6.9.1, Solidity *v*0.5.16, Truffle Suite *v*5.1.15, and Remix IDE. In this work, the authors discuss the prototype model and the results obtained from their simulations. However, they do not discuss the underlining work of the prototype model and cryptographic mechanism.

3.2. Industrial Sectors. Wen et al. [63] proposed an improved structure of blockchain-based supply chain system (BSCS) which ensures the security of data, transparency, and access control policies in the chain by setting access policies to smart contracts. The BSCS consists of 3interdependent parts: supply chain management, supply chain network structure, and supply chain business process. In BSCS, attribute-based encryption (ABE) is used as the supply chain network to address data-sharing, information occlusion, and lack of supervision issues. Business processes are enabled by BSCS to determine which core processes should be connected and integrated into the supply chain system by using smart contracts. The entities of the system may interact with the network without manual operations and efficiently carry out the flow of goods by using IIoT as the process interface at the boundary in the blockchain. Early detection of SPOF issues in the network is also addressed.

Chen et al. [64] proposed a blockchain-enabled searchable encryption scheme for electronic health records (EHRs) sharing. It is a logical approach that ensures data integrity without additional verification, standardized auditing procedures, and some formalized contracts for accessing the data. This framework securely facilitates data-sharing and provides much convenience to patients and also allows information-sharing among researchers. It also supports complex queries by different healthcare agents to request permission for accessing the records. A smart contract is used in the proposed work to trace rewards and transaction fees and also ensures that the owner of the data is paid as long as they reveal the transcript, which allows other users to search the database. The EHRs are created by data owners (human or organization). The data owner then constructs the index through complex logic expressions and creates a smart contract to describe how one can search the index and then it is stored in the blockchain for the respective EHRs. The symmetric encryption algorithm is used to encrypt the EHRs and is stored in a cloud server. The data owner authorizes the user who needs the required EHR. However, this scheme lacks the effective countermeasure to punish the dishonest and malicious entity.

Curbera et al. [65] focused on the use of blockchain for data exchange across the health ecosystem. Several cases of healthcare and life sciences are presented, including patient consent, outcome-based contracts, data exchange (related to the health), next-generation clinical trials, and payments and claims, where, by the adoption of blockchain technology, current practices can be disrupted and transformed. The authors proposed a blockchain-based architecture for providing the secure services for the above-mentioned use cases. Described architecture adds a layer of data encryption, and data access is restricted to authorized users only. Encryption of data stored on the ledger is done with a data key, and only authorized users are given access to the decryption key. The decryption key will be expired or will be no longer available

Table 1: Comparison table based on different parameters of the existing data storage and management technique.

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
1.	[57]	2016	(a) Smart contract, (b) centralized cloud server, (c) IIoT	Framework called BPIIoT to make the centralized cloud resource management and access trustworthy information. Deployed a public blockchain with IoT devices as nodes and smart contract with the rules and policies for secure data exchange	(a) No performance analysis and measurement, (b) centralized cloud server adopted and therefore SPOF problem still remains	(a) Implement distributed cloud, (b) use private blockchain instead	Should present with performance analysis of the proposed framework
2.	[11]	2017	(a) Smart contract, (b) IoT	Framework for synchronization and communication of IoT devices when thousands of them are connected to a network. In this, all the devices will be configured on the blockchain and smart contracts will be used for monitoring the behavior of the IoT devices	(a) No attention on fair and trusted exchange of resources, (b) storage problem, (c) lacked on part of network performance and security optimization	(a) Use smart contract for data exchange as well, (b) use distributed cloud for data storage	Network performance and security compromised by not considering storage problems of IoT devices
3.	[58]	2018	(a) Smart contract, (b) centralized cloud server, (c) IoT	Framework works for data provenance. There is a private blockchain with different smart contracts with specific purpose, which guarantees provenance receipt to actual data in the cloud	(a) No attention to fair and trusted data exchange, (b) centralized cloud server for actual data storage, (c) high computational cost	(a) Use smart contract for data-sharing, (b) use distributed cloud storage	Increased use of smart contract has increased cost of computation
4.	[56]	2018	(a) Smart contact, (b) edge computing, (c) centralized cloud server, (d) IoT	Framework called EdgeChain for improving scalability of the centralized cloud by deploying edge computing. They used a permissioned blockchain smart contract for monitoring, controlling, and regulating IoT devices behaviors	(a) Centralized cloud server, (b) no steps for fair and trusted exchange of resources, (c) complex, expensive, and space-intensive	(a) Use distributed cloud, (b) use smart contracts for data-sharing	Edge computing is expensive and complex to implement
5.	[55]	2019	(a) Smart contract, (b) proxy reencryption scheme, (c) distributed cloud server, (d) IoT	Framework with distributed cloud server and blockchain smart contract, providing guaranteed services such as security and integrity of the data during their exchange; they used proxy reencryption	(a) Communication and computation costs are high, (b) security validation of the protocol is not present, (c) problems in scalability	Use some other encryption methods to reduce computation cost and improve scalability	Present with formal security validation for more credibility on the proposed work

to the user, when the access is revoked. Hence, privacy and security of data are achieved to a greater extent. Moreover, their framework achieves scalability and data integrity and provides more flexibility to the participating entities. The additional layer of encryption included in architecture adds to the overall latency of chain code calls.

Table 2: Comparison table based on different parameters of the existing data storage and management technique (cont…).

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
6.	[54]	2020	(a) Smart contract, (b) array	Explored the cost of storing the collected data in blockchain for low computation power in terms of storage and processing; for this, they worked on different ways to store data	Key generation and communication protocols need to be addressed	Use smart contracts for generation of keys and store them through blockchain	Solidity (Ethereum) and ganache can be used
7.	[59]	2020	(a) IOTA Tangle, (b) IPFS	IOTA Tangle and IPFS-enabled decentralized IIoT data management framework based on the proof-of-concept protocol	Only the theoretical analysis of the solution	Smart contract for this system can be designed for sharing the IIoT data and storing them in the IPFS	Solidity language can be used for writing the smart contracts
8.	[60]	2021	(a) Smart contract, (b) IPFS, (c) elliptic curve integrated encryption	Off-chain storage and blockchain-enabled service model for the IoT system in which node credentials and records are stored in IPFS	Carelessly investigated the smart contract implementation	Remix IDE and solidity-enabled contracts can be designed	Proof-of-authority model consumes less GAS than the proof-of-work model
9.	[61]	2021	(a) Golang, (b) IPFS, (c) public key infrastructure	FusionChain: a decentralized lightweight framework to store the IoT data and solve the memory required to store a full copy of blockchain in the device	The formal verification of smart contracts is not done	The tools such as Oyente and SmartChecker can be used to provides the full analysis of the contract	Only 49MB of memory and 6%of CPU on the ARM core are required for the consensus process
10.	[62]	2021	(a) IoT, (b) IPFS, (c) smart contract	A decentralized prototype model for smart cities using IoT, blockchain, and IPFS	In-depth study of the proposed prototype model has not been done	Cryptography primitives can be used to provide more security, privacy, and trust in IoT-enabled smart cities applications	Formal security validation tools can be used to verify the security protocols

Suliman et al. [66] proposed a smart contracts-based blockchain solution to monetize the IoT data systematically with automated payment that does not involves the third party. The proposed architectural design considers four components, each possessing Ethereum addresses: IoT device, device owner, MQTT broker, and customers. Furthermore, scripting of smart contracts is done using the Ethereum blockchain. The ether token (cryptocurrency) is used for payment purposes. The proposed system comprises code (written in Solidity language), which is used by device owners to set the rules, and conditions for automating the sale of the data of IoT devices owned by them. If the end-user wants to use the data, they can interact and call the smart contracts without the third party. Furthermore, an MQTT broker hosted in the cloud collects and aggregates the data generated by IoT devices. It also authenticates valid customers through the smart contracts. The hosting in the cloud environment of the MQTT broker provides scalability, reliability, and accessibility to all the customers with low latency. A payment (ether) that is based on use time of the device is directly deducted from customer balance upon successful data access and is sent to the IoT device owner. The gas consumption (ether) when a smart contract calls the function is paid by the customer. It is not debited from the funds within the smart contract.

Lombardi et al. [67] proposed a reliable, decentralized, and cost-effective infrastructure for trading energy, which was further based on smart contracts-enabled blockchain. Here, blockchain stores the energy transactions. Blockchain and smart contracts-based architecture is presented for transactive grids, which offers functionalities like managing energy trading policies, isolating devices with known vulnerabilities, carrying out energy auctions within the grid, and so forth. Security is improved in the presented work. Presented architecture also provides new relevant functionalities such as energy trading policy management. Tables 3 and 4 show the brief overview of existing IoT-enabled industrial sectors.

TABLE 3: Comparison table based on different parameters of the existing IoT-enabled industrial sectors.

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
1.	[66]	2018	(a) Smart contract, (b) MQTT broker to collect data	Proposed a blockchain with smart contracts to monetize the IoT data systematically with automated payment without involvement of third parties. MQTT broker is used to collect and aggregate the data generated by IoT devices.	Customers need to pay for ether gas consumption when smart contracts call the function, instead of funds	Using funds of smart contract to reduce gas consumption of customer	Ethereum-enabled smart contracts can be used
2.	[67]	2018	(a) Smart contract, (b) smart meters within smart grids, (c) Byzantine fault tolerance	Proposed decentralized and cost-effective infrastructure for trading energy, based on smart contracts enabled blockchain for transactive grids. The presented architecture provides relevant functionalities such as energy trading policy management.	Real-time realization of the proposed protocol is required	Smart contracts enable permissioned blockchain to be used	Hyperledger fabric and Raspberry Pi devices
3.	[63]	2019	(a) Smart contract, (b) attribute-based encryption	Blockchain with ABE is used as the supply chain network to address data-sharing, information occlusion, and lack of supervision issues. Entities of the system interact automatically and efficiently and carry out the flow of goods by using IIoT as the interface. Smart contract is used in business processes.	Increased blocking time as the number of nodes increases	Use off-chain storage mechanism to store the data in case of increasing number of nodes	Solidity (Ethereum-based) and IPFS can be used
4.	[64]	2019	(a) Smart contract, (b) Symm. Encryption algorithm	A system for EHRs-sharing, a logical approach ensuring data integrity and security. Data is stored by constructing indexes using complex expressions. Symm. Encryption algorithm is used to encrypt the EHRs.	Lacks the effective countermeasure to punish the dishonest and malicious entity	Some effective countermeasures for malicious entities	A secure searchable encryption for EHRs
5.	[65]	2019	Smart contract	Several cases of healthcare and life sciences have been presented followed by a platform to enable those use cases. Additional layer of data encryption is added. Scalability and integrity are achieved to a greater extent.	Addition of extra data encryption layers add-on to latency in chaincode calls.	Instead of additional layer for encryption, some strong encryption algorithm	Real-time implementation based on hyperledger fabric is required

Table 4: Comparison table based on different parameters of the existing IoT-enabled industrial sectors (cont…).

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
6.	[68]	2020	(a) IoT, (b) Ethereum blockchain, (c) Web3API	Integration of blockchain and IoT for food supply chain traceability	All the data are stored on blockchain; therefore the load on the Ethereum node can be increased.	IPFS-enabled solutions can be used to achieve the full decentralization	External blockchain test network with the integration of IPFS module can be used
7.	[69]	2020	(a) IoT, (b) blockchain, (c) cloud center	Integration of blockchain and IoT to develop a smart agriculture system	The authors do not present the required security protocols to develop the smart agriculture system.	Cryptographic primitives can be used to develop the security protocols	Smart contracts can be designed to automate the agriculture system
8.	[70]	2021	(a) IoD, (b) blockchain, (c) cloud center, (d) ground station server	An access control protocol for detection of malicious unmanned aerial vehicles in IoD environment	All the transactions are stored in the peer-to-peer cloud servers which maintain the blockchain. Therefore, full decentralization was not achieved by this solution.	Off-chain storage mechanism can be used to provide the full decentralization	AVISPA tool utilized by the authors for the validation of security protocols
9.	[71]	2021	(a) IoT, (b) blockchain, (c) smart grid	A framework that combines the IoT and blockchain to provide an access control mechanism for the smart grid	Most of the sensitive data is stored on the blockchain. Therefore storage cost may be increased.	Various off-chain storage mechanisms can be used, which solve the storage problem of blockchain network	Experimental results shows that the computational cost of service providers is 3.303 msec, and communication cost is 3040 bits

The authors in [68] developed a framework that directly integrates the IoT and blockchain (Ethereum) without relying on the TTP. The food-chain application (monitoring the temperature of fish products) is considered as a use case. The solution is implemented in Ethereum-enabled smart contracts, and Web3API does the transactions on the real Ethereum network. In the proposed solution, devices do execute the mining procedure, and also there is no need to store the entire blockchain. Vangala et al. [69] presented the generalized architecture for smart agriculture based on blockchain technology. In this paper, the authors discuss the essential security requirements and the possible security threats for developing the smart agriculture system. After this, they provide the crucial functionalities and the various challenges that arise when developing the blockchain-based decentralized smart agriculture system. The generalized architecture of their system uses the cloud servers to maintain the full copy of the blockchain. Moreover, the future research challenges and open issues are also presented in the paper. Bera et al. [70] proposed an access control protocol for the detection and mitigation of unmanned aerial vehicles using the private blockchain in the Internet-of-drones (IoD) environment. In this work, the authenticated transactions are collected by the ground station servers and a valid block is created based on the practical Byzantine fault tolerance consensus algorithm. The Real-Or-Random oracle security model, with the AVISPA as a formal security validation tool, is used for formally analyzing the protocol. The solution uses elliptic curve cryptography (ECC), hash functions, and a symmetric-key encryption algorithm to achieve mutual authentication between the drones and station servers and supports the session key agreement. Furthermore, the incorporation of blockchain provides the desired trust, decentralization of authenticated transactions, and desired level of security for IoD. Similarly, a paper in [71] designed an access control scheme named DBACP-IoTSG for the IoT-enabled smart-grid system based on blockchain technology. In this protocol, the sensitive data collected by the smart meters are sent to the service providers through public channels. To ensure the security of data, cryptographic primitives such as ECC and hash functions are used. After this, the service providers create a valid block based on the voting consensus mechanism. The security protocol is verified informally and formally based on the AVISPA validation tool, and it is confirmed that the protocol is resilient against various security attacks, such as smart meter physical capture attack, impersonation attack, and many more.

3.3. Big Data, Cloud Computing, and Network Security Management Techniques.

The functionality of resource-constrained IIoT can be extended using on-demand service provisioning schemes in which service providers can provide local lightweight terminal services via the network [72]. However, this poses various security challenges in untrusted distributed IIoT systems as dishonest providers can deny service provisions or client can deny usage, for their own benefit. Tables 5 and 6 show the brief overview of big data, cloud computing, and network security management technique.

Xu et al. [76] proposed a blockchain-enabled fair non-repudiation service provisioning scheme where blockchain is utilized as a service publisher and an evidence recorder.

Table 5: Comparison table based on different parameters of the existing big data, cloud computing, and network security management technique.

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
1.	[73]	2017	(a) Smart contract, (b) cloud storage	Framework for reliable data integrity verification for both the data owners and the data consumers, without relying on any third-party auditor (TPA)	(a) Did not fully implement proposed protocols, (b) test environment is small	Implement all the protocols and test on a larger environment	Implementation of all proposed protocols has not been done
2.	[74]	2018	(a) Smart contract, (b) edge computing	Compared to centralized CAC, their scheme achieves the fine-grained access control and decentralized authorization	Storage-capacity constraint may be one of the problems in the proposed scheme	Fully distributed storage scheme is one of the possible solutions	Decentralized capability-based access control
3.	[75]	2018	(a) Smart contract, (b) IoT	Studied the use of smart contracts for addressing transparency, longevity, and trust by designing and evaluating framework for an automated gasoline-purchasing application	(a) Low transaction throughput, (b) 95 percentile transaction latency of the order of hours, (c) limited applications	Use different consensus mechanism to reduce transaction time	High delay in transactions
4.	[76]	2019	(a) Smart contract, (b) Ethereum, (c) homomorphic hash functions	Fair nonrepudiation service provisioning scheme using blockchain as service publisher and evidence recorder to prevent service providers and clients from dishonestly denying service or usage	IoT devices are not directly connected to blockchain network; instead they communicate through an arbitration node	IPFS mechanism can be used for storing the IIoT data	Dispute resolution in case of storing massive amounts of data on servers has not been considered
5.	[77]	2019	(a) Smart contract, (b) distributed hash table	Address security, trust, and island connection problems in decentralized manufacturing applications using on-chain and off-chain networks	Not fully decentralized	Use fully decentralized architecture instead of selecting only a few nodes to maintain blockchain activities	On-chain network used for transaction, off-chain networks used for other tasks

They used blockchain for recording the interactive evidence of service providers and IIoT clients. Each service is divided up into two nonexecutable parts and both parts are delivered separately via on-chain and off-chain channels. The larger part of the program is delivered off-chain to reduce cost and expose code. After recognizing evidence of this, the remainder is delivered on-chain for fair nonrepudiation purposes. A very lightweight service verification methodology using the homomorphic hash technique is designed, which can verify using only the on-chain evidence, and to resolve disputes between the clients and service providers, smart contracts are used. The work provides a scheme to tell whether a promised service has been provided or not but dispute resolution in case of storing massive amounts of data on servers has not been considered.

Bai et al. [77] proposed addressing security, trust, and island connection problems in decentralized manufacturing applications using lightweight blockchain-based architecture consisting of on-chain and off-chain networks. Distributed hash tables among nodes are used for off-chain network. The smart contract is used as a service contract between consumers and on-demand manufacturing service providers. The transactions are digitally signed for the admission control and activities like programmable licenses and so forth that are performed via the on-chain network, while storage and complex data processing is handled via the off-chain network. Although their scheme utilizes blockchain, the architecture is still partially decentralized.

Privacy and security are major concerns in large-scale IoT applications. Access authorization plays a critical role in resource-sharing and information protection. Access control using a centralized authorization server poses problems, such as SPOF. A blockchain-enabled decentralized capability-based access control (CAC) scheme for

Table 6: Comparison table based on different parameters of the existing big data, cloud computing, and network security management technique (cont…).

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
6.	[78]	2020	(a) Smart contract, (b) Ethereum blockchain, (c) federated ML, (d) IPFS	Framework combines smart contracts (Ethereum blockchain), differential privacy, and federated ML to enforce trustworthiness and privacy on IIoT data. The work is simulated using Python and socket programming.	There is significant latency	Investigate different approaches to reduce latency which further improves the efficiency of the system	Ganache *v*2.0.1 is used as a test network for the local experiments
7.	[79]	2020	(a) IoT, (b) blockchain, (c) cloud server	Blockchain and cloud assisted secure authentication protocol for the IoT-enabled telecare medical information system	Service providers store the data on cloud servers. Therefore, SPOF may exist in the system	IPFS mechanism can be used as distributed storage	Protocol simulation shows that the computational cost is 41.6587*msec*, and communication cost is 3456*bits*
8.	[80]	2020	(a) IoT, (b) blockchain, (c) cloud server, (d) edge computing server	A blockchain-enabled framework to minimize the energy consumption of IoT devices integrating the edge and cloud computing servers	Blockchain only used to store the IoT data	Only few parameters are simulated, and blockchain execution in the real networks is one of possible solutions to increase the throughput of the system	Average response time and energy consumption of the solution are lower than those in the existing schemes
9.	[81]	2021	(a) IoT, (b) blockchain	Private blockchain-enabled cipher-policy attribute-based encryption scheme for IIoT	Deep analysis of smart contract mechanism required	State machine model-based smart contracts can be designed	Smart contract languages such as Solidity can be used for writing the contracts among the IIoT entities
10.	[82]	2021	(a) IoT, (b) blockchain, (c) cloud server, (d) software-defined network	A software-defined networking and blockchain-enabled framework for the evidence collection and provenance preservation	Smart contract mechanism can be used to automate the whole system	State machine model-based smart contracts can be designed	Simulation result reveals that the performance of the system is better while increasing the number of users and load on the system

the security of IoT devices has been proposed by the authors in [74]. They have transcoded their model to smart contracts, and it works on the Ethereum private blockchain. A proof of concept has been built using Raspberry Pi devices as edge computing nodes that provide and access IoT services, and desktops and laptops serve as miners. Compared to centralized CAC, their work claims to have the following advantages: decentralized authorization which is important for heterogeneous, scalable, and dynamic IoT applications, mitigating performance bottleneck and SPOF by moving the intelligence and power from the centralized to the edge network with the fine-grained access control, and lightweight design using JSON-based capability token structure.

The ongoing automation of industries and manufacturing processes termed Industry 4.0 uses machine learning (ML) on massive data collected from IIoT devices. Sensitive data are used for training the ML models, but they are prone to privacy leaks through adversarial attacks, man-in-the-middle attacks, and so forth.

Arachchige et al. [78] have introduced a framework called PriModChain which combines differential privacy, smart contracts (Ethereum blockchain), and federated ML to enforce privacy and trustworthiness on IIoT data. They have used InterPlanetary File System (IPFS) for managing the data in an off-chain manner because it provides immutability and achieving the fast decentralization with secure peer-to-peer content delivery. Ethereum blockchain-enabled smart contracts provide transparency, traceability, and immutability. Federated ML has been used in which different models are trained on local datasets at different locations, and then their parameters are collected to create a global model. In this way, local datasets are not exposed. Python and socket programming are used for simulations.

Machine-to-machine (M2M) communication (communication between devices with limited or no human intervention) encounters mainly three problems: transparency (it is difficult to audit and make sure that private user information is not sent to the cloud), longevity (IoT devices are expected to work for decades, but they need the central entity that manages their state and communication protocols, so if the central entity stops supporting an IoT device it becomes vulnerable and may not work at all), and trust (IIoT transactions require the consumers to trust vendors and third parties). Hanada et al. studied the use of smart contracts for addressing these problems by designing and evaluating the automated gasoline purchasing (AgasP) application. Their work shows that transparency is achieved, since the transaction is done via a smart contract. In addition, longevity is ensured as the infrastructure is completely distributed and depends on the infrastructure of Ethereum instead of a centralized entity. The need for a trusted third party for payment is also eliminated as the payment is distributed via smart contract. All this helped to reduce the fees paid by the gas station for a typical transaction.

Because IoT data are inherently dynamic in nature, it is challenging to ensure data integrity for cloud-based IoT applications. Traditionally, the third party is used for data integrity verification, which is not reliable. Liu et al. [73] proposed a blockchain-based data integrity service framework for IoT data. Their framework has four parts: data owner's application and consumer's application, blockchain, and cloud storage service. The cloud is used to store the general purpose data (data owners) and a peer-to-peer file system for sharing the data between consumers and owners. They have only implemented the fundamental functions of their proposed protocols, and their test environment is of small scale.

The authors in [81] presented an access control scheme for the end-users based on the blockchain mechanism in the IIoT environment which further provides the data security and scalability to the system. In this protocol, the cipher-policy attribute-based encryption scheme is used to encrypt the data gathered by the IoT smart devices, and then the encrypted data are forwarded to the gateway nodes. The gateway nodes create the partial blocks from the encrypted data and hand them over to the cloud servers. After this, the cloud server forms the full block based on the practical Byzantine fault tolerance voting mechanism and maintains the peer-to-peer blockchain network. The cipher-policy attribute mechanism allows the end-user to access the blocks from the blockchain. The simulation result captures the computation costs for the varied numbers of transactions in a block. Son et al. [79] designed a secure authentication protocol based on the blockchain for the telecare medical information system which consists of an IoT-enabled wireless body area network. The cipher text-policy attribute-based encryption scheme is used as an access control mechanism to retrieve the data stored in the cloud server. Therefore, only the authentic users can access the stored data. In addition to that, the scheme integrates the consortium blockchain (based on the proof-of-authority consensus mechanism) maintained by the health centers and local hospitals, which ensures the integrity of data and increases the trust in the telecare medical information system. The simulation analysis of the protocol shows that it achieves the desired security for the system and resilience against various security attacks, such as session key disclosure attacks and privileged-insider attacks.

The authors in [82] created a cloud-based software-defined networking (SDN) framework which mainly consists of IoT mobile nodes, blockchain as a controller, cloud server, investigator, and authentication server. The mobile nodes encrypt the data packet based on the elliptic curve integrated encryption scheme and SHA-256 hashing algorithm and transfer to the cloud servers. In this scheme, the SDN controller maintains the blockchain (based on the proof-of-work consensus) to provide the evidence provenance further. The user registration and authentication, data encryption and storage, evidence collection from blockchain, and mining of evidence information are the main modules of their proposed system. Wu et al. [80] proposed a blockchain-enabled task offloading mechanism by leveraging the concept of edge and cloud computing paradigm. The proposed mechanism addresses the limited computational capacity of IoT devices and high latency problems when the gathered data are sent to edge or cloud servers through the public channel (an online mechanism). The mobile edge computing paradigm solves the latency problems, whereas mobile cloud computing servers solve the computational problems of the traditional IoT-based system. Furthermore, to minimize the response time and energy consumption of devices, this mechanism uses the energy-efficient task offloading algorithm, where the edge or cloud servers execute this algorithm depending on the application scenario, and the Lyapunov optimization technique is applied to reduce the computational and communication cost incurred by the different applications.

3.4. Healthcare Sector. The healthcare sector is one of the promising areas of IIoT application. Recently, we have experienced a health crisis due to the newly discovered COVID-19 disease. The disease not only affects human life but also affects the economy of the country and world [83]. Although the recent advancement in the field of IoT and artificial intelligence (AI) brings about opportunities to win the battle against this disease, currently, the internet-of-medical-things (IoMT) devices provide medical facilities to different healthcare organizations because of the availability of various wearable devices, biosensors, and wireless communication technologies. However, the IoMT system also faces privacy and security vulnerabilities, and the blockchain brings the hope that it can solve these problems. Dai et al. [84] studied the integration of IoT technology in the medical sector and tried to provide a solution for the various challenges that arise due to the COVID-19 pandemic. The proposed solution captures the five different perspectives of this pandemic: the origin of the pandemic, social distancing and quarantine people, hospital equipped with the Internet of medical devices, patient data, and remote telemedicine system. The authors also discussed how the proposed methodology fights against this. However, the proposed solution is only in early stage, and its actual implementation still needs to be investigated. The authors in [85] proposed a solution for sharing the medical data based on the attribute-based cryptosystem and blockchain technology. The medical data are stored in the cloud servers in this solution, whereas blockchain stores the storage address and medical-related information to provide easy access. The attributed-based encryption and signature scheme provides the end-user's data privacy, access control, and authenticity. To reduce the computation overhead, the cloud service does the decryption on the partial medical data. As a result, the overhead on the user side decreases but simultaneously increases on the server side and dependency on the third party.

The paper in [89] proposed a protocol named MEdge-Chain, which leverages the concept of edge computing and blockchain for medical data exchange. The automated patient monitoring scheme is deployed on the edge servers, which provides the remote monitoring of patients and efficient retrieval of medical data. However, the computational and communication overhead increased while sharing the medical data with the other health entities. To solve this issue, the authors suggested a blockchain-enabled optimization model. The priority assignment model for the various categories of medical data (i.e., emergency data, patient confidential message, biosignals features) is designed based on the queuing model to effectively manage the entire health framework. The healthcare data are complex and heterogeneous in nature. The authors in [86] presented the blockchain and cloud-based solution to manage the Medicare data. The domain experts, including the lab technician and doctors, patients, and health insurance providers, are the three main components of this system. All these components access and provide their data to the cloud servers, finally maintaining the blockchain. The various cryptographic primitives are used in the solution to validate the user. If an end-user or patient wants to access or provide data to the blockchain, the request is sent to the blockchain, maintained by the cloud servers. It verifies the user, and, after the verification, a new block is proposed based on the transaction of the end-user. Once validation of the block is successful, it is added to the blockchain and notifies the end-user accordingly.

To provide security, confidentiality, and integrity in the electronic health record (EHR) system, Shahnaz et al. [87] proposed a solution based on the blockchain. The role-based access policy scheme leverages that only the trusted entities of the system can access the medical records. Here, the authors utilize the off-chain storage mechanism IPFS for storing the records. The advantage of using IPFS is that the duplicated files are not allowed, and the users keep only the hash of the file if they want to retrieve the file. Furthermore, the smart contract for the patient record is used, which is written in the Solidity programming language. The proposed solution provides the content-addressable storage system, medical record confidentiality, and enhancing the system's scalability. The experimental result shows that the throughput of the system increases as the users and load (request) increase in the system. Therefore, the system can maintain a linear relationship. Garg et al. [88] proposed a blockchain-based authentication and key-agreement protocol BAKMP-IoMT to provide secure communication between the cloud and personal servers and between the personal servers and medical devices in the IoMT environment. Once secure communication is established, the user can access the required information from the cloud server that maintains the blockchain network, which is further based on the voting-based consensus mechanism. To reduce the computation cost, the solution only uses the cryptographic hash and X-OR functions. The AVISPA tool is used for the simulation of protocol, and its formal analysis verifies that the solution is robust against the ephemeral secret leakage attack, privileged-insider attack, and so forth. Table 7 shows the brief overview of existing IoT-enabled healthcare sectors.

4. Future Research Challenges

The integration of IoT and blockchain brings about a variety of opportunities for the upcoming Industry 4.0 [90]. But, still, there are a number of challenges that exist, which need to be resolved before releasing the full blockchain-enabled IoT or IIoT system. Here, we mentioned some of the important open research challenges.

4.1. Resource Constraint Devices. The devices that are used in the IoT and IIoT systems are mostly resource-constraint. These devices have limited capabilities such as limited processing power and storage space. As a result, they are not directly suitable to deploy over the blockchain network as huge computational power and storage space are required. In addition, consensus algorithm such as proof of work requires the huge amount of energy and electricity for the mining process [4]; therefore, the algorithm that is based on this category (longest chain rule) is not suitable for the resource-constrained system.

4.2. Suitable Incentive Mechanism for Blockchain-Enabled IoT System. The incentive mechanism is the core functionality of blockchain technology. The incentive mechanism based on the proof-of-work mechanism is not adoptable by the IoT system because it requires much computational power to solve the puzzles. Also, the block reward is halved after the mining of 210, 000 blocks [91]. Therefore, considering the incentive mechanism which is suitable to the IoT or IIoT system is an open research question for the researchers.

4.3. Big Data Analytics Scheme. The IoT system is generally used for data-related applications, where the devices generate a huge amount of multimedia data [92]. The generated data are stored in the cloud server in which the machine learning algorithm does the data preprocessing, data extraction, and data analytics. The average time taken by the algorithm varies from days to months. Moreover, privacy leakages, access control mechanisms, and so forth are the major issues associated with this scheme.

4.4. Scalability of Blockchain-Enabled IoT System. The scalability of the current blockchain mechanism also limits the applicability of IoT and IIoT systems. The bitcoin system has low transaction throughput (5 to 7 transactions per second where average block time is 10 minutes), whereas the average

Table 7: Comparison table based on different parameters of the existing IoT-enabled healthcare sectors.

S. no.	Reference	Year	Technology used	Summary of the work	Shortcoming of the work	Possible solution	Implementation remarks
1.	[86]	2018	(a) Cloud, (b) blockchain	A decentralized framework to manage the healthcare data based on the cloud-enabled blockchain system	Only the prototype model is discussed.	Private blockchain-enabled cryptographic protocol is one of the possible solutions	Only the theoretical study of the proposed solution
2.	[87]	2019	(a) IPFS, (b) blockchain, (c) Solidity	Off-chain storage mechanism and role-based access policy scheme for the electronic health records based on the blockchain	Deep analysis of cryptographic primitives behind the role-based access policy scheme is required	Cipher-text attributed-based encryption scheme can be used	Solution increases the scalability of the system
3.	[84]	2020	(a) IoMT, (b) blockchain	A decentralized blockchain-enabled prototype model to combat $COVID-19$ by using the Internet-of-medical-things devices (IoMT)	Simulation of the proposed solution is not addressed	Cryptography primitives and smart contracts can be used to achieve more security in the IoMT application	Smart contract languages such as Solidity or Golang with security validation tools can be used
4.	[85]	2020	(a) IoMT, (b) blockchain, (c) attributed-based encryption and signature scheme	A framework for the medical data-sharing based on the blockchain and cloud servers	The protocol mostly depends on the third party for its operations	A distributed storage system such as swarm and IPFS can be used to achieve the full decentralization	The protocol is not analyzed formally. The security validation tools, i.e., AVISPA and Scyther do this
5.	[88]	2020	(a) IoMT, (b) blockchain, (c) cloud server	Blockchain-enabled authentication and key-agreement protocol for IoMT	Cloud server storage cost may be increased	Off-line storage scheme can be used for reducing the storage cost	Protocol simulation confirms that the computation cost is 23.18msec, and communication cost is 1376bits
6.	[89]	2021	(a) IoMT, (b) blockchain, (c) edge computing	Blockchain-enabled optimization and priority assignment model for medical data exchange	Did not investigate the analysis of medical data used in real scenario	Possible machine learning and deep learning algorithm can be used for proper analysis of medical data	EMOTIV EPOC+ used for simulating the EEG data

block time for Ethereum is 15 seconds [93]. On the other side of the coin, IoT devices-based applications (such as smart healthcare) generate data very quickly. Therefore, the current platforms are not directly suitable for the IoT or IIoT system.

4.5. Dynamic Security Framework. In the IoT system, heterogeneous devices are connected ranging from low-power devices to high-power servers. Therefore, a uniform solution may not work for all blockchain-enabled IoT systems. Furthermore, the security solution should consider the nature of the resource-constrained IoT devices, and it also meets the minimum security solutions of the end customers (or users) [22]. Hence, the design of an adaptable and dynamic security framework for the blockchain-enabled IoT (or IIoT) system is a good research area.

4.6. Security Vulnerability and Privacy Leakage. The adoption of blockchain technology in the field of IoT surely improves the security of IoT systems through encryption and hashing, which is the inherent mechanism of blockchain. But the devices are connected via the wireless communication system (mostly), and, due to the open wireless medium, they are suffering from the security breaches such as replying attack, eavesdropping, and jamming. In addition to this, the transactions in the blockchain system are done via the account address (or IP address). Therefore, a certain level of anonymity is also achieved. But this scheme does not provide enough protection because it is cracked via the machine learning algorithm [94].

4.7. Advance Smart Contract System. The traditional IoT system uses the centralized architecture, where the IoT devices send data to the cloud server for processing. In return, the cloud server does the task and sends it back to the IoT device. The limited scalability is the issue associated with the centralized system. This platform is not suitable for those scenarios (e.g., a smart hospitalization system with automated payment), where the devices want to initiate the payments with their interest to others. Application logic contracts perform better for these requirements which allow the device to function autonomously and securely and further achieve greater automation and cheaper transactions.

4.8. Federated Learning for IoT. Due to distributed and private datasets, the classical learning algorithm cannot be used for the IIoT. Federated learning provides a solution where devices perform the local training and send the result to the cloud for the global model aggregation. The key to using federated learning is that migrating a massive amount of data from the IoT device to a cloud or edge server is not required. However, using federated learning for IoT-based systems itself has various challenges; for example, a secure encryption method is needed to send the learning model parameters to other devices or servers. Moreover, to achieve better learning, a set of IoT devices must connect with the aggregation server under the communication constraint. This is the new research direction, and deep analysis is required to integrate the blockchain-enabled federated learning for resource-constrained IoT devices [95].

5. Our Observations

The upcoming Industry 4.0 connects the latest technologies such as blockchain, machine learning, cloud computing, and IoT for enhancing the productivity and efficiency of their systems [96]. Among those, the incorporation of IoT and blockchain is the latest topic for researchers. In this section, we discuss our observation for the state-of-the-art research, and that can increase the security and trust in the IoT (or IIoT) system. Along with the incorporation of blockchain and IoT, researchers also use artificial intelligence and machine learning algorithm for enhancing the efficiency of the system. The machine learning algorithm processes and classifies the huge amount of data generated by the devices. Although only a few of the research papers discuss the machine learning algorithm in the IoT system, it is also a new research direction that could increase the efficiency of the IoT- (or IIoT-) based system. The state-of-the-art research used simulators such as Solidity and Remix IDE for simulating the smart contracts, and a few of them also used IPFS for storing the data in a distributed manner. The hyperledger fabric [97] is also a simulator where the researcher could incorporate the blockchain and IoT. In addition to this, researchers are focusing on an incentive mechanism that is adaptable in nature for the resource-constrained IoT devices, because the existing mechanisms (e.g., those based on the PoW) are not inherently suited for these devices.

6. Concluding Remarks

The current internet-of-things- (IoT-) enabled industrial sectors are facing many challenges (e.g., security and privacy vulnerability, etc.), and blockchain technology brings hope that it can resolve the aforementioned issues without the trusted third party (TTP). In this paper, we have investigated the need for blockchain in IoT and industrial IoT (IIoT) and provided state-of-the-art research. The state-of-the-art research is broadly classified into four major categories: data storage and management technique, industrial sectors, big data, cloud computing, and network security technique, and healthcare sector. In addition to this, the paper presents a number of future research challenges with observations that can be useful for the research community to proceed in the right direction.

Data Availability

The data are available upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by Dr. SPM International Institute of Information Technology, Naya Raipur.

References

[1] L. Tan and N. Wang, "Future internet: the internet of things," in *Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, vol. 5, pp. V5–V376, Chengdu, China, September 2010.

[2] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[5] S. Grover and N. Feamster, "The internet of unpatched things," *Proc. FTC PrivacyCon*, 2016.

[6] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, Article ID 102481, 2020.

[7] K. Mahmood, S. Shamshad, M. Rana et al., "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," *Journal of Information Security and Applications*, vol. 61, Article ID 102900, 2021.

[8] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18295–18325, 2018.

[9] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, 2021.

[10] L. D. Xu, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[11] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proceedings of the 2017 19th International Conference on Advanced Communication Technology*

(ICACT), pp. 464–467, IEEE, PyeongChang, Korea, March 2017.

[12] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, Article ID 106382, 2020.

[13] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, 2020.

[14] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Dublin, Ireland, June 2020.

[15] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[16] J. Srinivas and A. K. Das, "9 lightweight security protocols for blockchain technology," *Cyber Defense Mechanisms: Security, Privacy, and Challenges*, vol. 131, 2020.

[17] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[18] J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, *Blockchain and Applications*, Springer, Berlin, Germany, 2020.

[19] S. Aggarwal and N. Kumar, "Blockchain 2.0: smart contracts," *Advances in Computers*, vol. 121, pp. 301–322, 2020.

[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[21] N. Kumar and A. Miglani, *Probabilistic Data Structures for Blockchain-Based Internet of Things Applications*, CRC Press, Boca Raton, Florida, 2021.

[22] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[23] Z. Zheng, S. Xie, H.-N. Dai et al., "An overview on smart contracts: challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.

[24] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 254–269, Vienna, Austria, October 2016.

[25] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019.

[26] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale," in *Proceedings of the 2018 Annual Computer Security Applications Conference*, pp. 653–663, San Juan, Puerto Rico, December 2018.

[27] Y. Murray and D. A. Anisi, "Survey of formal verification methods for smart contracts on blockchain," in *Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–6, IEEE, Canary Islands, Spain, June 2019.

[28] J. Chiu and T. V. Koeppl, "Blockchain-based settlement for asset trading," *Review of Financial Studies*, vol. 32, no. 5, pp. 1716–1753, 2019.

[29] Q. Zhang, J. Zhu, and Y. Wang, "Trustworthy dynamic target detection and automatic monitor scheme for mortgage loan with blockchain-based smart contract," in *Communications in Computer and Information Science*, pp. 415–427, Springer, Berlin, Germany, 2020.

[30] K. M. Alam, J. A. Rahman, A. Tasnim, and A. Akther, "A blockchain-based land title management system for Bangladesh," *Journal of King Saud University-Computer and Information Sciences*, 2020.

[31] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: an analysis through the review of academic and trade literature," *Telematics and Informatics*, vol. 58, no. 5, Article ID 101532, 2020.

[32] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[33] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, Article ID 101654, 2020.

[34] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent advances in smart contracts: a technical overview and state of the art," *IEEE Access*, vol. 8, pp. 117782–117801, 2020.

[35] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Studies in Health Technology and Informatics*, vol. 254, pp. 105–115, 2018.

[36] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[37] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proceedings of the International Conference on Data Processing and Applications*, pp. 62–68, Guangdong, China, May 2018.

[38] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–9, IEEE, Hangzhou, China, July 2018.

[39] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, 2018.

[40] J. Chen, X. Ma, M. Du, and Z. Wang, "A blockchain application for medical information sharing," in *Proceedings of the 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE)*, pp. 1–7, IEEE, Beijing, China, April 2018.

[41] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for business applications: a systematic literature review," in *Business Information Systems*, pp. 384–399, Springer, Berlin,Germany, 2018.

[42] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[43] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[44] Z. Li, H. Guo, W. M. Wang et al., "A blockchain and automl approach for open and automated customer service," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3642–3651, 2019.

[45] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, IEEE, Kunming, China, June 2016.

[46] M. Nakasumi, "Information sharing for supply chain management based on block chain technology," in *Proceedings of the 2017 IEEE 19th Conference on Business Informatics*, pp. 140–149, IEEE, Thessaloniki, Greece, July 2017.

[47] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *Journal of Information Security and Applications*, vol. 54, Article ID 102554, 2020.

[48] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

[49] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[50] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3661–3669, 2019.

[51] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2017.

[52] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Blockchain technology based medical healthcare system with privacy issues," *Security and Privacy*, vol. 2, no. 5, p. e83, 2019.

[53] S. K. Dwivedi, R. Amin, S. Vollala, and R. Chaudhry, "Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities," *Computers & Electrical Engineering*, vol. 86, Article ID 106719, 2020.

[54] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, "A cost analysis of internet of things sensor data storage on blockchain via smart contracts," *Electronics*, vol. 9, no. 2, p. 244, 2020.

[55] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure IoT data sharing," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 99–103, IEEE, Seoul, Korea, May 2019.

[56] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, 2018.

[57] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 09, no. 10, pp. 533–546, 2016.

[58] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric internet of things via blockchain smart contracts," in *Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 991–998, IEEE, Guangzhou, China, October 2018.

[59] X. Zheng, J. Lu, S. Sun, and D. Kiritsis, *Decentralized Industrial IoT Data Management based on Blockchain and IPFS, IFIP Advances in Information and Communication Technology*, pp. 222–229, Springer, Berlin,Germany, 2020.

[60] H. Zareen, S. Awan, M. B. E. Sajid, S. M. Baig, M. Faisal, and N. Javaid, "Blockchain and IPFS based service model for the internet of things," in *Proceedings of the 7th International Conference on the Internet of ThingsAt*, Linz, Austria, October 2017.

[61] D. Na and S. Park, "Fusion chain: a decentralized lightweight blockchain for IoT security and privacy," *Electronics*, vol. 10, no. 4, p. 391, 2021.

[62] A. Tiwari and U. Batra, "IPFS enabled blockchain for smart cities," *International Journal of Information Technology*, vol. 13, no. 1, pp. 201–211, 2021.

[63] Q. Wen, Y. Gao, Z. Chen, and D. Wu, "A blockchain-based data sharing scheme in the supply chain by IIoT," in *Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pp. 695–700, IEEE, Taipei, Taiwan, May 2019.

[64] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.

[65] F. Curbera, D. Dias, V. Simonyan, W. Yoon, and A. Casella, "Blockchain: an enabler for healthcare and life sciences transformation," *IBM Journal of Research and Development*, vol. 63, no. 2/3, pp. 8–1, 2019.

[66] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of IoT data using smart contracts," *IET Networks*, vol. 8, no. 1, pp. 32–37, 2018.

[67] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," 2018.

[68] J. Grecuccio, E. Giusto, F. Fiori, and M. Rebaudengo, "Combining blockchain and IoT: food-chain traceability and beyond," *Energies*, vol. 13, no. 15, p. 3820, 2020.

[69] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart secure sensing for IoT-based agriculture: blockchain perspective," *IEEE Sensors Journal*, vol. 21, no. 16, 2020.

[70] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in internet of drones environment," *Computer Communications*, vol. 166, pp. 91–109, 2021.

[71] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2021.

[72] V. Puri, I. Priyadarshini, R. Kumar, and L. C. Kim, "Blockchain meets IIoT: an architecture for privacy preservation and security in IIoT," in *Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp. 1–7, IEEE, Gunupur, India, March 2020.

[73] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proceedings of the 2017 IEEE International Conference on Web Services (ICWS)*, pp. 468–475, IEEE, Honolulu, HI, USA, June2017.

[74] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: a blockchain-enabled decentralized capability-based access control for iots," in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1027–1034, IEEE, Halifax, NS, Canada, July 2018.

[75] Y. Hanada, L. Hsiao, and P. Levis, "Smart contracts for machine-to-machine communication: possibilities and limitations," in *Proceedings of the 2018 IEEE International*

Conference on Internet of Things and Intelligence System (IOTAIS), pp. 130–136, IEEE, Bali, Indonesia, November 2018.

[76] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.

[77] L. Bai, M. Hu, M. Liu, and J. Wang, "BPIIoT: a light-weighted blockchain-based platform for industrial IoT," *IEEE Access*, vol. 7, pp. 58381–58393, 2019.

[78] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial iot systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[79] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, pp. 192177–192191, 2020.

[80] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, and M. Xu, "EEDTO: an energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2163–2176, 2020.

[81] S. Banerjee, B. Bera, A. K. Das, S. Chattopadhyay, M. K. Khan, and J. J. P. C. Rodrigues, "Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT," *Computer Communications*, vol. 169, pp. 99–113, 2021.

[82] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.

[83] D. Marbouh, T. Abbasi, F Maasmi et al., "Blockchain for COVID-19: review, opportunities, and a trusted tracking system," *Arabian Journal for Science and Engineering*, pp. 1–17, 2020.

[84] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat COVID-19," *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 52–57, 2020.

[85] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[86] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of Medical Systems*, vol. 42, no. 8, pp. 156–211, 2018.

[87] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[88] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[89] A. A. Abdellatif, L. Samara, A. Mohamed et al., "MEdge-chain: leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet of Things Journal*, 2021.

[90] 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, 2020.

[91] K. Saito and M. Iwamura, "How to make a digital currency on a blockchain stable," *Future Generation Computer Systems*, vol. 100, pp. 58–69, 2019.

[92] S. Vyas, M. Gupta, and R. Yadav, "Converging blockchain and machine learning for healthcare," in *Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 709–711, IEEE, Dubai, United Arab Emirates, February 2019.

[93] K. Croman, C. Decker, I. Eyal et al., "On scaling decentralized blockchains," in *Financial Cryptography and Data Security*, pp. 106–125, Springer, Berlin, Germany, 2016.

[94] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[95] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 2021, Article ID 3090430, 2021.

[96] U. Bodkhe, S. Tanwar, K. Parekh et al., "Blockchain for industry 4.0: a comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[97] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, pp. 1–15, Porto, Portugal, April 2018.