IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 November 2022, accepted 15 November 2022, date of publication 18 November 2022,
date of current version 28 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223370

SURVEY

Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review

ABDULLAH AYUB KHAN[1,2], ASIF ALI LAGHARI[1], ZAFFAR AHMED SHAIKH[2], ZDZISLAWA DACKO-PIKIEWICZ[3], AND SEBASTIAN KOT[4,5]

[1]Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Pakistan
[2]Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Pakistan
[3]Department of Management, Faculty of Applied Sciences, WSB University, 41-300 Dąbrowa Góornicza, Poland
[4]Faculty of the Management, Czestochowa University of Technology, 42-201 Częstochowa, Poland
[5]Faculty of Economics and Management Sciences, North-West University, Vanderbijlpark 1900, South Africa

Corresponding author: Abdullah Ayub Khan (abdullah.khan00763@gmail.com)

The research was funded under the program of the Minister of Education and Science titled "Regional Initiative of Excellence" in 2019-2023, project number 018/RID/2018/19, the amount of funding PLN 10 788 423,16."

ABSTRACT With the rapid enhancement in the design and development of the Internet of Things creates a new research interest in the adaptation in industrial domains. It is due to the impact of distributed emerging technology and topology of industrial Internet of Things and the security-related resource constraints of industrial 5.0. This conducts new paradigm along with critical challenges to the existing information preservation, node transactions and communication, transmission, trust and privacy, and security protection related problems. These critical aspects pose serious limitations and issues for the industry to provide industrial data integrity, information exchange reliability, provenance, and trustworthiness for the overall activities and service delivery prospects. In addition, the intersection of blockchain and industrial IoT has gained more consideration and research interest. However, there is an emerging limitation between the inadequate performance of industrial IoT and connected nodes, and the high resource requirement of permissioned private blockchain ledger has not yet been tackled with the complete solution. Due to the introductions of NuCypher Re-Encryption infrastructure, hashing tree and allocation, and deployment of blockchain proof-of-work required more computational power as well. This paper is divided into three different folds; first, we studied various related literature of blockchain-enabling industrial Internet of Things and its critical implementation challenging aspects along with the solution. Secondly, we proposed a blockchain hyperledger sawtooth-enabled framework. This framework provides a secure and trusted execution environment, in which service delivery mechanisms and protocols are designed with an acknowledgment, including the immutable ledger storage security, along with the peer-to-peer network on-chain and off-chain communication of industrial activities. Thirdly, we design pseudo-chain codes and consensus protocols to provide smooth industrial node streamline transactions and broadcast content. The proposed multiple proof-of-work investigated and simulated using Hyperledger Sawtooth-enabled docker for testing to exchange information between connected devices of industrial Internet of Things within the limited usage of resource constraints.

INDEX TERMS Blockchain, hyperledger technology, chain codes (smart contracts), Internet of Things (IoT), nucypher re-encryption, Industrial Internet of Things (IIoT).

I. INTRODUCTION

The changeover in information technology because of the evaluation and development of the Internet of Things (IoT). This digital connection establishes a node-to-node smart communication with different service automation that reduces the human affords [1]. It is also because of the exponential growth of artificial intelligence (AI), distributed connectivity, and intelligent communication protocols, which enabled dynamic data optimization and management in industrial processes [2]. In the beginning, digitalization has been focused on the efficiency of operational industrial data

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

optimization and automation to maintain IoT-enabled industrial manufacturing. This is the current electronic information transactions-related ledger development procedure utilized in the production systems. The advent of the Fourth Industrial Revolution (industry 4.0) has incorporated several positive features, such as the involvement of IoT in industrial manufacturing and product development [3], [4]. However, to robust the development of industrial things, the Industrial Internet of Things (IIoT) has emerged with a new paradigm that strengthens production in a smooth and smart manner. In the recent environment, this technology involves in every domain of transportation, intelligent manufacturing of automobiles, resource management, renewable energy management, and smart cities development [5]. The number of advancements in the industrial manufacturing units has captured the expert's attention in the past few years. In this regard, various related applications have been proposed that enhance the performance of production units. It includes the flow of operations and control management, digital enterprise/factory, alert of industrial things configuration, safety, and maintenance measures, and health monitoring of employee/workers, etc. [6], [7], as shown in Figure 1.

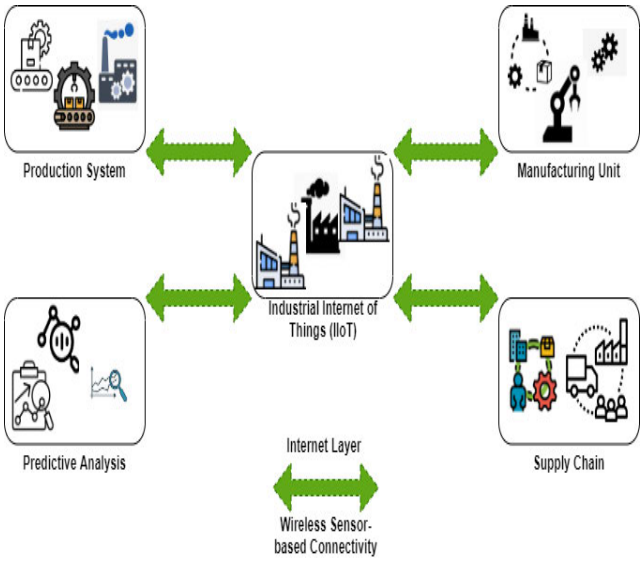


FIGURE 1. The current scenario of industrial IoT (IIoT).

The complete process of IIoT is designed and created with the primary components of IoT-enabled sensors devices. The wireless sensors network is used to handle and manage all the operational controls and coordinate different activities, dynamic monitoring, real-time checking, remote system diagnostic, and dynamic control of production systems [8], [9]. Till now, there is an insecure environment derived from the number of nodes' connectivity. In fact, the current communication protocols utilized for the exchange of information are weak in terms of privacy and security [10]. One of the main reasons for these emerging vulnerabilities and their involvement in the industrial domain because of the number of devices published by various unregistered companies without testing in accordance with the standard verification and validation [11]. However, intelligent manufacturing consists of different internet of production systems (IoPS), a complex combination of components is closed in terms of hardware, software, and connected devices to communicate smartly, as shown in Figure 1. Each associative layer of IoPS is insecure/vulnerable to network attacks. In the current scenario, there is various malicious attacks are registered, such as reverse engineering attacks, distributed denial-of-services, etc. The code of software components can also be vulnerable because it associates with a virus, trojans, and dynamic programming attacks [12]. On the other side, the communication channels can be compromised to third-party, man-in-middle, client-server-based network protocols, which are weak in nature as compared to the distributed network [13]. So, to design manual IoPS, it is harder to maintain complex transaction procedures and is affected by social attacks, for example, spamming, phishing, etc.

The current security and privacy solutions are insufficient because the different heterogeneous IoT devices and networks channels are connected increasingly due to the popularity of the Industrial Internet of Things [14], [15]. To create a strongly protected environment and private ecosystem that automatically performs operations and avoids intermediate intrusions. In this regard, a secure ecosystem has required that handle and manage industrial production unit to be available, which means the system should be prevented from unnecessary delay and protected from malicious attacks against the IoPS [16]. In addition, the integrity and transparency of the IIoT-enabled transactions is another critical aspect of the existing smart production systems. To avoid physical damage, the experts of IIoT designed high protection infrastructure in their proposed work by raising the cryptographic encryption mechanism against malicious attacks. It causes low quality and provides a strongly encrypted ledger structure, which ultimately means that this procedure consumes more resource constraints of industrial things in terms of computational power, network bandwidth, and preservation. In this regard, to reduce the load of traffic in an industrial environment, avoidance of unauthorized access and restricting unintentional use of IoT-devices is the primary objective [17], [18]. To handle and maintain the authenticity of vendors' access is another challenging prospect and only allows operations to be performed along with the requirement of security in the IIoT. Further, integrity and confidentiality for employees and connected participated stakeholders' personal information by protecting industrial smart code, dynamic data monitoring, and intelligent configuration of industrial production units.

Recently, blockchain distributed ledger technology is adopting by different enterprises to protect the entire processes of current systems. And so it also helps to maintain secure supply-chain transactions, along with ledger privacy, transparency, provenance, traceability, and easy access through the distributed application (DAPP) [19]. In industrial IoT, blockchain technology provide a secure, encrypted, and

permissioned modular infrastructure that handles events of nodes transaction execution and preserves individual logs on immutable storage to enable a transparent process of IIoT [20], [21]. However, the IIoT-enabled events are stored in chronological order in the chain-like structure that is connected with two different channels (on-chain and off-chain) in a peer-to-peer (P2P) network. In addition, customizable chain codes are provided that allow for the management of dynamic deliverance and automate control transactions to achieve decentralized autonomous execution. This immutable ledger provides nonrepudiation information management, in which this industrial information is hard to tamper with and forged and retain details in a protected manner in a data preservation container (InterPlanetary File Storage) [22].

The blockchain enabling technologies have been envisioned, utilized, and adopted for different industrial production units to achieve integrity, transparency, traceability, and provenance to enable secure industrial data analysis and storage [23]. Whereas most of the IIoT experts are shifting towards blockchain and utilizing this technology as its decentralized nature, which provides strong protection against a number of cyber-attacks [24]. The variety of attacks is usually intended for client-server-based architecture and other relevant types of centralized systems [25], [26]. In fact, the blockchain decentralized modular architecture enables IIoT ecosystems to enhance the defense between distributed IoT nodes and their ability to deliver in a protected way using cryptographic encryption/NuCypher Re-Encryption algorithm. However, the technology is also able to deploy intrusion detection that provides prevention and restricts malicious attacks. Installation of firewalls, anti-disclosure tools, procedures, and protocols implementation ensure by the platform that guarantees the security, privacy, and information immutability along with ledger transparency and trustworthiness [27].

A. MOTIVATION

This paper addresses the current security and privacy challenges and limitations in the industrial IoT environment. It also highlights the involving implementation and deployment-related issues while connecting two or more nodes together. Interoperability is another challenging prospect that is a concern in this paper and proposed a solution in terms to design a consortium communication channel, where both the private and public transactions take place over the protected Peer-to-Peer (P2P) network, respectively. In this regard, a novel and secure blockchain-enabled framework is proposed. This proposed framework provides robust security while IoT-based transactions initiate from the source to the destination (devices-to-device) over the consortium network. Throughout the data deliverance, the protection of individual data packages is possible because of NuCypher Re-Encryption (batch-to-batch privacy). This collaborative approach of IoT-blockchain provides proper ledger integrity, transparency, provenance, traceability, trustworthiness, and assurance for performing all the IoT-related operations, including sensor-based data acquisition, streamlining business processes, automating task execution, efficient business decision, and accessibility. However, the process of IoT-enabling devices-based generated data capturing, examining, analyzing, preserving, presenting, and reporting are designed for secure interpreting the chain-of-analyzed records. This act ensures security and privacy for the whole IoT-related transactions and stores detail of each event of execution in the form of data blocks in the immutable storage (IPFS).

B. RESEARCH OBJECTIVES AND CONTRIBUTIONS

The critical objective of this study is to improve the process of IoT-enabled devices data investigation, including data capture, examination, analysis, preservation, presentation, and documentation, that is used in the industrial environment for the purpose of security measures. To perform a dynamic structure deliverance and maintain a secure infrastructure for IoT-based transactions to trace exactly what factors are involved in the distributed network or between computing nodes that affect ecosystems execution. And so, an adequate process of analysis for it to mitigate the involving risk in the events of IoT-nodes transactions execution and management throughout the lifecycle. However, the blockchain-enabling technology is attaining more acceptance and adaptation as it is being used to protect the process of IoT-based data collection. It also provides a secure channel against malicious attacks and the intruders involved in the current sensors network environment. These incidents are reported that help to interpret and create attributes of the security and privacy lacks so it can be restricted in the future. Because of blockchain distributed ledger technology, the detailed report of vulnerabilities is preserved in the immutable storage along with the depositions and related testimonies registration. The main contributions of this paper are discussed as follows:

- In this paper, we studied more than a hundred research articles based on the Internet of Things (IoT), industrial data management, distributed network connectivity, communication protocols, blockchain, and hyperledger technology. The main highlight of this study is to define privacy and security and related concerns in the current deployment of IoT in the industrial environment. For instance, the review perspective is reported in accordance with the shape of a systematic point-of-view.
- A novel and secure blockchain hyperledger-enabled framework is proposed for the industrial internet of things (IIoT) along with the process hierarchy of transaction executions.
- This paper presents different chain codes for the purpose to automate events of nodes transactions executions, such as IoT-enabled industrial devices registration, the process of data collection and examination, data preservation, management, and organization, and managing distributed network transmission (on-chain and off-chain) automatically, respectively.

- The hyperledger sawtooth-enabled pre-defined consensus is tuned in accordance with the limited range, which means reducing the consumption of blockchain distributed resources in terms of computational energy, the bandwidth of network transmission, and storage.
- At last, we evaluate, examine, and analyze various involving designed-related futuristic issues, challenges, and limitations. And so, mentioned a few solutions that make IoT-enabled industrial ecosystems more efficient and reliable and provide effective performance in a distributed network environment.

The remainder of this paper is organized as follows. In Section 2, various literature is discussed related to the different industrial IoT-based devices and their security and privacy protocols. And so, the role of blockchain-enabling technology and its associated impact on the recent developing environment is discussed. The application of blockchain-enabled IIoT ledger protection and privacy are discussed in Section 3. In Section 4, a blockchain hyperledger-enabled novel and secure framework are proposed for industrial IoT. The list of involving implementation and deployment-related issues, challenges, and limitations and their possible solutions are mentioned in Section 5. Finally, we conclude this research in Section 6.

II. AN INTEGRATION OF INTERNET OF THINGS WITH BLOCKCHAIN TECHNOLOGY

Internet of Things (IoT) technology has become one of the promising setups for industrial, production, supply chain, and manufacturing ecosystems [28]. Various experts on IoT analyze the billion-dollar impact of internet things in the industrial environment [29]. Currently, an on-demand model of industrial, production and manufacturing running that leverages internet of things, such as cloud-enabled industrial and manufacturing technology [30]. This model enables a number of ubiquitous, on-demand, convenient, client-server-based network access, a shared pool of resources, and dynamic configuration, that required minimal management and effort from services providers [31]. However, in this paper, we also provide detail of industrial IoT evaluation with the reason for adaptation of the distributed environment. Various related literature is studied, in which several benefits of industrial IoT are highlighted along with the privacy and security measures of existing associative.

A. INDUSTRIAL INTERNET OF THINGS (IIoT) AND SMART INDUSTRIES

In general, intelligent industrial and manufacturing execution is a concept of the Industrial Internet of Things (IIoT) and the processes of smart service deliverance that drive a new paradigm to facilitate the next generation of automation [32], [33]. However, the concept of industrial and intelligent manufacturing utilizes a collection of distinct methods that correspond to new tendencies in the client-server-based centralized network, where information is traveled. In fact, the technology is designed to redefine the industrial domain [34]. To make IIoT more efficient and reliable, various experts present different proposed methods that create the current ecosystems better. And so, these previous publications defined the level of improvement in the development of industrial IoT [35], such as smart communication, distributed network, dynamic nodes transactions execution, services deliverance, information preservation, security, and privacy.

However, the number of features of intelligent industrial and manufacturing executions are listed as follows [35]: (i) Digitalization, (ii) Intelligent automation, (iii) Service-orientation, (iv) Smart connection and communication, (v) Digital equipment, (vi) Collaborative network, (vii) Cost-efficient and flexibility preservation. These are the reasons that enhance the performance of industrial and manufacturing executions in industry 4.0, which directly affects the rate of productivity, and reduce human interventions with the use of artificial intelligence and cognitive automation in the industry [36]. For instance, it is hard to say that the industrial production units are fully capable to automate all the sectors' transactions executions; there is a certain gap that needs customize solutions to improve systems executions for the sake of intelligent manufacturing and productivity.

The efficient communication that resists attacks is proposed by Liu et al. [36], which described the use of federated learning in an industrial IoT environment. This collaborative technology significantly promotes the development of the fourth industrial revolution (industry 4.0) [37]. Through this, the existing federated learning with IIoT faces two different types of critical issues, one is information privacy and security, and the other is communication overhead [38]. It is considered one of the costliest communication methods while training a huge scale of multi-node modeling. However, there are a lot of vulnerabilities involved that are recorded due to the weak security of federated learning, which leads to label flipping and gradient leakage-based attacks [39], [40]. The process of training the general model is compromised directly by different adversaries.

Thereby, there are several collaborative approaches proposed by various experts of IIoT; in this scenario, Zhou et al. [41] presented a revolutionaries futuristic manufacturing and industrial setup by integrating the IoT and machine learning technologies into an industrial setting. With this development and deployment, a massive network is handled, which supports a powerful data-driven structure to optimize the load of the wireless network [42]. Recently, the quality-of-service requirements of the IIoT non-critical and critical aspects are another challenging problem that needs concern along with the cross-layer issue in the current industrial IoT [42].

B. BLOCKCHAIN ENABLING TECHNOLOGY

The distributed ledger technology enables stakeholders to verify and validate, store, and synchronize the contents of information duplication with the secure and protected form by connected participants [43]. This ledger technology has

provided various considerable benefits and incentives to enterprises, such as enabling better services and efficient deliverance [44]. In addition, it also emphasizes various models and innovations of the IoT and AI revolutions. It has a direct impact on all manufacturing and industrial things and makes an opportunity to improve industrial processes and create trust in information exchanging and records management in day-to-day units. However, a few involving challenges and limitations are highlighted in the domain of blockchain enabling the industrial internet of things as follows (as discussed in Table 1):

III. BLOCKCHAIN-ENABLED SECURITY IN INDUSTRIAL IoT ENVIRONMENT

The rapid enhancement in the current industrial IoT makes the system more efficient and reliable; apart from this, intelligent and self-adaptive devices of the internet of things are gathering attention towards itself in this recent era. The main purpose is to provide an accurate collective environment to capture a large amount of data, efficient processing, examination, and information exchanging between participating stakeholders [51], [52]. However, the process of industrial self-adaptation is unsecure; there are various gaps that affect (the operating system) and slow down the manufacturing and production executions, such as a delay due to malicious attacks, dependencies in the layered hierarchy, ledger preservation-related problems [53]. And so, most of the conventional privacy and security algorithms (for example, traditional cryptography) are not up to mark to prevent industrial actions.

In this manner, various experts of IIoT and enterprises managements are shifting towards distributed environment and adopts blockchain hyperledger technologies. It leads to build smart, intelligent, and secure industrial processes and structures for robust productivity. In industrial things, blockchain hyperledger technology provides a secure, efficient, trustworthy, reliable, and sustainable platform that manages authentication by introducing blocks of chain in a chronological order, which consumes less computational energy along with preservation [54], [55].

A. THE CURRENT ARCHITECTURE OF IIoT

Currently, there is no single technology and reserved protocols, procedure, and standards to design, create, and establish the secure Internet of Things architecture. Indeed, it is the platform that needs concerns, most importantly, on the IoT with industrial infrastructure and related applications used recently. IIoT is a collaborative system with smart, interdependent, interconnected nodes of heterogeneous nature, wireless sensors, transaction processors, actuators, network connectives, and transceivers in the existing environment. However, these integrated technologies and their working operations are categorized into four different layers [56], [57], [58]. Each has some preliminaries to establish a connection, interaction, and communication between IoT devices. The detailed design of individual layers and their role in the industrial environment are discussed as follows:

1) APPLICATION LAYER

This layer is able to handle various running applications that need to control and monitor dynamically while IoT devices are connected. It is a layer that played an intermediate role between participating stakeholders and their interconnected nodes [59]. In fact, the layer acts as a mediator to handle end-to-end nodes and their transactions executions and networks, as shown in Figure 2. And so, it creates communication channels with the authorized automated software components that are connected with the centralized database in accordance with the existing client-server-based protocols.

2) SUPPORT LAYER

A support/middleware layer is used in the central server architecture ''a three-level traditional setup'' is enough to protect as the detail is directly passed to the internet layer (responsible for data transmission among intelligent devices) [60], [61]. At the same time, it establishes breaches for the purpose to tackle various types of malicious attacks. To reduce the rate of attacks, the middleware layer supports the previous three-level architecture to handle a number of implicit flaws involved in the industrial environment and protect against malicious attacks. However, the working of the middleware layer is defined as the industrial data collected from the perception layer, which is authenticated with the private key cryptography. And so, it is transmitted to the internet layer, respectively. Recently, some attacks are needed the concern of experts in the domain of industrial security, which directly affect the production systems, such as distributed denial of service (DDoS), phishing, unauthorized access, and malicious insiders.

3) PERCEPTION LAYER

The perception layer is integrated with the physical and sensor devices [62]. The main objective of this layer is to provide IoT devices registration details (identity) and connected network records. After that, it collects data (homogeneous nature) and sends it to the client-server environment for further processing, as shown in Figure 2. However, this layer is more sensitive and most probabilistic to be attacked because of weak layered protocols. This list of related attacks is as follows [63]:

- Eavesdropping
- Tampering and forgery of ledger
- Node capturing
- Replay and time attacks, etc.

4) SECURE BUSINESS LAYER

This layer is used for managing secure enterprise-related transactions according to the defined business rules [64], [65]. The contracts/rules are designed for secure IIoT transactions execution, which is also applied to manage and handle the

TABLE 1. Literature of IIoT-blockchain and its enabling technologies.

Research Method	Research Description	Research Characteristics	Challenges in the Current Mechanism/Procedure	Similarities/ Differences with the Proposed Blockchain-IIoT
A blockchain-enabled data sharing, traceability, and recovery framework proposed for industrial internet of things [45]	The authors of this paper highlighted the role and importance of blockchain-enabling technology in the IIoT environment. It supports IIoT-enabled industrial transactions traceability and recoverability and their impact in the industrial and intelligent manufacturing for smart factories.	• An attribute-based access control scheme • For unified identity authenticatio n, blockchain-ethereum and public key cryptography used	• Intermediate level of decrypted parameter from edge/cloud • Cross platform issue • Multi-exchanging, sharing, and preservation limitation	• Decisional Bilinear Diffie-Hellman assumptions • Resist multiple attacks
A blockchain technology in industrial internet of things (IIoT) for information tampering-resistance [46]	This paper presented an integrated approach of blockchain, artificial intelligence, and industrial things that provide a standardization solution in terms of production-related executions with scalability and interoperability.	• A systematic and comprehensiv e literature review presented to integrate blockchain into IIoT applications • The number of techniques highlighted that covers industrial executions, such as operational schemes, etc.	• Scalability • Privacy and security • Distributed preservation • Network channel distribution	• A distributed tamper-resistant ledger • Data preserved at different locations with hash-encryption protection
The blockchain public permissionle ss network architecture for IIoT [47]	This paper discussed the role of blockchain ethereum technology in the overall secure network connectivity, dynamic authenticity, restriction authorized access, availability, and control access of the industrial IoT activities.	• A solution for IIoT to manage resource constraints throughout the manufacturin g executions • A secure channel for intelligent communicati on is derived.	• Cross platform issue • Model-driven limitation • Two-way authentication • Scope of privacy and preservation challenges	• Public chain • Permission network • Ethereum • Hash-encryption
An adoptive learning and blockchain enabled framework for resource sharing of	In this paper, the authors discussed the role of blockchain technology in the IIoT environment to create a trusted multi-hop of a multi-collaborative computing system for the	• A distributed network designed to create a trusted management system for	• Blockchain overhead • Hit rate and rewards of blockchain issues • Queue delay	• Blockchain ethereum • Cryptographic encryption • Consensus proof-of-work

TABLE 1. *(Continued.)* **Literature of IIoT-blockchain and its enabling technologies.**

industrial IoT [48]	efficient utilization of clustered devices.	collaborative computing • For task offloading, a social-aware multi-criteria device selection model is maintained.	• Learning regret	• Local transaction management
A blockchain ethereum-based anonymous storage and verification system proposed for industrial internet of things [49]	This proposed system ensured the industrial and manufacturing ledger preservation and protection with efficient optimization anonymously.	• The permissioned private blockchain network is designed to manage automate data processing • An index-based polynomial interpolation algorithm used to automate system	• Data acquisition • Layered hierarchy • Cross-chaining issues • Double color ball algorithm's limitations	• Permissioned network • Hyperledger technology • Direct verification and validation executions
Federated learning and blockchain-enabled integrated low computing transactions through edge for industrial IoT [50, 51]	The concept of edge computing in the IIoT environment is introduced by P. Zhang et al.; the study focused on the efficient use of federated learning in IIoT to ensure data transmission, information exchange, ledger preservation, and security. For this purpose, blockchain technology is used to provide secure and more protected authentication to perform secure communication/transactions between participating stakeholders.	• A new strategy that consumes low computing power • The process of data transmission is designed • Collaborate federated learning and transfer learning with blockchain technology is presented	• Network traffic • Security patches • Interoperability and interconnectivity • Boarder development issue	• Blockchain public network • Hash-encryption (SHA-256) • Streamline automation • Predefine consensus policies used

overall IoT system, as shown in Figure 2. In the industrial environment, these contracts are deployed to tackle traffic of business applications, models of profit and analysis, and personal information of participated stakeholders related problems.

B. ROLE OF WIRELESS SENSOR NETWORKS IN INDUSTRY, VULNERABILITY, AND SECURITY PATCHES

In an industrial environment, wireless sensor networks have gained ground almost in every unit of industrial, manufacturing, and production. Recently, the technology is expected to project an increase up to 540% in the coming next couple of years; and so, to almost 20+ million sensor points installed [66], [67]. Apart from this, it helps to develop wireless connectivity for efficient communication, power management, large miniaturization, and embedded computing systems that lead the technology for most demanding in every aspect of smart factories [67], [68]. One more reason for the growth is that the technology is accepted in a reliable manner; most of the industrial uses are shifted towards, that

is for because of the level of standards, which provide several benefits. Monitoring is one of the key prospects in this whole scenario, where wireless systems are used to take control and perform different operations, actions, and computes [68], [69]. However, the working executions of wireless sensor networks are dependent on the node's transactions; these nodes consist of microcontroller, preservation, intelligent sensors, analog to digital converters, transceiver, power management, and other controllers (for tie different pieces).

The intelligent sensors of industries are incorporated manufacturing and production-related hand-off data to other participating sensors via different channels in the distributed network [69], as shown in Figure 3. Potentially, it leads main streaming location (local LANs), where exchanging information can be seen by connected stakeholders [69], [70]. In addition, the collected data from the sensors are processed and preserved for further executions. However, the redundancy of multi-path of communication channels creates a mesh. It poses various potential challenges and limitations in terms of weak privacy and security, such as vulnerabilities, risks, control issues, and unavailability, which leads to attacks (for example, DDoS, etc.). The list of vulnerabilities and their related patches is discussed as follows:

- **Botnet:** On the Internet of Things environment, a botnet is a network that helps to connect various devices. It typically allows routers to manage pathways for package deliverance. The chances of being infected are too high; most probably, malware infections that compromised control operations of the system by falling credentials, which means malicious attackers get access to it and harm the system's authenticity [71]. The major impact of this vulnerability is that it is launching distributed denial of service on target entities to disrupt their operations and services.
- **Sybil attack:** A number of malicious attacks create several forged identities of individuals that affect the overall performance of client-server-based centralized networks [72], [73]. In industrial IoT, these nodes are capable of generating wrong/tampered reports, which directly impact the performance; further, spamming identities with false messages and causing gaps in node privacy are another part of the list.
- **Clone attack:** It is also referred to as duplication/replica attacks. This attack is used to capture physical sensor-enabled devices from the client-server-based centralized IoT network and extract their confidential credential, for example, the capturing of individual identity (either in a public or private manner), which harm the system's integrity and traceback [73], [74].
- **Distributed attack (DDoS):** In the recent industrial scenario, IoT devices are becoming an integral form of various distributed denial of service attacks [75]. However, as the number of IoT devices increases in the industry, the rate of attack will also robust exponentially. These kinds of attacks consider the only dangerous attacks in the futuristic environment of IIoT.

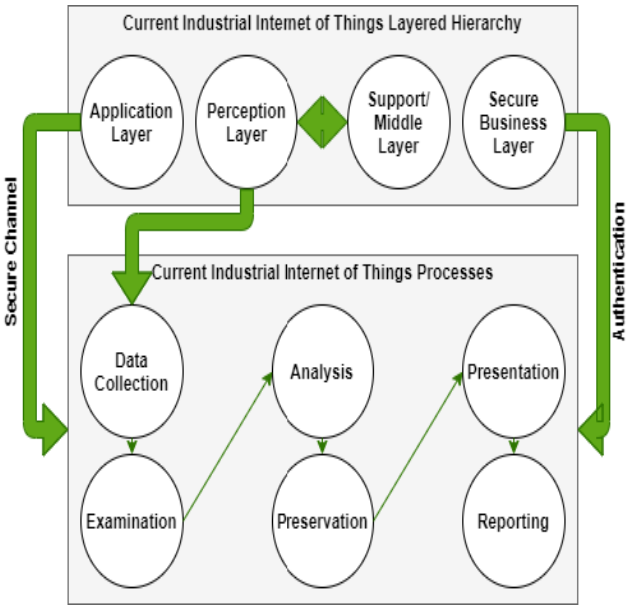


FIGURE 2. The existing block diagram of industrial internet of things (iiot) layered hierarchy.

- **Selective forwarding attack:** It is one of the parts of black-hole attacks, mainly compromised with the reason to drop node selectively, where all the packets are interconnected. It leads to the deterioration of the network, which directly impacts the performance of execution and deliverance [76].

A few wireless sensor networks involving implementation challenges in the industrial IoT, which is highlighted and explained as follows:

- **Power fluctuation and efficiency:** The main involved issue in the current wireless sensor networks is power fluctuation and related management. It is considered a resource constraint of the distributed networks [77]. The power consumption (and related fluctuation) usage during the information exchange through data packets via network routing and activities, such as path management. This is completely based on the lifespan of the wireless nodes of the sensor battery.
- **Quality-of-Service (QoS):** In the current industrial environment, the quality-of-service is one of the important prospects that provide each application (operation) analysis according to quality measures [78]. This procedure requires different quality-of-service processing. But, due to hardware limitations, individual processing of an industrial application is becoming a challenging problem in the existing scenario.
- **Hardware requirement and their complexity:** The performance of the hardware node of the wireless sensor is dependent on the functions, such as storage, processing, power source, consumption, and transmission [78]. The hardware devices are used in almost every aspect but are most probably utilized in the network to manage executions efficiently and effectively. Whereas

the operating system (OS) is independent; for example, the hardware nodes are managed by OS separately.

- **Fault tolerance:** The wireless sensor nodes are sustained; which means the functions of all the nodes are carried out in accordance with the network protocols [79]. While each node's transactions execute in the distributed network faced some limitations in terms of energy usage of the attached battery, failure rate between nodes connectivity, and network interference from external sources.
- **Data availability and Storage:** In the current IIoT technology, the availability of data is a well-focused issue analysis by experts in the domain of client-server centralized architecture [79]. And so, the preservation of individual entities in storage with security is another challenging aspect. For this purpose, a decentralized distributed architecture is proposed to manage data availability in every connected node and handle redundancy over the network before preserving records in the storage.

C. IIoT WITH BLOCKCHAIN AND 5G TECHNOLOGY

It is well proven that the internet of things (IoT) technology enhances the performance in terms of processing, control, and preservation, and maintain the efficiency of the system in a wider range of distributed environment [80]. These factors becoming the acceptance of IoT in the industrial domain, mainly leveraging the internet in manufacturing and production to enable reconfiguration of current processes and automate industrial executions, which is greatly evolved. The industrial IoT commits to bringing a large number of operations initiated, controlled and executed in an efficient manner along with improving productivity, and providing effective management of industrial things [82], [83]. However, the existing architecture of IIoT is based on the client-server-enabled centralized network structure. Each execution of node transactions is dependent on the single channel of a central server and preserves all the records (logs) in the central database environment, which leads to privacy and security issues. Further, this poses a massive problem in terms of industrial limitations, such as requiring more computations power, lack of maintenance of intelligent devices, allow third-party involvement (vendors), all of which consider a big problem from a business perspective.

Blockchain distributed technology offers solutions to the mentioned issues, challenges, and limitations raised in Industrial IoT. With an association of blockchain and fifth generation (5G) network technology, the IIoT-blockchain delivers distributed solutions to meet the industrial demand, along with a focus on specific-applicational vulnerabilities. The blockchain and IIoT with 5G-enabling technology to provide a viable switch to exploring the potential of the current industry [84]. The 5G network allows blockchain technology to design an automated registry of industrial, manufacturing, and production things, including network channels, which handle service delivery, ledger maintenance, on-chain and off-chain communication, and stakeholders' request [84], [85]. These key factors improve the events of IIoT node transactions executions in the distributed domain with protected industrial deliverance and ledger security before preservation.

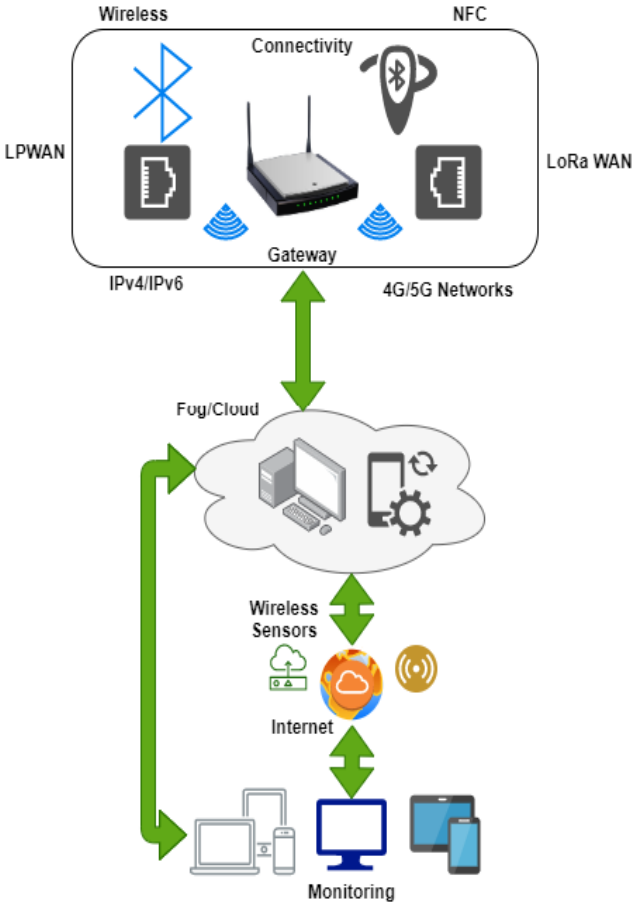


FIGURE 3. Working procedure of wireless sensor networks in industrial environment.

IV. PROPOSED FRAMEWORK

Figure 4 presents a hierarchy of the proposed framework, which is categorized into six different folds, such as IoT devices registration, industrial/manufacturing monopoly connectivity, processes of industrial transactions executions, connected stakeholders, hyperledger sawtooth-enabled secure deliverance, and IPFS-based distributed storage of ledger. First, the proposed framework declares the list of existing registered IoT devices, and also provides a platform to add newly IoT devices (along with the category, for example, ESP32, LoRa WAN, etc.) and the purpose to serve for which unit. After receiving requests, the Blockchain Hyperledger-Sawtooth Expert verifies and validate each request and grant permission to connect with distinct units of IIoT. The completion of this procedure is possible because of a defined chain code/smart contract (IIoTReg() contract), as discussed in Table 2. These connected IoT devices captured and transmit a number of transactions to the industrial units

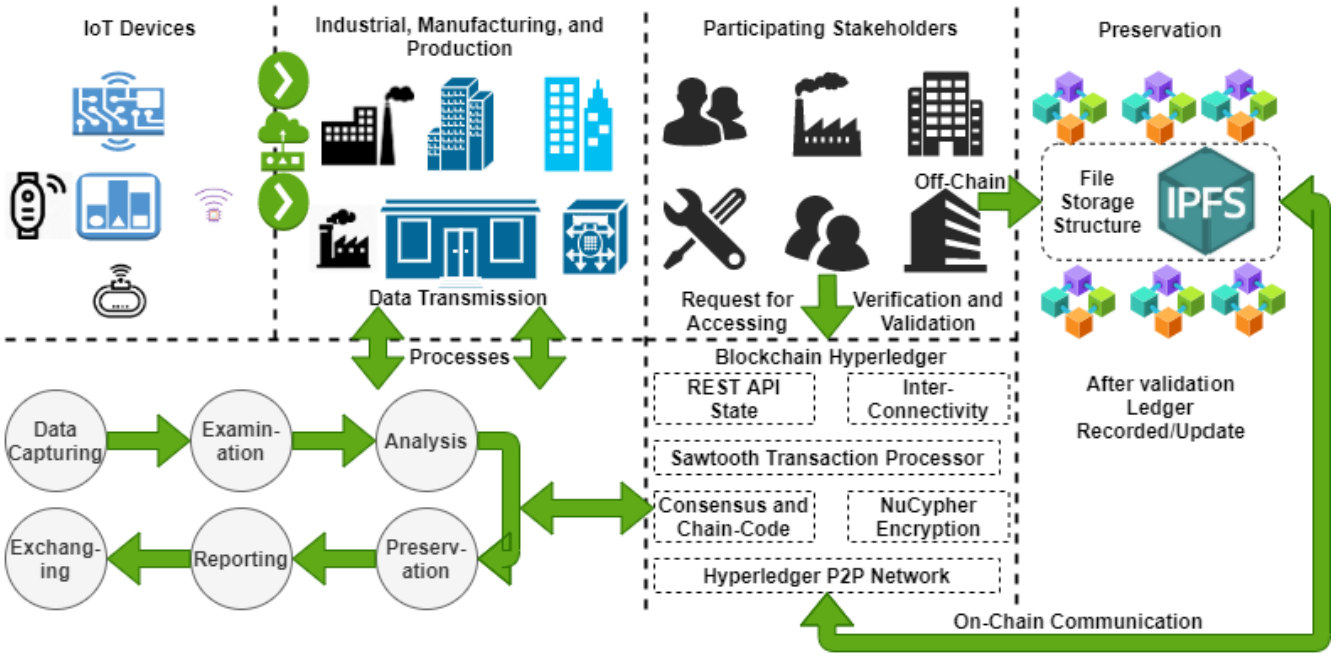


FIGURE 4. The proposed industrial iot with blockchain hyperledger sawtooth-enabled privacy preservation and security solution.

for further manufacturing processes with the help of a wireless sensor network, as shown in Figure 4. Whereas each unit is defined by its working protocols, such as industrial, manufacturing, and production executions. However, each unit runs on the proposed process for the purpose of secure executions of events of node transactions efficiently and effectively.

Although, this proposed framework allows a number of participating stakeholders, whose tasks are assigned in accordance with the role of participation, such as manufacturer, the state ministry of industries and supply, the federal ministry of industries and supply, business experts, analysts, tester, and other crucial board members, etc. These participating stakeholders initiate a number of IIoT transactions or requests to register/access the chain, as shown in Figure 4. However, each transaction initiate to execute completely is based on the defined protocols, Manu&ProAddRec() manage all the new updates, records, and exchange details with the participating stakeholder according to the consensus policies, as shown in Figure 5 and Table 2.

With the association of Hyperledger Sawtooth technology, each transaction passes through the step of secure executions, such as transaction processor (handle number of transactions and manage in a sequence of manner), REST API (reset state if previously utilized), node connectivity, handle transactions over the P2P network and protect ledger with the use of NuCypher Re-Encryption algorithm. For secure IIoT transaction executions, we design a blockchain hyperledger sawtooth-enabled consortium network, in which two communication channels are derived. On-chain communication channels manage and handle all the internal (chain transactions), implicitly. Whereas off-chain channels are designed

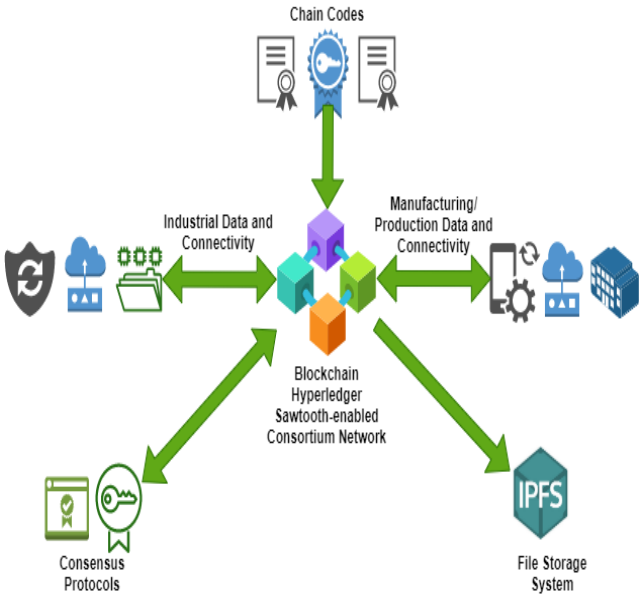


FIGURE 5. The IIoT-enabled events of nodes transactions execution/working operation.

to maintain external transactions (cross-platform), explicitly. All the logs (records of transactions) are stored in InterPlanetary File Storage System (a third-party distributed file storage structure that provides an immutable preservation scenario with minimally charged (cost: 10$/month) as compared to other states of the art). Each activity is recorded, preserved, and shared in the IPFS; however, if any changes occur in a single transaction after it is stored in the immutable storage

TABLE 2. Pseudo-contract: A conceptual chain code, consensus protocols, and executions.

Data and Assumptions: Blockchain Hyperledger-Sawtooth Expert is the Responsible for Managing all the Transactions Executions
Collect Industrial, Manufacturing, and Production Related Records and Manage Preservation
Handle Industrial Resource Consumption
Add Individual Record in the Ledger and Exchange Information
Manage Request of Participating Stakeholders
Handle Overall Industrial Verification and Validation Request
Secure Process of Industrial/Manufacturing Things
Initialization: int main: [A].X(a),
IoT devices registration,
IoTDR();
industrial/manufacturing things registration,
IIoTReg();
capturing industrial data,
CapID();
examine,
ExID();
analysis,
AnID();
preserve,
PrID();
exchange industrial transactions,
ExIT();

Blockchain Hyperledger Sawtooth-enabled timestamp,
[execution/run];
Process:
Blockchain Hyperledger-Sawtooth Expert is the Responsible that Manage all the Industrial Transactions and Recorded,
Verification/Validation();
if Blockchain Hyperledger-Sawtooth Expert == True;
then,
if IIoTReg == False
then, register first;
and maintain IIoTReg() contract;
else initiate node transactions in accordance with the secure processes
capturing industrial data CapID(), examine ExID(), analysis AnID() preserve PrID(), exchange industrial transactions ExIT();
NuCypher Re-Encryption;
and record each logs in the Manu&ProAddRec() contract with Nucypher Re-Encryption;
counter +1 (count);
else IoT device register, and previously ledger recorded,
any changes occur in the previous recorded transactions,
updateRec() contract and exchange update information to the participating stakeholders;
counter +1 (count);
check error, generate new state, store, exchange, rollback, and terminate;
Output: IIoTReg(), Manu&ProAddRec(), updateRec()

can be changed if the event gets a 51% vote of connected participants (consensus). These changes are possible because of the updateRec() contract, as shown in Figures 4, and 5.

- **Distributed Nodes Connectivity:** It allows for building secure channels (platforms) where industrial IoT nodes are interconnected. It restricts the direct path of messages/request deliverance and received events of transactions in a protected manner in terms of integrity, transparency, provenance, privacy, and security between a subspace of consortium hyperledger network members.
- **Certificate Authority (CA):** A CA is designed over the consortium network to create trust between participating stakeholders.
- **Peer-to-Peer (P2P):** The blockchain hyperledger sawtooth-enabled IIoT distributed network services initiated the node transactions. It contains a digital signature and NuCypher Re-Encryption before each peer is endorsed.
- **Consensus and Chain Code:** An automated execution of node transactions, including stakeholder participation, digital signature, IoT device registration, adding a new ledger, and updating the ledger, as shown in Table 2.

In addition, a comparative analysis of the proposed distributed framework with other state-of-the-art hyperledger involve in IIoT, most probably, in industrial, manufacturing, and productions, as mentioned in Table 3, and 4.

V. OPEN RESEARCH ISSUES AND FUTURE DIRECTION

This section discusses the preliminaries of the proposed framework and the events of nodes transactions execution and related problems while implementation. In addition, we highlight a few open challenges and limitations involved in the advanced industrial IoT development and deployment with some relevant solutions.

A. CROSS-CHAINING PLATFORM BETWEEN IoT-DEVICES

In the domain of blockchain-enabled IIoT technology, the platform interoperability is one of the challenging prospects involved while initiating transactions from one chain to the other with an explicit outer chain, which is not interconnected [90], [91]. The cross-chain platform solution allows different nodes to interconnect with each other, for example,

TABLE 3. Comparative analysis with other states of the art Hyperledger (1).

Other States of the Art Hyperledger	Two-way Authentication (A)	Network (N)	Channel (C)
Hyperledger Fabric [86]	Support	Consortium	On-chain and off-chain
Hyperledger Besu [87]	Require tunning	Private	Single
Hyperledger Indy [88]	Support	Used public/ private as well	Single
Hyperledger Composer [89]	Require tunning	Private	Single

TABLE 4. Comparative analysis with other states of the art Hyperledger (2).

Other States of the Art Hyperledger	Transaction Encryption (TE)	Storage (S)	Cost (Co)
Hyperledger Fabric [86]	Supports another encryption algorithm as well	IPFS/ Filecoin	Not required before simulating
Hyperledger Besu [87]	Hash-encryption	Third-party preservation mechanism used	Guest charge required
Hyperledger Indy [88]	Hash-encryption	Third-party preservation mechanism used	Guest charge required
Hyperledger Composer [89]	Hash-encryption	Third-party preservation mechanism used	Guest charge required

smart production units, manufacturing systems, supply chain management, and monitoring ecosystems. However, by this adaptation, the solution can provide a more efficient and effective industrial environment that supports and manage a secure service deliverance of industrial things-enabled transactions in a better manner in the distributed network infrastructure [92]. A single node of this designed platform, and various distinct nodes of other chains direct interact, communicate, exchange, and manage transactions in a secure preservation channel, and conduct meaningful nodes activities in the industrial environment. The existing legacy of industry, the process of production and services deliverance, and the current network structure create a lack of cross-chaining and intercommunication. Till now, it is hard to adopt and deploy platform interoperability between the devices and the industry due to the distribution and unsecure connectivity.

B. LACK OF INDUSTRIAL STANDARDIZATION

In this context, the IIoT ecosystem analysis every perspective of industrial things involved in the domain. There is a various range of data generation and processing that contributes to a lack of standardization in every channel of IoT because no standard protocols are established and yet not to be presented [92], [93]. However, the process layer of IIoT from data generation, capturing, and examination to documenting individual records are less reliable. As a result, the unavoidable distort consequences are provided, with minimal quality and consistency along with the increased rate of resource constraints consumption. To standardize the process of execution of IIoT, the blockchain hyperledger technology enforces an efficient platform and their standard approach with improved quality of finishing results [94].

C. DISTRIBUTED PRESERVATION AND PRIVACY ISSUES

The significant objective of this solution is to proper use of blockchain-enabling technology in the industrial environment for the purpose to protect personal information-connected participants, overall industrial transactions, data scheduling and processing, computation management, and organization, and gratifying individual types of records [94], [95]. All the records are stored on the blockchain distributed immutable storage along with the process of memory schedule (in terms of static, and dynamic). For the data management and preservation, there are two channels are derived to maintain inner and outer layer transactions properly and concurrently, such as on-chain and off-chain communication. The on-chain communication executes internal transactions, while the off-chain handles all the transactions and preservation explicitly. In the industrial ecosystems, the information of different units, such as production, supply chain, etc. is more sensitive and confidential. To protect communication channels while the data is exchanged, for example, production records, processing information, supply chain, and data sharing details, record management, organization, optimization, and computation; these issues consider one of the challenging aspects in the current IIoT. In this scenario, the individual information must check against and analyzed before being preserved in the distributed storage [96]. In addition, the most critical prospect is to structure preserved records in the blockchain network. The unexceptional transaction in this distributed network makes more costly services deliverance that directly affects the market cost.

D. OUTSOURCING COMPUTATION AND SECURITY MEASURES

Recently, cloud computing technology considering a successful technology in terms of offering scalable storage and computational resources [97]. In this manner, the data from the Internet of Things-enabled sensors is outsourced remotely and dynamically to the cloud-based central servers. The working process of outsourcing is preserving, sharing, processing, and executing collected data through the sensors via client-server-based centralization. This poses an extreme problem related to the attacks on IoT-enabled devices, such as complete system compromise, malicious attacks (DDoS), malicious insider (internal attacks), etc [98], [99], [100]. However, the blockchain-enabling distributed technology adopting for the purpose to reduces the number of existing attacks over the centralized server architecture. It associates with the cloud environment to protect the process of IoT-enabled sensor-based data collection to preserve against potential malicious attackers and unknown adversaries. The cryptographic hash-encryption algorithm has been utilized that ensure the ledger (transactions) protection in terms of integrity, transparency, confidentiality, provenance, and availability. It also performs arithmetic computations (hashing) once the transactions are scheduled for encryption. Business enterprises are needed to shift centralized outsourcing toward the fully homomorphic blockchain-enabled highly protected environment, which is based on lattices. It provides in-principle, an efficient solution, and better performance of IoT-cloud-enabled outsourcing computations with security [99], [100].

E. COMPLIANCE AND REGULATORY LIMITATIONS

The giant industries and policy management connect with the governmental authorities to design a new pathway of industrial layered-based transactions for secure services delivery in terms of data collection from units, examination, analysis, preservation, and records document in accordance with the defined protocols [99], [101], [102], [103]. The production units of industrial management need to consider the process of services scheduling, executing, managing, optimizing, and storing implications and ascription [104], [105]. However, considering these regulatory issues, the federal industrial governance and authority need to collaborate with the different private organizations and blockchain-enabling distributed technologies to design a secure environment for information transmission connectivity and exchange to reduce the cost of resources and computation energy utilization [106], [107]. The distributed application of IIoT is developed for the purpose of evaluating the performance of industrial things dynamically. And so, to calculate dissimilarities and formulate new authoritative protocols and procedures.

VI. CONCLUSION

The main objective of this study is to extract the current problem involved in industrial processes, due to this, we examine various state-of-the-art frameworks and their associative working operations, procedures, and protocols along with the IoT-enable efficient and secure executions. Thus, an analysis of the gap between two or more connected IoT devices during data transmission over the distributed network is discussed. In this paper, we discussed three different folds. First, we review almost a hundred research articles related to IoT, IIoT, blockchain, hyperledger, and distributed networks. Extracting knowledge in the previous studies related to privacy & security, analyzing current situations, proposing new pathways, and presented in a better manner. However, the second fold presents the working mechanism of the proposed blockchain hyperledger sawtooth-enabled distributed consortium framework, where a novel and secure industrial internet of things processes is highlighted. For the protected IIoT nodes transactions, we design two distinct communication channels, such as off-chain and on-chain over the consortium network to handle a number of transactions in a smooth manner. The on-chain communication channel is used to manage overall internal (implicitly) transactions execution; on the other side, off-chain channels tackle all the explicit chain transactions. Third, chain codes and consensus policies (multi-proof-of-work) are created that alleviate the resource adaptation of Blockchain-IIoT (B-IIoT) and make the ecosystem more suitable in the distributed environment. In addition, this proposed framework provides a resource-efficient platform, which does not affect the B-IIoT provenance, ledger integrity, transparency, traceability, availability, reliability, and maintains trustworthiness between participating stakeholders with no repudiation of hyperledger. Finally, the adaptation of proposed framework is considered as one of the good candidates for the giant-level implementation. Furthermore, the futuristic target of this research is to be deploying as the general-purpose solution of industrial, manufacturing, and production environments.

CONFLICT OF INTEREST

The authors of this paper declared that there is no conflict of interest.

AUTHORS CONTRIBUTIONS

- A.A.K. has written the original draft, preparation, and organization.
- A.A.K., A.A.L., Z.A.S., Z.D-P., and S.K. have analyzed, reviewed, suggested, rewrote, performed literature survey, edited, investigated, designed the framework, and explored tools for smart contracts (chain codes/consensus).

All authors of this paper read and agreed to the current published (online) version.

LIST OF ABBREVIATION

- IoT = Internet of Things
- IIoT = Industrial Internet of Things
- SHA-256 = Hash-256 Encryption Mechanism
- CA = Certificate Authority
- P2P = Peer-to-Peer network

- IIoTReg() = Industrial Internet of Things-enabled devices registration
- Manu&ProAddRec() = Add New Records of Manufacturing and Productions of IIoT
- updateRec() = Update Records
- QoS = Quality of Service
- 5G = Fifth generation network/Internet
- DDoS = Distributed Denial of Service
- LAN = Local Area Network
- Industry 4.0 = The Fourth Industrial Revolution
- PoW = Proof-of-Work
- IoPS = Internet of Production System

REFERENCES

[1] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Comput. Ind. Eng.*, vol. 155, May 2021, Art. no. 107174.

[2] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of art of Internet of Things (IoT)," *Arch. Comput. Methods Eng.*, vol. 29, pp. 1395–1413, Jul. 2021.

[3] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[4] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 88–122, 1st Quart., 2022.

[5] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *J. Ind. Inf. Integr.*, vol. 21, Mar. 2021, Art. no. 100190.

[6] A. A. Khan, A. A. Shaikh, Z. A. Shaikh, A. A. Laghari, and S. Karim, "IPM-model: AI and Metaheuristic-enabled face recognition using image partial matching for multimedia forensics investigation with genetic algorithm," *Multimedia Tools Appl.*, vol. 81, no. 17, pp. 23533–23549, Jul. 2022.

[7] D. G. S. Pivoto, L. F. F. de Almeida, R. da Rosa Righi, J. J. P. C. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial Internet of Things applications in industry 4.0: A literature review," *J. Manuf. Syst.*, vol. 58, pp. 176–192, Jan. 2021.

[8] Y. Guo, Z. Zhao, K. He, S. Lai, J. Xia, and L. Fan, "Efficient and flexible management for industrial Internet of Things: A federated learning approach," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108122.

[9] R. A. Khalil, N. Saeed, M. Masood, Y. M. Fard, M.-S. Alouini, and T. Y. Al-Naffouri, "Deep learning in the industrial Internet of Things: Potentials, challenges, and emerging applications," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11016–11040, Jul. 2021.

[10] A. A. Khan, A. A. Laghari, and S. A. Awan, "Machine learning in computer vision: A review," *EAI Trans. Scalable Inf. Syst.*, vol. 8, no. 32, p. e4, 2021.

[11] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy-efficient industrial Internet of Things: Overview and open issues," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7225–7237, Nov. 2021.

[12] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. J. Piran, and M. S. Hossain, "Toward accurate anomaly detection in industrial Internet of Things using hierarchical federated learning," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7110–7119, May 2022.

[13] G. Rathee, F. Ahmad, R. Sandhu, C. A. Kerrache, and M. A. Azad, "On the design and implementation of a secure blockchain-based hybrid framework for industrial Internet-of-Things," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102526.

[14] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2351–2383, 4th Quart., 2021.

[15] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for industrial Internet of Things: Opportunities, applications, and challenges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10430–10451, Jul. 2021.

[16] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, May 2022, Art. no. 103614.

[17] X. Cai, S. Geng, J. Zhang, D. Wu, Z. Cui, W. Zhang, and J. Chen, "A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7650–7658, Nov. 2021.

[18] B. Sujitha, V. S. Parvathy, E. L. Lydia, P. Rani, Z. Polkowski, and K. Shankar, "Optimal deep learning based image compression technique for data transmission on industrial Internet of Things applications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, Apr. 2020, Art. no. e3976.

[19] N. Malik, K. Alkhatib, Y. Sun, E. Knight, and Y. Jararweh, "A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems," *Appl. Stochastic Models Bus. Ind.*, vol. 37, no. 3, pp. 391–412, May 2021.

[20] A. A. Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission," *Appl. Sci.*, vol. 11, no. 22, Nov. 2021, Art. no. 10917.

[21] R. Kumar, F. K. Lakshmana, S. Kadry, and S. Rho, "A survey on blockchain for industrial Internet of Things," *Alexandria Eng. J.*, vol. 61, no. 8, pp. 6001–6022, 2022.

[22] A. A. Khan, Z. A. Shaikh, L. Belinskaja, L. Baitenova, Y. Vlasova, Z. Gerzelieva, A. A. Laghari, A. A. Abro, and S. Barykin, "A blockchain and Metaheuristic-enabled distributed architecture for smart agricultural analysis and ledger preservation solution: A collaborative approach," *Appl. Sci.*, vol. 12, no. 3, p. 1487, Jan. 2022.

[23] Q. Zhang, Y. Li, R. Wang, L. Liu, Y. Tan, and J. Hu, "Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things," *Int. J. Intell. Syst.*, vol. 36, no. 1, pp. 94–111, Jan. 2021.

[24] M. Sharma, S. Pant, D. K. Sharma, K. D. Gupta, V. Vashishth, and A. Chhabra, "Enabling security for the industrial Internet of Things using deep learning, blockchain, and coalitions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, 2021, Art. no. e4137.

[25] A. A. Khan, Z. A. Shaikh, A. A. Laghari, S. Bourouis, A. A. Wagan, and G. A. A. A. Ali, "Blockchain-aware distributed dynamic monitoring: A smart contract for fog-based drone management in land surface changes," *Atmosphere*, vol. 12, no. 11, p. 1525, Nov. 2021.

[26] R. Saha, G. Kumar, M. Conti, T. Devgun, T.-H. Kim, M. Alazab, and R. Thomas, "DHACS: Smart contract-based decentralized hybrid access control for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3452–3461, May 2022.

[27] Y. P. Tsang, C. H. Wu, W. H. Ip, and W.-L. Shiau, "Exploring the intellectual cores of the blockchain–Internet of Things (BIoT)," *J. Enterprise Inf. Manage.*, vol. 34, no. 5, pp. 1287–1317, Nov. 2021.

[28] M. A. Khan and K. A. Abuhasel, "Advanced metameric dimension framework for heterogeneous industrial Internet of Things," *Comput. Intell.*, vol. 37, no. 3, pp. 1367–1387, Aug. 2021.

[29] I. U. Din, A. Bano, K. A. Awan, A. Almogren, A. Altameem, and M. Guizani, "LightTrust: Lightweight trust management for edge devices in industrial Internet of Things," *IEEE Internet Things J.*, early access, May 18, 2021, doi: 10.1109/JIOT.2021.3081422.

[30] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning for industrial Internet of Things in future industries," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 192–199, Dec. 2021.

[31] L. C. Souza, E. R. Neto, E. S. Lima, and A. C. S. Junior, "Optically-powered wireless sensor nodes towards industrial Internet of Things," *Sensors*, vol. 22, no. 1, p. 57, Dec. 2021.

[32] R. G. Lins and S. N. Givigi, "Cooperative robotics and machine learning for smart manufacturing: Platform design and trends within the context of industrial Internet of Things," *IEEE Access*, vol. 9, pp. 95444–95455, 2021.

[33] J. Bader and A. L. Michala, "Searchable encryption with access control in industrial Internet of Things (IIoT)," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–10, May 2021.

[34] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, "A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions," *ACM Comput. Surv.*, vol. 55, no. 1, pp. 1–35, Jan. 2023.

[35] S. Latif, M. Driss, W. Boulila, Z. E. Huma, S. S. Jamal, Z. Idrees, and J. Ahmad, "Deep learning for the industrial Internet of Things (IIoT): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions," *Sensors*, vol. 21, no. 22, p. 7518, Nov. 2021.

[36] Y. Liu, R. Zhao, J. Kang, A. Yassine, D. Niyato, and J. Peng, "Towards communication-efficient and attack-resistant federated edge learning for industrial Internet of Things," *ACM Trans. Internet Technol.*, vol. 22, no. 3, pp. 1–22, Aug. 2022.

[37] K. Mao, G. Srivastava, R. M. Parizi, and M. S. Khan, "Multi-source fusion for weak target images in the industrial Internet of Things," *Comput. Commun.*, vol. 173, pp. 150–159, May 2021.

[38] X. Chen, J. Hu, Z. Chen, B. Lin, N. Xiong, and G. Min, "A reinforcement learning-empowered feedback control system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2724–2733, Apr. 2022.

[39] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF)," *Neurosci. Informat.*, vol. 2, no. 1, Mar. 2022, Art. no. 100030.

[40] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, "Botnet attack detection using local global best bat algorithm for industrial Internet of Things," *Electronics*, vol. 10, no. 11, p. 1341, Jun. 2021.

[41] H. Zhou, C. She, Y. Deng, M. Dohler, and A. Nallanathan, "Machine learning for massive industrial Internet of Things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 81–87, Aug. 2021.

[42] L. Ma, X. Wang, X. Wang, L. Wang, Y. Shi, and M. Huang, "TCDA: Truthful combinatorial double auctions for mobile edge computing in industrial Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 21, no. 11, pp. 4125–4138, Nov. 2022.

[43] M. K. Lim, Y. Li, C. Wang, and M.-L. Tseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Comput. Ind. Eng.*, vol. 154, Apr. 2021, Art. no. 107133.

[44] A. A. Khan, Z. A. Shaikh, L. Baitenova, L. Mutaliyeva, N. Moiseev, A. Mikhaylov, A. A. Laghari, S. A. Idris, and H. Alshazly, "QoS-ledger: Smart contracts and Metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing," *Electronics*, vol. 10, no. 24, p. 3083, Dec. 2021.

[45] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7669–7678, Nov. 2021.

[46] G. Wang, "Sok: Applying blockchain technology in industrial Internet of Things," *Cryptol. ePrint Arch.*, to be published.

[47] R. Sharma, "Blockchain for industrial Internet of Things (IIoT)," in *Blockchain and AI Technology in the Industrial Internet of Things*. Hershey, PA, USA: IGI Global, 2021, pp. 32–47.

[48] S. Iqbal, R. M. Noor, A. W. Malik, and A. U. Rahman, "Blockchain-enabled adaptive-learning-based resource-sharing framework for IIoT environment," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14746–14755, Oct. 2021.

[49] T. Liu, J. Liu, J. Wang, D. Zhai, Y. Liu, and X. He, "Anonymous storage and verification model of IIoT based on blockchain: Anonymous storage and verification model of IIoT production status based on blockchain," in *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, 2021, pp. 144–150.

[50] P. Zhang, H. Sun, J. Situ, C. Jiang, and D. Xie, "Federated transfer learning for IIoT devices with low computing power based on blockchain and edge computing," *IEEE Access*, vol. 9, pp. 98630–98638, 2021.

[51] S. Goyal, N. Sharma, I. Kaushik, and B. Bhushan, "Industrial revolution: Blockchain as a wave for industry 4.0 and IIoT," *Blockchain Appl. Secure IoT Frameworks, Technol. Shaping Future* vol. 1, p. 108, Jul. 2021.

[52] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 181, May 2021, Art. no. 103007.

[53] H. Khujamatov, E. Reypnazarov, D. Khasanov, and N. Akhmedov, "IoT, IIoT, and cyber-physical systems integration," in *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*. Cham, Switzerland: Springer, 2021, pp. 31–50.

[54] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of industrial Internet of Things (IIoT): A survey," *Sensors*, vol. 21, no. 19, p. 6647, Oct. 2021.

[55] Y. Lin, Z. Gao, W. Shi, Q. Wang, H. Li, M. Wang, Y. Yang, and L. Rui, "A novel architecture combining Oracle with decentralized learning for IIoT," *IEEE Internet Things J.*, early access, Feb. 11, 2022, doi: 10.1109/JIOT.2022.3150789.

[56] L. Arnold, J. Jöhnk, F. Vogt, and N. Urbach, "IIoT platforms' architectural features—A taxonomy and five prevalent archetypes," *Electron. Markets*, vol. 32, no. 2, pp. 927–944, Jun. 2022.

[57] K. Lin, X. Xu, and H. Gao, "TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107974.

[58] D. Stefanescu, P. Galán-García, L. Montalvillo, J. Unzilla, and A. Urbieta, "Towards a holistic DLT architecture for IIoT: Improved DAG for production lines," in *International Congress on Blockchain and Applications*. Cham, Switzerland: Springer, 2021, pp. 179–188.

[59] V. C. S. Rao, P. Kumarswamy, M. S. B. Phridviraj, S. Venkatramulu, and V. S. Rao, "5G enabled industrial Internet of Things (IIoT) architecture for smart manufacturing," in *Data Engineering and Communication Technology*. Singapore: Springer, 2021, pp. 193–201.

[60] Y. Zhao, M. Prabhu, R. R. Ahmed, and A. K. Sahu, "Research trends and performance of IIoT communication network-architectural layers of petrochemical industry 4.0 for coping with circular economy," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–32, Apr. 2021.

[61] S. Sen and L. Song, "An IIoT-based networked industrial control system architecture to secure industrial applications," in *Proc. IEEE Ind. Electron. Appl. Conf. (IEACon)*, Nov. 2021, pp. 280–285.

[62] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, "SecureIoT environment: Federated learning empowered approach for securing IIoT from data breach," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6406–6414, Sep. 2022.

[63] F. Banaie and M. Hashemzadeh, "Complementing IIoT services through AI: Feasibility and suitability," in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*. Cham, Switzerland: Springer, 2021, pp. 7–19.

[64] S. Mantravadi, C. Møller, C. Li, and R. Schnyder, "Design choices for next-generation IIoT-connected MES/MOM: An empirical study on smart factories," *Robot. Comput.-Integr. Manuf.*, vol. 73, Feb. 2022, Art. no. 102225.

[65] P. Goswami, A. Mukherjee, M. Maiti, S. K. S. Tyagi, and L. Yang, "A neural-network-based optimal resource allocation method for secure IIoT network," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2538–2544, Feb. 2022.

[66] A. Singh, S. Sharma, and J. Singh, "Nature-inspired algorithms for wireless sensor networks: A comprehensive survey," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100342.

[67] Y. Li, Q. Cheng, and W. Shi, "Security analysis of a lightweight identity-based two-party authenticated key agreement protocol for IIoT environments," *Secur. Commun. Netw.*, vol. 2021, pp. 1–6, Feb. 2021.

[68] T. Yang, "Multiple fixed target location algorithms in large-scale MIMO wireless sensor networks for IIoT," *IETE J. Res.*, pp. 1–10, 2022.

[69] S. Messaoud, S. Bouaafia, A. Bradai, M. A. Hajjaji, A. Mtibaa, and M. Atri, "Network slicing for industrial IoT and industrial wireless sensor network: Deep federated learning approach and its implementation challenges," 2022.

[70] A. N. Far, M. B. Hossein, A. K. Das, M. Fotouhi, S. M. Pournaghi, and M.-A. Doostari, "LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," *Wireless Netw.*, vol. 27, no. 2, pp. 1389–1412, 2021.

[71] M. Ibrahim, M. T. Abdullah, A. Abdullah, and T. Perumal, "The impact of memory-efficient bots on IoT-WSN botnet propagation," *Wireless Pers. Commun.*, vol. 119, no. 3, pp. 2093–2105, Aug. 2021.

[72] S. Singh and H. S. Saini, "PCTBC: Power control tree-based cluster approach for sybil attack in wireless sensor networks," *J. Circuits, Syst. Comput.*, vol. 30, no. 7, Jun. 2021, Art. no. 2150129.

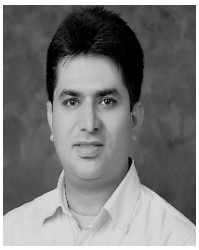
[73] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST," *Comput. Netw.*, vol. 198, Oct. 2021, Art. no. 108413.

[74] P. S. Chatterjee, "Detection of node cloning attack in WSN to secure IoT-based application: A systematic survey," in *IoT Applications, Security Threats, and Countermeasures*. Boca Raton, FL, USA: CRC Press, 2021, pp. 247–260.

[75] Yadav, Ashok, and Arun Kumar, "Intrusion detection and prevention using RNN in WSN," in *Inventive Computation and Information Technologies*. Singapore: Springer, 2022, pp. 531–539.
[76] T. A. S. Srinivas and S. S. Manivannan, "Black hole and selective forwarding attack detection and prevention in IoT in health care sector: Hybrid meta-heuristic-based shortest path routing," *J. Ambient Intell. Smart Environ.*, vol. 13, no. 2, pp. 133–156, Mar. 2021.
[77] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," *Mater. Today, Proc.*, vol. 51, pp. 161–165, 2022.
[78] S. Sharma and A. Kaur, "Survey on wireless sensor network, its applications and issues," *J. Phys., Conf. Ser.*, vol. 1969, no. 1, Jul. 2021, Art. no. 012042.
[79] I. Naydenova, Z. Kovacheva, and K. Kaloyanova, "Data quality: Enterprise Initiatives' issues and WSN challenges," *Sensors Transducers*, vol. 251, no. 4, pp. 37–46, 2021.
[80] A. Miglani and N. Kumar, "Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review," *Comput. Commun.*, vol. 178, pp. 37–63, Oct. 2021.
[81] H. Wang, D. He, J. Yu, N. N. Xiong, and B. Wu, "RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks," *J. Parallel Distrib. Comput.*, vol. 152, pp. 1–10, Jun. 2021.
[82] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90075–90083, 2021.
[83] A. D. Dwivedi, R. Singh, K. Kaushik, R. R. Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans. Emerg. Telecommun. Technol.*, 2021, Art. no. e4329.
[84] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K.-R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.
[85] S. Kaushik, "Blockchain and 5G-enabled Internet of Things: Background and preliminaries," in *Blockchain for 5G-Enabled IoT*. Cham, Switzerland: Springer, 2021, pp. 3–31.
[86] C.-L. Chen, J. Yang, W.-J. Tsaur, W. Weng, C.-M. Wu, and X. Wei, "Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application," *Sensors*, vol. 22, no. 3, p. 1146, Feb. 2022.
[87] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17236–17260, Dec. 2021.
[88] A. Banerjee, B. Dutta, T. Mandal, R. Chakraborty, and R. Mondal, "Blockchain in IoT and beyond: Case studies on interoperability and privacy," in *Blockchain based Internet Things*. Springer, Singapore, 2022, pp. 113–138.
[89] P. W. Khan and Y.-C. Byun, "Secure transactions management using blockchain as a service software for the Internet of Things," in *Software Engineering in IoT, Big Data, Cloud and Mobile Computing*. Cham, Switzerland: Springer, 2021, pp. 117–128.
[90] R. Kumar, R. Sindhwani, and P. L. Singh, "IIoT implementation challenges: Analysis and mitigation by blockchain," *J. Global Operations Strategic Sourcing*, vol. 15, no. 3, pp. 363–379, Aug. 2022.
[91] N. Jha and D. Prashar, "Using blockchain in resolving the challenges faced by IIoT," in *Industrial Internet of Things*. Boca Raton, FL, USA: CRC Press, 2022, pp. 189–216.
[92] M. Kaur, M. Z. Khan, S. Gupta, and A. Alsaeedi, "Adoption of blockchain with 5G networks for industrial IoT: Recent advances, challenges, and potential solutions," *IEEE Access*, vol. 10, pp. 981–997, 2022.
[93] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, "Secure data of industrial Internet of Things in a cement factory based on a blockchain technology," *Appl. Sci.*, vol. 11, no. 14, p. 6376, Jul. 2021.
[94] L. K. Ramasamy and S. Kadry, "Combination of blockchain and IIOT," in *Blockchain in the Industrial Internet of Things*, 2021.
[95] A. A. Khan, A. A. Laghari, D.-S. Liu, A. A. Shaikh, D.-D. Ma, C.-Y. Wang, and A. A. Wagan, "EPS-ledger: Blockchain hyperledger sawtooth-enabled distributed power systems chain of operation and control node privacy and security," *Electronics*, vol. 10, no. 19, p. 2395, Sep. 2021.
[96] S. Najjar-Ghabel, S. Yousefi, and H. Karimipour, "Blockchain applications in the industrial Internet of Things," in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*. Cham, Switzerland: Springer, 2021, pp. 41–76.
[97] D. Job and V. Paul, "Challenges, security mechanisms, and research areas in IoT and IioT," in *Internet of Things and Its Applications*. Cham, Switzerland: Springer, 2022, pp. 523–538.
[98] S. R. Shakya and S. Jha, "Challenges in industrial Internet of Things (IIoT)," in *Industrial Internet of Things*. Boca Raton, FL, USA: CRC Press, 2022, pp. 19–39.
[99] Z. A. Shaikh, A. A. Khan, L. Baitenova, G. Zambinova, N. Yegina, N. Ivolgina, A. A. Laghari, and S. E. Barykin, "Blockchain hyperledger with non-linear machine learning: A novel and secure educational accreditation registration and distributed ledger preservation architecture," *Appl. Sci.*, vol. 12, no. 5, p. 2534, Feb. 2022.
[100] A. Aoun, A. Ilinca, M. Ghandour, and H. Ibrahim, "A review of industry 4.0 characteristics and challenges, with potential improvements using blockchain technology," *Comput. Ind. Eng.*, vol. 162, Dec. 2021, Art. no. 107746.
[101] W. Zhou, M. Liu, C. Chen, and Z. Luo, "A research on the development and application of blockchain technology in industrial Internet of Things," in *Proc. Comput., Commun. IoT Appl. (ComComAp)*, Nov. 2021, pp. 83–88.
[102] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, and I. Kaushik, "Applicability of industrial IoT in diversified sectors: Evolution, applications and challenges," in *Multimedia Technologies in the Internet of Things Environment*. Singapore: Springer, 2021, pp. 45–67.
[103] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-based Internet of Things and industrial IoT: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2021, pp. 1–21, Aug. 2021.
[104] S. Lee, M. Kim, J. Lee, R.-H. Hsu, and T. Q. S. Quek, "Is blockchain suitable for data freshness? An age-of-information perspective," *IEEE Netw.*, vol. 35, no. 2, pp. 96–103, Mar. 2021.
[105] Y. Zuo, "Making smart manufacturing smarter—A survey on blockchain technology in industry 4.0," *Enterprise Inf. Syst.*, vol. 15, no. 10, pp. 1323–1353, Nov. 2021.
[106] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1918–1929, Mar. 2022.
[107] Z. Fang, J. Wang, Y. Ren, Z. Han, H. V. Poor, and L. Hanzo, "Age of information in energy harvesting aided massive multiple access networks," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 5, pp. 1441–1456, May 2022.

ABDULLAH AYUB KHAN received the Ph.D. degree from the Department of Computer Science, Sindh Madressatul Islam University, Karachi. He has published around 40 research articles in well-reputed journals/publishers (such as IEEE Access, IEEE Transactions, MDPI, Elsevier, Spring, Wiley, and Hindawi) in the domain of digital forensics, cyber security, blockchain, hyperledger technology, cloud computing, and artificial intelligence.

ASIF ALI LAGHARI received the B.S. and master's degrees in information technology from the Quaid-e-Awam University of Engineering Science and Technology Nawabshah, Pakistan, in 2007 and 2014, respectively. From 2007 to 2008, he was a Lecturer at the Computer and Information Science Department, Digital Institute of Information Technology, Pakistan. In 2015, he joined the School of the Computer Science and Technology, Harbin Institute of Technology, where he was a Ph.D. Student. He is currently an Assistant Professor at Sindh Madressatul Islam University, Karachi, Pakistan. He has published more than 60 technical articles in scientific journals and conference proceedings. His current research interests include machine learning, computer networks, cloud computing, the IoT, fog computing, and multimedia QoE management.



ZAFFAR AHMED SHAIKH received the Ph.D. degree in computer sciences from IBA-Karachi, Pakistan. He has completed the Doctoral Research work at EPFL (Switzerland). He is an HEC-approved Ph.D. Supervisor in the field of physical sciences. He has published more than 45 research articles in reputed journals and conferences. He contributes to reviewing manuscripts of high-impact journals for more than ten years. His current research interests include AI, big data, data sciences, educational technology, e-learning, e-governance, expert systems, food processing, green technology, ICT policy and planning, the IoT, learning environments (theories, models, and frameworks), metals, MOOCs, OERs, pharmacoinformatics, social software, solar energy, sustainability, and TEL.

ZDZISLAWA DACKO-PIKIEWICZ received the Ph.D. degree in sociology, specializing in education sociology, youth sociology, and EU integration, and the doctor's and habilitation degrees. She has been a Professor at AWSB and a Rector at WSB University, since 2008. In addition to this function, she also holds the position of the Vice President of the Council of Chamber of Commerce and Industry in Katowice (since 2014) and the Chairperson of the Commission for Competitiveness, Innovation and Cooperation between Science and Business (since 2015). She is also a member of the Lewiatan Confederation, which represents the interests of polish private entrepreneurs. In recognition of her contribution and achievements in the field of education, she has been honored with several awards, which include: the Medal of the Commission of the National Education awarded by the Ministry of National Education in 2004, the Bronze Cross of Merit in 2007, an Honorary Medal awarded by the Ministry of Foreign Affairs of the Czech Republic in 2007, the Silver Medal of Merits for the Police in 2013, the Dąbrowa Górnicza Citizen of the Year in 2014, and the Manager of the Region in the category of Education in 2014. She is also a double laureate of the second degree individual award granted by the Minister of Science and Higher Education for outstanding organizational achievements in academic year 2014/2015 and 2015/2016. For several years, she has been actively contributing, inter alia, to the development of cooperation between science and business sectors.

SEBASTIAN KOT is currently an Associate Professor of management and supply chain management at the Faculty of Management, Czestochowa University of Technology. He has over 20 years of teaching, research, and managerial experience in higher education. He is also the Extraordinary Professor at the North-West University and University of Johannesburg, South Africa. He is a Founder and the Co-Editor of PJMS. He is a member of SB: Advanced Logistics Systems; Supply Chain Management Journal.