WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing IoT Security Through Blockchain Integration

Mahi Rajput[1], Tanisha Tyagi[2], Aarzoo Tyagi[3], Ms. Jyoti[4]

[1,2,3]Scholar Student, [4]Assistant Professor
Computer Science & Engineering, IOT DEPARTMENT
Raj Kumar Goel Institute of Technology, Ghaziabad, UP, India
[1]mahikpc3@gmail.com,[2]tyagitanisha34@gmail.com,[3]aarzootyagi57@gmail.com

ABSTRACT :

The rapid expansion of Internet of Things (IoT) technologies has increasingly captured the interest of the research community, particularly in the context of industrial applications. This momentum is driven by advancements in Industrial Internet of Things (IIoT) infrastructure and the evolving requirements posed by Industry 5.0, which emphasize both innovation and efficiency under resource and security constraints. As these systems evolve, they introduce novel architectural concepts while also posing critical challenges related to data security, device interoperability, transaction integrity, trust management, privacy, and holistic system protection. Effectively addressing these challenges is vital for optimizing industrial operations and delivering high-quality services.

Furthermore, integrating blockchain with the Industrial Internet of Things (IIoT) has emerged as a significant focus of current research and development. Despite its potential, one of the key obstacles is the limited performance capacity of IIoT devices and their associated nodes, which contrasts sharply with the significant computational demands of permissioned private blockchain networks. Current approaches—such as re-encryption frameworks like Uncypher, hash-based data structures, and proof-of-work algorithms—often require extensive processing power, making their implementation in IIoT

I. INTRODUCTION

The growth and advancement of the Internet of Things (IoT) have brought about transformative shifts in the field of information technology. By enabling interconnected devices to communicate effortlessly, IoT supports intelligent automation across multiple domains, minimizing the reliance on manual operations. Furthermore, progress in artificial intelligence (AI), networked connectivity, and smart communication protocols has enhanced the ability to optimize and manage data dynamically—especially within industrial environments.

Maintaining the integrity and transparency of transactions is vital for the efficient functioning of IIoT-based smart manufacturing systems. To protect against physical and cyber threats, experts have implemented advanced security frameworks that leverage cryptographic encryption. These methods strengthen data protection by using secure ledger systems; however, they also impose considerable strain on processing power, network capacity, and overall system performance.

Optimizing industrial environments involves minimizing network load, blocking unauthorized access, and preventing the misuse of IoT devices. A continual challenge lies in managing and validating vendor access to ensure that only approved actions are executed without compromising system security. Equally important is the protection of sensitive personal data related to employees and stakeholders. This encompasses securing proprietary industrial code, facilitating real-time data monitoring, and maintaining safe configuration settings for intelligent manufacturing units.

Blockchain technology has been adopted in diverse industrial production environments to improve data reliability, ensure transparency, support traceability, and verify authenticity, thereby enabling secure data management and analysis. With its decentralized nature, blockchain is gaining traction among IIoT professionals as a strong defense against cyber threats that frequently exploit centralized systems like client-server models, underscoring the demand for more resilient security solutions.

The decentralized modular structure of blockchain fortifies IIoT ecosystems by boosting security across distributed IoT nodes. It ensures secure data transmission using cryptographic techniques like the NuCypher Re-Encryption algorithm. Moreover, blockchain supports the deployment of intrusion detection systems, which are essential for identifying and responding to cyber threats effectively.

Further security measures, such as firewalls, anti-disclosure tools, and strong protocols, are integrated to enhance the platform's protection. These safeguards help maintain security, privacy, data integrity, and transparency, while also building confidence in the reliability of the blockchain ledger.

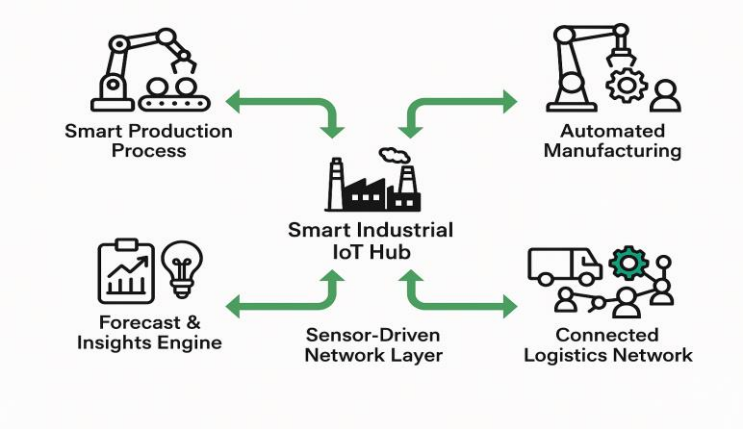

Figure1. Integrated Architecture of a Smart Industrial IoT Ecosystem

A. RATIONALE BEHIND THE STUDY

This study explores the security and privacy issues within the Industrial IoT (IIoT) environment and examines the complexities involved in connecting numerous nodes across the network. One key issue highlighted is interoperability, for which the paper suggests a solution involving the creation of a consortium communication channel. This channel facilitates both private and public transactions securely within a Peer-to-Peer (P2P) network.
To tackle these issues, a new blockchain-based framework is proposed, providing improved security for IoT transactions as they travel from source to destination (device-to-device) within the consortium network. This framework guarantees the safeguarding of individual data packets during transmission by utilizing NuCypher Re-Encryption, which supports batch-level privacy.

B. RESEARCH AIMS AND KEY CONTRIBUTIONS

The main objective of this research is to improve the handling of data produced by IoT-enabled devices in industrial settings, covering stages such a`s data collection, inspection, analysis, storage, presentation, and documentation, with a focus on enhancing security. The study proposes a flexible framework for safeguarding IoT transactions, allowing for accurate tracking of elements that affect distributed systems and computing nodes within the ecosystem. It also highlights the importance of a strong analytical strategy to reduce risks tied to the execution and management of IoT-node transactions across their entire lifecycle.
The core contributions of this study are summarized as follows:

- **Extensive Literature Review:** This research reviews over 100 academic sources focused on areas including IoT, industrial data management, decentralized network architectures, communication protocols, blockchain systems, and Hyperledger frameworks. It offers a structured analysis of the existing privacy and security challenges within current Industrial IoT implementations.
- **Proposed Framework**: This research introduces a secure blockchain framework built on Hyperledger, specifically designed for the Industrial Internet of Things (IIoT), featuring a layered structure to streamline transaction processing.
- **Automated Processes:** This study explains how chain codes are utilized to streamline different transaction activities involving IoT nodes. These activities include registering IIoT devices, gathering and analyzing data, securely storing and structuring information, and effectively handling data transmission across distributed networks—both on-chain and off-chain.Finally, the study evaluates and analyzes various design-related future challenges, issues, and limitations associated with IoT-enabled industrial ecosystems. It also proposes several solutions aimed at enhancing efficiency, reliability, and performance within distributed environments.

II. INTEGRATING INTERNET OF THINGS (IoT) WITH BLOCKCHAIN TECHNOLOGY

The Internet of Things (IoT) has become a transformative force across industrial, manufacturing, production, and supply chain domains. Researchers have highlighted its substantial economic potential, with contributions projected in the billions. Presently, industries are adopting on-demand models that leverage IoT technologies, including cloud-based platforms, to streamline operations. These models enable broad, real-time access, facilitate client-server connectivity, support resource sharing, and allow for flexible system configurations—all while requiring minimal intervention from service providers.
This study provides a comprehensive assessment of Industrial IoT, exploring the reasons for embracing distributed systems. The literature review highlights the main benefits of Industrial IoT and explores the privacy and security issues found in current implementations.

A. ADVANCEMENTS IN INDUSTRIAL INTERNET OF THINGS (IIoT) AND SMART MANUFACTURING

Smart industrial and manufacturing execution is a central concept in the Industrial Internet of Things (IIoT), shaping the future of automation. This approach integrates a range of techniques that correspond with evolving trends in centralized, client-server network architectures used for data exchange. The primary goal is to revolutionize industrial operations. To boost the effectiveness and dependability of IIoT systems, researchers have proposed various strategies aimed at refining existing infrastructures. These include advancements in intelligent communication, distributed network frameworks, dynamic transaction processing, service optimization, and the enhancement of data security and privacy.

Intelligent industrial and manufacturing systems are defined by several core features: (i) digital transformation, (ii) automated intelligent operations, (iii) a focus on service-driven architectures, (iv) seamless connectivity and communication, (v) smart and digitized machinery, (vi) cooperative network structures, and (vii) efficient, adaptable maintenance strategies. These elements play a crucial role in advancing industrial capabilities under the Industry 4.0 paradigm, enhancing productivity and reducing reliance on human labor through the integration of artificial intelligence and cognitive automation technologies.

B. BLOCKCHAIN ENABLING TECHNOLOGY

Recent advancements in industrial IoT have greatly enhanced system efficiency and reliability. Moreover, intelligent and self-adaptive IoT devices are receiving increasing attention. The main objective is to develop an environment that efficiently captures and processes large amounts of data, facilitating seamless information exchange among all stakeholders. However, the self-adaptive processes in industrial systems are still susceptible to vulnerabilities. Issues such as delays induced by malicious attacks, reliance on hierarchical layers, and difficulties in maintaining ledger integrity can disrupt

A. EXISTING ARCHITECTURAL FRAMEWORK OF INDUSTRIAL IoT (IIoT)

At present, no unified technology, protocol, methodology, or standardized framework exists to comprehensively guide the design, development, and deployment of secure IoT architectures. This remains a major challenge, particularly with the growing integration of IoT into industrial environments. The Industrial Internet of Things (IIoT) operates as a coordinated network of interconnected components—including wireless sensors, transaction handlers, actuators, communication interfaces, and transceivers—that work together within industrial systems to support operational functionality.

Each layer has a specific function in establishing connections, enabling interactions, and facilitating communication between IoT devices. A thorough overview of each layer and its role within the industrial environment is provided below:

1 APPLICATION LAYER

This layer is responsible for overseeing the operation of various applications that dynamically manage and monitor IoT devices. Acting as a bridge between stakeholders and their connected nodes, the application layer enables interaction between end-point devices and transactional activities. It establishes communication pathways through authorized automated software systems, which interface with a centralized database using conventional client-server communication protocols.

2 MIDDLEWARE AND SUPPORT INFRASTRUCTURE LAYER

The middleware or support layer functions within a centralized server-based architecture, often following a traditional three-tier model to facilitate secure data flow to the internet layer, which handles communication between smart devices. This layer also plays a crucial role in defending against cyber threats. By maintaining the three-tier configuration, it mitigates security risks and addresses vulnerabilities within industrial systems. It verifies data originating from the perception layer using private key encryption methods before transmitting it to the internet layer. Common security concerns in industrial settings that demand focused mitigation strategies include DDoS attacks, phishing attempts, unauthorized system access, and insider threats.

3 SENSING AND DATA ACQUISITION LAYER

The middleware layer functions within a centralized server-based architecture, commonly following a three-tier traditional model to ensure the secure transfer of data to the internet layer, which handles communication among smart devices. In addition to managing data flow, this layer acts as a security barrier against various cyber threats. By leveraging the three-tier structure, it helps to mitigate risks and address vulnerabilities in industrial systems. It also performs authentication of data collected from the perception layer using private key encryption before transmitting it onward.

4 SECURE BUSINESS LAYER

The secure business layer oversees enterprise-level transactions, guided by predefined business rules. These rules ensure the secure execution of IIoT transactions and the effective management and operation of business processes associated with IoT deployment.

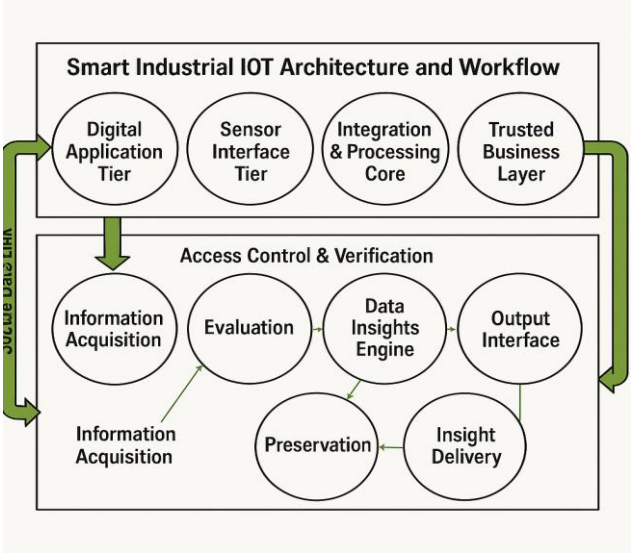

Figure2. Layered Architecture and Workflow of a Secure Industrial IoT Ecosystem

B. FUNCTIONS OF WIRELESS SENSOR NETWORKS IN INDUSTRY: RISKS AND SECURITY MEASURES

Wireless sensor networks are increasingly used in industrial environments to support smart manufacturing through efficient communication, monitoring, and embedded computing. Their growth is driven by reliability and widespread adoption. These networks, made up of interconnected components, face security challenges, which are addressed through targeted protective measures discussed below.

• **Botnet:** In IoT environments, a botnet is a group of connected devices that can be hijacked and controlled to carry out coordinated malicious activities. These networks often utilize routers to manage data transmission paths. However, they are highly susceptible to malware infections, which can compromise system control by exploiting weak or stolen credentialsAfter being compromised, attackers can infiltrate the system without authorization, jeopardizing its integrity. One major risk associated with this is the execution of distributed denial-of-service (DDoS) attacks, which are designed to interrupt the normal operations and availability of targeted systems.

• **Distributed attack (DDoS):** In today's industrial settings, IoT devices are increasingly exploited both as targets and instruments for carrying out distributed denial-of-service (DDoS) attacks. With the growing number of IoT deployments, these attacks are projected to become more frequent and large-scale. DDoS attacks are considered among the most severe threats in the evolving landscape of Industrial IoT (IIoT), posing serious risks to system stability and operational continuity.

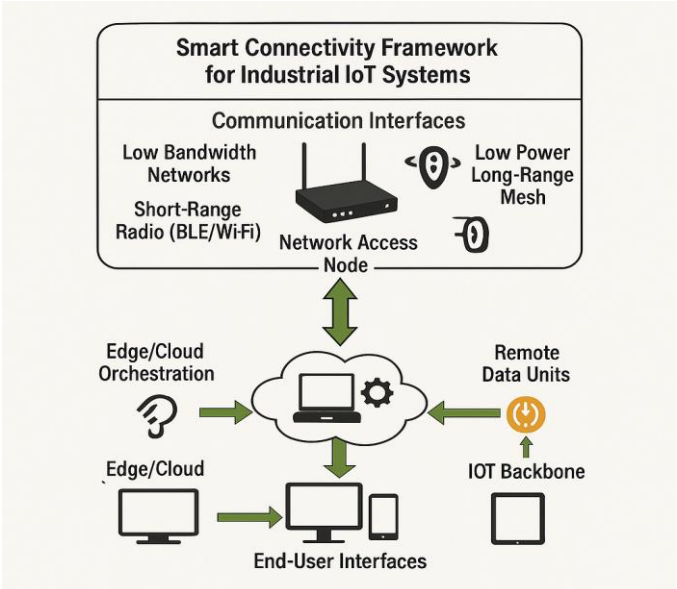

Figure3. Architecture of Smart Connectivity in Industrial IoT Environments

• **Hardware Demands and Associated Complexity:** The efficiency of wireless sensor hardware nodes relies on several functional aspects, including data storage, processing capabilities, power supply, energy consumption, and data transmission. These hardware components are widely utilized across

various areas, particularly within network systems, to ensure smooth and effective operations. Although hardware plays a central role, it typically operates under the control of independent operating systems, with each hardware node managed separately by its respective OS.

• **Fault tolerance:** Wireless sensor nodes are designed to operate reliably within the constraints of network protocols. However, executing transactions across a distributed network introduces certain limitations. These include energy consumption due to battery dependency, potential node failures affecting connectivity, and interference from external sources, all of which can impact overall network performance and resilience.

C INTEGRATING IIoT WITH BLOCKCHAIN AND 5G TECHNOLOGIES

The Internet of Things (IoT) has significantly improved operational efficiency, control, and data management in distributed systems, leading to its widespread use in industrial sectors like manufacturing. By automating and modernizing conventional processes, Industrial IoT (IIoT) enhances productivity and asset management. However, most current IIoT systems still depend on a centralized client-server model, where data flows through a single channel and is stored in one central location. This setup introduces limitations in terms of scalability, security, and privacy. Moreover, it results in higher computational loads, complex device maintenance, and reliance on third-party services, creating key challenges for industrial adoption

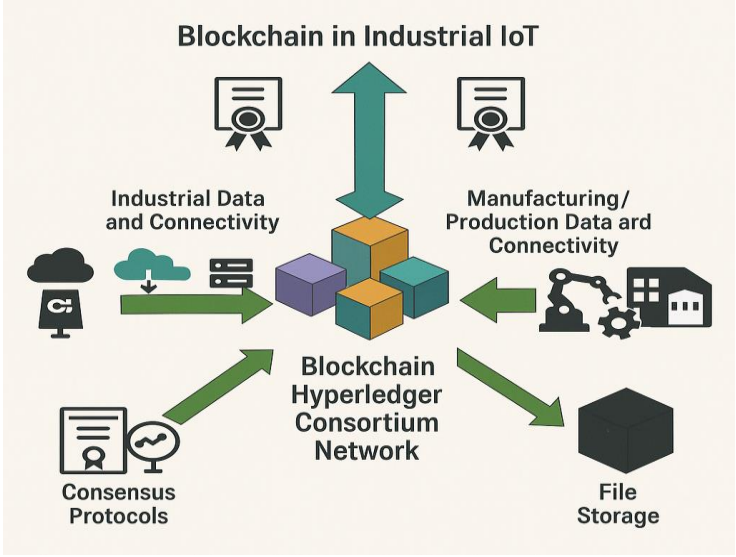

Figure5. Blockchain-Enabled Framework for Industrial IoT Integration

IV RECOMMENDED SYSTEM FRAMEWORK

Figure 4 demonstrates a six-layered framework designed for secure IIoT integration using blockchain technology. The architecture begins with registering IoT devices—such as ESP32 and LoRaWAN—allowing for both current device inclusion and future expansion. Device validation is carried out by a Blockchain Hyperledger Sawtooth module using a smart contract function (IIoTReg()), ensuring only authorized devices can participate in network communication.

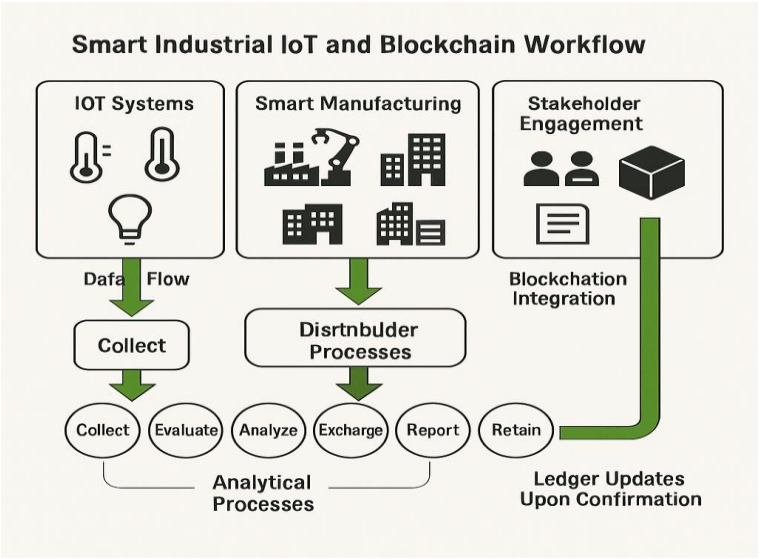

Figure4. Secure Workflow Integration of Industrial IoT and Blockchain Systems

Once validated, devices initiate industrial transactions via wireless sensor networks, guided by task-specific protocols in manufacturing and production. The system accommodates multiple stakeholders—such as manufacturers, analysts, and policymakers—who interact with the network under predefined roles and submit transaction requests. These requests are handled through smart contracts like Manu&ProAddRec(), with each operation subject to the platform's consensus policies.

The use of Hyperledger Sawtooth supports secure transaction processing through peer-to-peer channels and REST APIs, while the NuCypher algorithm reinforces data privacy. The framework employs both on-chain and off-chain communication pathways to separate internal operations from external exchanges.

V. CURRENT RESEARCH CHALLENGES AND FUTURE PROSPECTS

This section presents an overview of the proposed framework, emphasizing node transaction execution and related implementation challenges. It also highlights unresolved issues and constraints in developing advanced IIoT systems while suggesting possible approaches for overcoming these obstacles.

A. INTEROPERABLE CROSS-CHAIN FRAMEWORK FOR IoT DEVICES:

In IIoT environments supported by blockchain, cross-platform interoperability remains a major hurdle, particularly when managing transactions across isolated chains. Cross-chain frameworks address this by enabling integration between various systems such as production units, supply chains, and monitoring platforms. This enhances industrial efficiency by allowing secure, direct interaction and data exchange across nodes from different chains. Transactions are processed through protected channels to maintain data integrity. However, legacy systems and outdated network infrastructures present challenges for implementing such solutions, as they often lack the flexibility and security required for distributed cross-chain communication in industrial applications.

B. LACK OF INDUSTRIAL STANDARDIZATION

In the IIoT ecosystem, the analysis covers all aspects of industrial entities involved. There is a wide range of data generation and processing that contributes to the absence of standardization across IoT channels, as no universal protocols have been established or presented. The process layer of IIoT, which involves data generation capturing, analysis, and record-keeping, remains unreliable. This leads to inevitable distortions, reduced quality, inconsistency, and increased resource consumption. To address these challenges and standardize IIoT operations, blockchain Hyperledger technology provides an efficient platform and a standardized approach that enhances the quality and consistency of results.

Hyperledger Variant	Transaction Encryption (TE)	Storage (S)	Cost (Co)
Hyperledger Fabric	Compatible with various encryption schemes	IPFS/Filecoin	No fee needed for simulation
Hyperledger Besu	Hash-based encryption	External storage methods applied	Guest payment needed
Hyperledger Indy	Hash-based encryption	External storage methods applied	Guest payment needed
Hyperledger Composer	Hash-based encryption	External storage methods applied	Guest payment needed

Tabel 1: Comparison of Hyperledger Variants Based on Encryption, Storage Solutions, and Cost Factors.

C. DECENTRALIZED STORAGE AND DATA PRIVACY CHALLENGES

In industrial ecosystems, sensitive information related to various units, such as production and supply chain data, must be protected. This includes securing communication channels when exchanging critical data like production records, processing details, and supply chain information. Managing, organizing, and optimizing these records and computations poses a significant challenge in IIoT. In this context, individual data must undergo verification before being stored in the distributed blockchain storage. Moreover, structuring these preserved records within the blockchain network can lead to higher service delivery costs, directly impacting market pricing.

D EXTERNAL COMPUTATION AND PROTECTIVE MECHANISMS

Cloud computing has become a widely adopted solution, offering scalable resources for storing and processing data generated by IoT sensors. Typically, this data is offloaded to centralized cloud servers for handling tasks such as storage, analysis, and execution. However, this centralized model exposes

systems to risks like DDoS attacks and internal security breaches. To address these concerns, blockchain technology is integrated to decentralize data management and improve security. Through cryptographic hashing, transaction records are protected for integrity and confidentiality. Transitioning to homomorphic encryption and blockchain-based models further strengthens security, enabling secure outsourced computations while maintaining performance and safeguarding IoT-cloud operations.

E REGULATORY AND COMPLIANCE CHALLENGES

Major industries and policymakers often coordinate with government bodies to establish secure frameworks for conducting industrial transactions. These frameworks are responsible for the safe acquisition, analysis, and storage of data, adhering to regulatory protocols. Industrial administrators must handle task scheduling, execution, resource management, and secure data storage with regulatory compliance in mind. To address compliance concerns, collaboration between federal agencies and blockchain-based distributed systems is essential to ensure secure data flow and cost efficiency. These IIoT applications facilitate real-time performance monitoring of industrial systems, enabling the detection of anomalies and development of new procedures based on operational insights.

VI. CONCLUSION

This study aims to resolve key challenges in industrial processes by exploring advanced frameworks and protocols that support secure IoT-based operations. It reviews nearly 100 research articles covering IoT, IIoT, blockchain, and Hyperledger to identify existing gaps and propose efficient solutions. A Hyperledger Sawtooth-based consortium framework is introduced, featuring dual communication channels—on-chain for internal, and off-chain for external transactions—to enhance security. The framework incorporates chain codes and multi-proof-of-work consensus mechanisms to optimize resource usage. Ensuring transparency, trust, and data integrity, the model is proposed as a scalable solution suitable for broad deployment across industrial and manufacturing environments**.**

VIII. 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. 1001