Block chain based privacy preserving shop floor auditing architecture

[1]Mr. N. Sendhil Kumar, [2]M.Rohith rathna sekhar, [3]Pulluru Nayabrasool, [4]Mayakuntla Adarsh
[1].Associate Professor/MCA, Sri Venkateswara College of Engineering and Technology (Autonomous) Chittoor, Andhra Pradesh-517217
[2,3,4] MCA Students, Sri Venkateswara College of Engineering and Technology (Autonomous) Chittoor, Andhra Pradesh-517217

Abstract— In the rapidly evolving realm of the Industrial Internet of Things (IIoT), securing shop floor operations, especially in audit processes, is of critical importance. This paper confronts the challenge of ensuring data integrity and trust in IIoT systems by leveraging the capabilities of blockchain technology. The unique characteristics of blockchain, such as its immutable and decentralized ledger, establish a solid and transparent foundation for verifying shop floor transactions and activities. We introduce a privacycentric approach, meticulously designed to comply with stringent data privacy regulations. This method allows auditors to authenticate both IIoT data and devices, ensuring confidentiality and adhering to regulatory standards. Our practical implementation strategy, tailored for shop floor environments, not only
enhances the security of device and data integrity but also showcases robustness against specific adversarial threats, including network intrusion, data tampering, and unauthorized access. The findings indicate that our approach not only strengthens security protocols but also integrates effortlessly with existing IIoT infrastructures. It presents an efficient, scalable solution that elevates the safety and reliability of IIoT ecosystems, making it a significant step forward in the quest for secure and compliant industrial operations.

I. INTRODUCTION

The manufacturing sector is undergoing a transformative evolution, propelled by Industry 4.0, which ushers in an era of intelligent, data-driven production. This paradigm shift, characterized by the integration of Big Data analytics across the product lifecycle - from production to distribution, and after-sales support to retail - is reshaping how products are conceived, produced, and delivered. Such integration significantly impacts the industry, revolutionizing traditional manufacturing processes. The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio . However, this transition towards intelligent manufacturing brings forth significant challenges. A notable issue is the fragmentation of data within the manufacturing industry, as identified by Yu et al. This fragmentation acts as a barrier, impeding the efficient aggregation and analysis of vast data volumes, which is crucial for harnessing the full potential of Industry 4.0. Addressing this data fragmentation is key to enhancing the effectiveness and efficiency of production processes. At the heart of this transformation is the shop floor, where raw materials are converted into finished goods. Here, the need for efficient coordination and real-time information sharing is more pronounced than ever. Any lapse in data VOLUME 12, 2024 26747 IEEE Transaction Access on Blockchain,Volume:12,Issue Date:23.February.2024 management or tracking can lead to significant operational disruptions, ultimately impacting the competitiveness of industrial entities . In response to these challenges, blockchain technology emerges as a viable solution, offering a decentralized, transparent, and secure method for managing and tracking information on the shop floor. This study explores the development and application of a blockchain solution tailored to the specific needs of shop floor operations within the context of Industry 4.0. Our research is novel in its approach and contribution to the IIoT field, particularly in the following aspects:

1) We develop a unique blockchain-based framework specifically designed for the IIoT environment. This framework enhances data integrity and auditability on the shop floor, offering a more refined and practical solution compared to existing models.
2) We introduce a privacy-preserving verification process that allows auditors to authenticate IIoT data and devices without compromising sensitive information. This approach is aligned with current data privacy regulations, addressing a critical gap in existing research.

3) We provide empirical validation of our framework through real-world testing, demonstrating its effectiveness in improving operational efficiency and data security. This practical application distinguishes our study from others that primarily focus on theoretical aspects. These contributions represent significant advancements in the application of blockchain technology within the IIoT domain, especially in enhancing secure and efficient audit processes on the shop floor. The structure of the paper is organized as follows: Section II reviews related research in the field of industrial blockchain, emphasizing recent developments and advancements. Section IV provides background information on attribute-based authentication and industrial blockchain. Our proposed architecture is detailed in Section V, and an analysis of this architecture is presented in Section VI. In Section VII, we bring a practical use case to illustrate the application of our proposal. Finally, Section VIII concludes the paper

1. RELATED WORK

The paper titled "Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture" was authored by Fatemeh Ghovanlooy Ghajar,
Author ;- Mohammed B. M. Kamel, Christoph Reich, Fabrice Theoleyre, and Peter Ligeti.
It was published publication ;-in February 2024 in the journal *IEEE Access*
Description ;- This research addresses the critical need for securing shop floor operations within the Industrial Internet of Things (IIoT) by leveraging blockchain technology. The authors propose a privacy-centric approach that ensures data integrity and trust in IIoT systems. Their method allows auditors to authenticate both IIoT data and devices, maintaining confidentiality and adhering to stringent data privacy regulations. The practical implementation strategy is tailored for shop floor environments, enhancing security against adversarial threats such as network intrusion, data tampering, and unauthorized access. The findings indicate that this approach integrates seamlessly with existing IIoT infrastructures, offering an efficient and scalable solution to elevate the safety and reliability of IIoT ecosystems.

The paper titled "Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture"
Author ;- authored by Fatemeh Ghovanlooy Ghajar, Mohammed B. M. Kamel, Christoph Reich, Fabrice Theoleyre, and Peter Ligeti.
Publication;- It was published in February 2024 in the journal *IEEE*
Description:
This research addresses the critical need for securing shop floor operations within the Industrial Internet of Things (IIoT), particularly focusing on audit processes. The authors propose a privacy-centric approach that leverages blockchain technology to ensure data integrity and trust. By utilizing blockchain's immutable and decentralized ledger, the architecture provides a transparent and tamper-resistant platform for recording and verifying shop floor transactions and activities.

The proposed system allows auditors to authenticate both IIoT data and devices, ensuring confidentiality and compliance with stringent data privacy regulations. The implementation strategy is tailored for shop floor environments, enhancing security against adversarial threats such as network intrusion, data tampering, and unauthorized access. The findings indicate that this approach not only strengthens security protocols but also integrates seamlessly with existing IIoT infrastructures, offering an efficient and scalable solution to improve the safety and reliability of IIoT ecosystems.

The paper titled "Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture" was authored by
Author ;- Fatemeh Stodt, Mohammed B. M. Kamel, Christoph Reich, Fabrice Theoleyre, and Peter Ligeti.
Publication;- It was published in February 2024 in the journal *IEEE Acce*
Description:
This research addresses the critical need for securing shop floor operations within the Industrial Internet of Things (IIoT), particularly focusing on audit processes. The authors propose a privacy-centric approach that leverages blockchain technology to ensure data integrity and trust. By utilizing blockchain's immutable and decentralized ledger, the architecture provides a transparent and tamper-resistant platform for recording and verifying shop floor transactions and activities.

The proposed system allows auditors to authenticate both IIoT data and devices, ensuring confidentiality and compliance with stringent data privacy

regulations. The implementation strategy is tailored for shop floor environments, enhancing security against adversarial threats such as network intrusion, data tampering, and unauthorized access. The findings indicate that this approach not only strengthens security protocols but also integrates seamlessly with existing IIoT infrastructures, offering an efficient and scalable solution to improve the safety and reliability of IIoT ecosystems.

The paper titled "Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture" was authored by Fatemeh Stodt,
Author ;-Mohammed B. M. Kamel, Christoph Reich, Fabrice Theoleyre, and Peter Ligeti.
Publication;- It was published in February 2024 in the journal *IEEE Access*, Volume 12, pages 26747–26758.
Description:
This research addresses the critical need for securing shop floor operations within the Industrial Internet of Things (IIoT), particularly concerning auditing processes. The authors propose a blockchain-based architecture that ensures data integrity and trustworthiness in IIoT systems. By leveraging blockchain's immutable and decentralized ledger, the proposed framework provides a transparent and tamper-resistant platform for recording and verifying transactions and events on the shop floor. A key feature of this architecture is its privacy-preserving approach, allowing auditors to verify stored data and IIoT devices without compromising sensitive information. The study demonstrates that this framework can be effectively implemented in shop floor environments, offering a secure solution for auditing both devices and the data generated by IIoT devices. Additionally, the architecture is designed to withstand various adversarial attacks, enhancing the overall security and reliability of IIoT ecosystems.

2. RESEARCH METHODOLOGY

2.1. PROBLEM DEFINITION

The architecture proposed in this study is designed to integrate blockchain technology within heterogeneous network environments of IIoT, focusing on operational speed, transparency, legal liability, accountability, and privacy. The architecture adopts a hierarchical approach, as depicted in Fig. 2, and introduces ‘‘middle nodes’’ to interconnect subnetworks isolated by VLANs. These nodes are pivotal for executing computational tasks and maintaining network efficiency.
Module Split-Up:
User and Access Management

- Step 1;-Key Functions:
    - User authentication (e.g., through biometric, password, or smart card-based methods)
    - Role and permission assignment
    - Secure login/logout processes

Step;-2. Data Collection & Integration

- Key Functions:
    - Sensor data collection from machines, sensors, and devices
    - Integration with enterprise resource planning (ERP) or manufacturing execution systems (MES)
    - Formatting and pre-processing data for blockchain compatibility

3. step;-3 Data Encryption & Privacy-Preserving Mechanisms

- Key Functions:
    - Data encryption (e.g., using asymmetric encryption for data confidentiality)
    - Data anonymization techniques to obscure identities or sensitive production details
    - Use of zero-knowledge proofs (ZKPs) or homomorphic encryption to verify data without revealing sensitive information.

Step 4-
4. Blockchain Network and Consensus

- Key Functions:
    - Blockchain architecture design (e.g., private or consortium blockchain)
    - Consensus mechanism (e.g., PoW, PoS, or others depending on the system)
    - Block validation and verification
    - Timestamping and data immutability to prevent tampering

Step 5
Audit Trail Generation and Management

- Description: This module logs all the transactions and interactions on the shop floor and generates audit trails that can be reviewed and analyzed later. The audit trail

provides a transparent and immutable record of all activities on the shop floor.

- Key Functions:
  - Generation of auditable records for all actions, from data collection to access requests
  - Immutability and timestamping of data logs
  - Real-time or periodic audit reporting
  - Audit trail search, filtering, and query functionalities

Step 6. Smart Contract Implementation

- Description: Smart contracts are automated scripts stored on the blockchain that execute certain actions when specific conditions are met (e.g., trigger an audit event when certain thresholds are reached). This module automates and enforces compliance rules.
- Key Functions:
  - Automatic execution of predefined tasks based on shop floor events (e.g., production count, defect rate, machine uptime)
  - Conditional logic to execute audits when required
  - Smart contract auditing to ensure compliance with regulations
  - Alerts and notifications when smart contract conditions are met

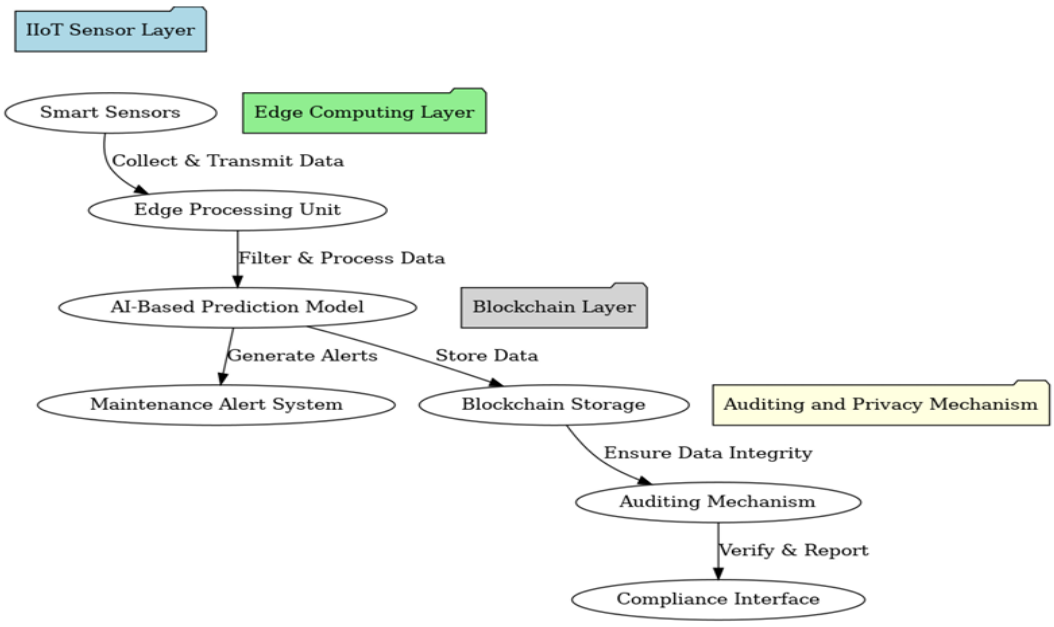
Step 7. Privacy-Preserving Auditing and Reporting

- Description: Ensures that audit information is available to authorized parties but remains private or masked for other parties. This module might include advanced reporting tools that aggregate and present data in a way that respects privacy requirements.
- Key Functions:
  - Permissioned access to audit reports
  - Anonymized or encrypted audit information for public or external sharing
  - Generation of compliance and regulatory reports
  - Secure and private sharing of audit data with external regulators or stakeholders

Step 8. Data Analytics & Insights

- Description: This module uses the data stored on the blockchain to generate insights about shop floor operations. It may use machine learning, AI, or data mining techniques to detect inefficiencies, predict failures, or optimize operations.
- Key Functions:
  - Data analysis and trend detection (e.g., performance metrics, defect rates)
  - Predictive analytics (e.g., maintenance needs, quality issues)
  - Reporting and visualization of actionable insights
  - Integration with existing business intelligence tools

3. ARCHITECTURE DESIGN:



Headings with Explanation Based on the Diagram

1. IIoT Sensor Layer
   - Smart Sensors: Devices responsible for collecting and transmitting real-time industrial data from equipment and shop floor processes.
   - Data Collection: Sensors monitor key parameters like temperature, pressure, and equipment status to enable predictive analysis.
2. Edge Computing Layer
   - Edge Processing Unit: Filters and processes sensor data closer to its source to reduce latency and bandwidth usage.
   - Local Processing: Preliminary data refinement occurs before transmission to higher layers for deeper analysis.
4. AI-Based Prediction Model
   - Generate Alerts: AI algorithms analyze processed data to detect anomalies and predict maintenance needs.

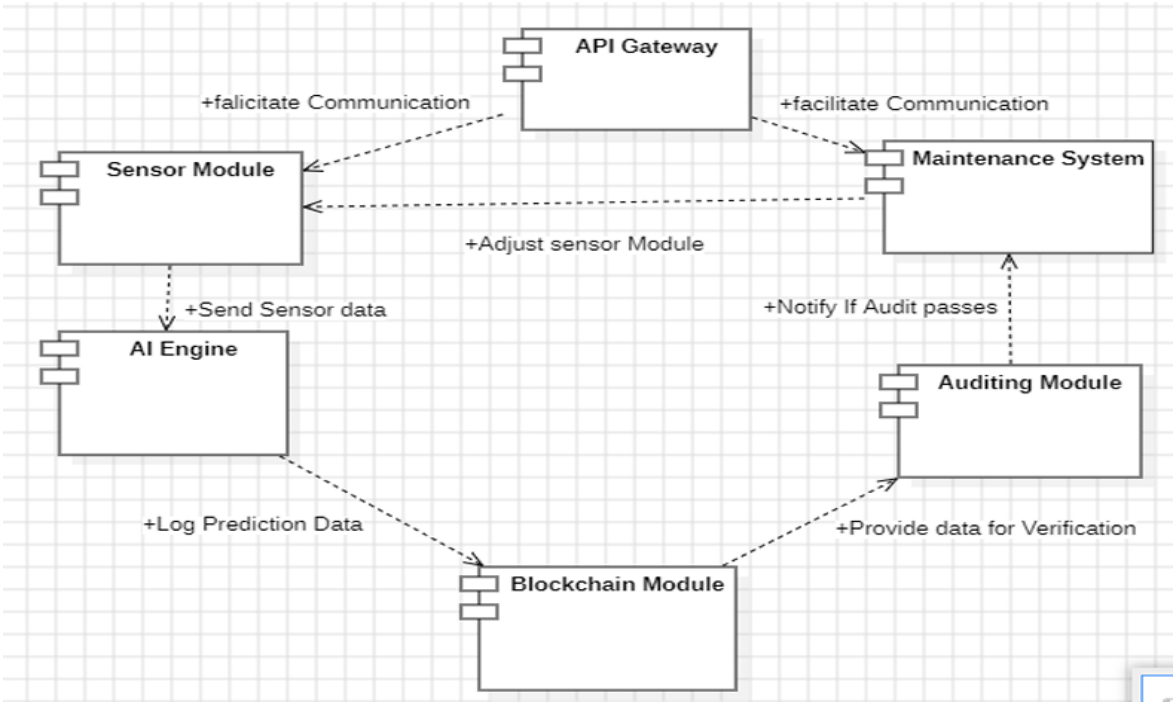
Structured Points Based on the Diagrams

1. Sensor Data Collection & Processing
   - IIoT Sensor Node collects real-time industrial data (sensorID, timeStamp, value).
   - Middle Node validates and processes the received sensor data.
   - If valid, data is forwarded for AI-based predictions; otherwise, it is discarded.
2. AI-Based Predictive Maintenance
   - AI Model analyzes validated sensor data using defined algorithms (modelID, algorithm, trainingData).
   - AI Model analyzes validated sensor data using defined algorithms (modelID, algorithm, trainingData).
   - Failure Prediction: AI detects potential faults based on historical patterns.
   - Predictive Maintenance System schedules proactive actions based on AI-generated recommendations.
3. Blockchain-Based Secure Record Keeping
   - Blockchain Ledger stores prediction results and maintenance decisions (transactionID, dataHash, timeStamp).
   - Tamper-Proof Storage ensures secure and immutable records.
   - Verification Process ensures auditability and compliance with regulatory standards.
5. Auditor Verification & Maintenance Execution
   - Auditor Node verifies blockchain-stored records for accuracy (auditorID, verificationLogs).
   - Audit-Based Maintenance Execution: Only verified AI predictions trigger maintenance actions.
   - Final Maintenance Actions ensure equipment reliability and operational efficiency.
6. Workflow Execution for Secure Predictive Maintenance
   - Sensors collect real-time data → Middle Node validates → AI Model predicts failures.
   - Blockchain stores predictions → Auditor verifies accuracy → Maintenance system executes actions.

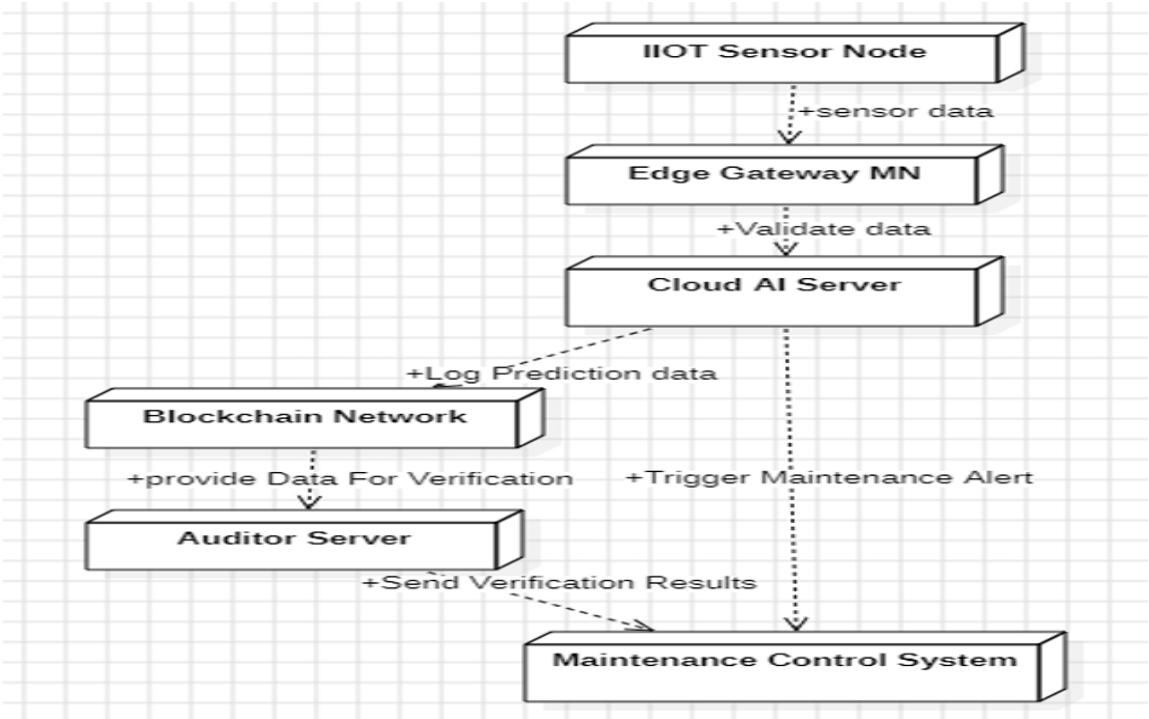
Structured Points Based on the Diagrams

1. Sensor Data Collection & Processing
   - IIoT Sensor Node collects real-time sensor data (sensorID, timeStamp, value) from industrial equipment.
   - Middle Node validates and processes the received data before forwarding it.
   - Decision Point: If the data is valid, it proceeds to AI model analysis; otherwise, it gets discarded.
2. AI-Based Predictive Maintenance
   - AI Model processes validated sensor data using predictive algorithms (modelID, algorithm, trainingData).
   - Failure Prediction: AI analyzes patterns to detect potential faults early.
   - Recommendations for Maintenance: AI suggests proactive maintenance measures based on predictions.
3. Blockchain Integration for Secure Record Keeping
   - Blockchain Ledger stores validated sensor data and AI predictions (transactionID, dataHash, timeStamp).
   - Tamper-Proof Data Storage: Ensures integrity and prevents unauthorized modifications.
   - Verification Process: Blockchain records are reviewed for compliance.

Component Diagram:



Deployment Diagram:



Structured Points Based on the Diagrams

1. Sensor Data Collection & Processing

- IIoT Sensor Node collects real-time industrial data (sensorID, timeStamp, value).
- Middle Node validates and processes the received sensor data.
- If valid, data is forwarded for AI-based predictions; otherwise, it is discarded.

2. AI-Based Predictive Maintenance

- AI Model analyzes validated sensor data using defined algorithms (modelID, algorithm, trainingData).
- AI Model analyzes validated sensor data using defined algorithms (modelID, algorithm, trainingData).

- Failure Prediction: AI detects potential faults based on historical patterns.
- Predictive Maintenance System schedules proactive actions based on AI-generated recommendations.

3. Blockchain-Based Secure Record Keeping
- Blockchain Ledger stores prediction results and maintenance decisions (transactionID, dataHash, timeStamp).
- Tamper-Proof Storage ensures secure and immutable records.
- Verification Process ensures auditability and compliance with regulatory standards.

4. Auditor Verification & Maintenance Execution
- Auditor Node verifies blockchain-stored records for accuracy (auditorID, verificationLogs).
- Audit-Based Maintenance Execution: Only verified AI predictions trigger maintenance actions.
- Final Maintenance Actions ensure equipment reliability and operational efficiency.

5. Workflow Execution for Secure Predictive Maintenance
- Sensors collect real-time data → Middle Node validates → AI Model predicts failures.
- Blockchain stores predictions → Auditor verifies accuracy → Maintenance system executes actions.

Algorithm And Techniques
Algorithms
1. Attribute Verification Protocol:
- Validates IIoT devices based on their attributes using privacy-preserving methods.

2. Practical Byzantine Fault Tolerance (PBFT):
- Ensures consensus and secure transaction validation across the blockchain network.

3. Cryptographic Hashing (SHA-1):
- Generates unique hashes for data and attributes, ensuring integrity and security.

Techniques
1. Privacy Preservation:
- Protects sensitive shop floor data through encryption and zero-knowledge validation.

2. Hierarchical Node Network:
- Local, Middle, and Full nodes optimize data collection, storage, and consensus processes.

3. Immutable Blockchain Records:
- Provides secure and tamper-proof audit trails for shop floor operations.

Datasets: DataSets and Inputs:

1. IIoT Device Data: Sensor readings (e.g., temperature, pressure), actuator logs, device IDs.
2. Blockchain Records: Hashes of transactions, audit logs, and blocks.
3. Attributes: Logical network sectors, installer signatures, power consumption, transmission patterns.
4. Operational Metrics: Performance reports, energy usage, and fault logs.
Inputs:
1. Node Identifiers: Unique IDs derived from MAC addresses and serial numbers.
2. Sensor Data: Real-time shop floor readings.
3. Attribute Tokens: Tokens issued after device verification.
4. Validation Challenges: Data integrity checks from middle and full nodes.

Expected Outcomes:
1. Enhanced Security: Immutable blockchain records prevent tampering and unauthorized access.
2. Privacy Preservation: Attribute verification protocol ensures confidentiality of IIoT data.
3. Operational Efficiency: Real-time data tracking optimizes shop floor processes and predictive maintenance.
4. Scalability: Architecture integrates seamlessly with diverse IIoT environments and scales efficiently.
5. Compliance: Aligns with stringent data privacy regulations, meeting legal and industrial standards.

REFERENCES

[1] X. Yao and Y. Lin, ‘‘Emerging manufacturing paradigm shifts for the incoming industrial revolution,’’ Int. J. Adv. Manuf. Technol., vol. 85, nos. 5–8, pp. 1665–1676, Jul. 2016.
[2] T. Zheng, M. Ardolino, A. Bacchetti, and M. Perona, ‘‘The applications of industry 4.0 technologies in manufacturing context: A systematic literature review,’’ Int. J. Prod. Res., vol. 59, no. 6, pp. 1922–1954, Mar. 2021.
[3] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, ‘‘IoTChain: Establishing trust in the

Internet of Things ecosystem using blockchain,'' IEEE Cloud Comput., vol. 5, no. 4, pp. 12–23, Aug. 2018.

[4] G. Culot, G. Orzes, M. Sartor, and G. Nassimbeni, ''The future of manufacturing: A delphi-based scenario analysis on Industry 4.0,'' Technol. Forecasting Social Change, vol. 157, Aug. 2020, Art. no. 120092.

[5] T. Pulikottil, L. A. Estrada-Jimenez, J. J. P. Abadía, A. Carrera-Rivera, A. Torayev, H. U. Rehman, F. Mo, S. Nikghadam-Hojjati, and J. Barata, ''Big data life cycle in shop-floor–trends and challenges,'' IEEE Access, vol. 11, pp. 30008–30026, 2023.

[6] A. Vatankhah Barenji, Z. Li, and W. M. Wang, ''Blockchain cloud manufacturing: Shop floor and machine level,'' in Proc. Eur. Conf. Smart Objects, Syst. Technol., Jun. 2018, pp. 1–6.

[7] A. Bahga, ''Blockchain platform for industrial Internet of Things,'' J. Softw. Eng. Appl., vol. 9, no. 10, pp. 533–546, Oct. 2016.

[8] J. Stodt, D. Schönle, C. Reich, F. Ghovanlooy Ghajar, D. Welte, and A. Sikora, ''Security audit of a blockchain-based industrial application platform,'' Algorithms, vol. 14, no. 4, p. 121, Apr. 2021.

[9] D. Mishra, P. Singh, and N. Singh, ''Role of blockchain in achieving solutions in ambiguous supply chain operations,'' in Blockchain VolatileUncertain-Complex Ambiguous World. Amsterdam, The Netherlands: Elsevier, 2023, pp. 57–73.