

BMTIIOT: Blockchain-based Multi-Technology Integrated Industrial Internet of Things Data Acquisition and Control Platform

Jinhan Ma¹, Guofeng Zhang¹, Yajie Pang¹, Wenxue Yang¹, Hongbo Wang¹, Hanxiao Yu¹, Junjie Lin¹
{m13595761288@163.com¹, zhangguofeng@tsu.edu.cn¹, 1228171562@qq.com¹}
{19323072830@163.com¹, 3314616612@qq.com¹, 3479289422@qq.com¹, 19959530197@163.com¹}
School of Information Science and Technology, Taishan University, Taian, China¹

Abstract. In order to cope with the challenges of data island, foreign technology card neck and lack of data traceability existing in the traditional Industrial Internet of Things (IIoT) data acquisition and control platform, this study designs and implements a Blockchain-based Multi-Technology Integrated Industrial Internet of Things Data Acquisition and Control Platform (BMTIIOT). The platform uses a four-layer architecture: edge data collection, blockchain and cloud database storage, cloud data processing and intelligent identification, and industrial scene interaction. It integrates core technologies such as Bluetooth beacons, intelligent robotic arms, and Yolo visual recognition to fully meet the data acquisition requirements in the industrial production process. It uses hybrid encryption mechanism, combined with SM4 algorithm and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm to ensure the security of data transmission and storage. It constructs a cloud storage mechanism of on chain and off chain collaboration, and realizes tamper proof data integrity and whole process traceability. Experimental results demonstrate that the IIoT data acquisition platform achieves 99.5% mAP@50 and 97.08% mAP@50-95 in energy label detection, a 95% command recognition rate for robotic arms, a 99% voice wake-up response rate, ≤ 1.5 s label printing response, and over 99% reduction in on-chain data storage. These capabilities effectively meet the demand for trusted data support in IIoT.

Keywords: Blockchain, IIoT, Multi-technology Integrated, Data Acquisition.

1 Introduction

1.1 Research Background

With the implementation of artificial intelligent, industrial intelligence has become the core direction of manufacturing transformation. IIoT is reshaping existing industries into data-driven intelligent sectors. However, inherent characteristics of IIoT have led to challenges such as fragmentation, poor interoperability, privacy breaches, and security vulnerabilities. Blockchain technology presents opportunities to address these IIoT challenges [1]. As the core infrastructure of

smart manufacturing, the IIoT Data Acquisition and Control Platform handles multi-dimensional data collection, transmission, and processing tasks including equipment status, product quality, and personnel management during production. However, existing platforms still face three major pain points: First, insufficient data credibility, where production data is easily tampered with during collection and transmission, making quality traceability and liability determination difficult; Second, multi-technology coordination barriers, where technologies like Bluetooth communication, AI recognition, and robotic arm control operate in silos, hindering production efficiency improvements; Third, incomplete security protection systems, where security vulnerabilities continue to increase and threats accelerate penetration, posing serious safety risks to industrial production, operations, and management processes [2].

Blockchain technology, with its characteristics of decentralization, tamper resistance and transparent traceability, provides a new idea for solving the credibility problem of industrial data [3]. Combining blockchain with IIOT[4] and Artificial Intelligence (AI) can build a safe and reliable industrial data ecosystem. However, direct chained storage of massive industrial data will bring excessive storage burden, and a single encryption scheme is difficult to balance data security and access flexibility [5]. Therefore, it has become a key challenge to promote the intelligent transformation and upgrading of IIoT to achieve efficient data collection through multi technology integration, and to design encryption mechanism and collaborative storage strategy to ensure data security and credibility.

1.2 Motivation and Contributions

This paper designs a multi-technology integrated IIoT data acquisition and control platform based on blockchain and cryptography, which realizes the whole process of industrial data collection-encryption-storage-traceability trusted management. The main contributions are as follows:

The four-layer architecture of edge collection, blockchain evidence storage, cloud processing and industrial scene interaction” is proposed, which integrates technologies such as Bluetooth beacon, visual energy efficiency label recognition, intelligent robotic arm dual-mode control, warehouse management and label printing, and supports the core production scenarios of IIoT.

The hybrid encryption scheme is designed based on SM4 and CP-ABE algorithm, which can achieve fine-grained access control of key while balancing data security and authorization flexibility.

The system establishes a collaborative storage mechanism of on chain and off chain cloud, only records the hash value and index information of energy efficiency identification data on the chain, and encrypted original images are stored in the IPFS distributed file system. This scheme not only ensures data integrity, but also reduces the storage burden of blockchain.

Develop a digital large-screen visualization system to enable real-time industrial data display, anomaly alerts, and full-process traceability, thereby enhancing production management efficiency.

2 Related Works

Research on industrial data acquisition and trusted management has achieved significant progress. While Research [6] advances remote communication between sensors and industrial controllers, it does not address trusted data transmission. Research [7] proposes a multi-sensor fusion-based condition monitoring system for electromechanical equipment, which integrates data from multiple sensors to achieve comprehensive and accurate monitoring. By leveraging IoT technology, the system ensures real-time data transmission and efficient processing, though it lacks a trusted data storage mechanism. Reference [8] presents an IIoT-based data acquisition architecture and application framework, applicable to remote monitoring and intelligent maintenance of various industrial equipment and smart products. However, it fails to achieve cross-system data coordination and traceability.

The application of blockchain technology in the industrial field is becoming more and more mature. Research [9] describes the advantages and challenges of using blockchain and smart contracts in the development of industry 4.0. Research [10] proposed an IIOT blockchain consensus mechanism based on trust mechanism, and set up a data access control framework to regulate the access rights of sensitive data. Research [11] designed a blockchain driven industrial Internet platform using distributed data storage and terminal authentication technology to improve platform security by ensuring data integrity and availability. However, this scheme ignores the requirement of efficient multi technology integration in the process of data acquisition.

The existing researches have not fully solved the problems of multi-technology acquisition, encryption mechanism optimization and collaborative storage. This paper integrates multi-technology acquisition module, designs hybrid encryption mechanism and collaborative storage strategy, and constructs a whole-process trusted IIoT data acquisition control platform to make up for the deficiencies of the existing researches.

3 System Design

3.1 System Architecture Design

The platform adopts a four-layer architecture: Industrial Scenario Interaction Layer, IIoT Platform Layer, On-chain and Off-chain Collaboration Layer, and IIoT Perception Layer, as shown in Figure 1.

1.Industrial Scenario Interaction Layer: This layer provides an interactive interface through industrial equipments (industrial rugged tablets, etc.) and digital dashboard. It supports equipment control and production data visualization, and realizes the seamless cooperation of multiple terminals in the industrial environment.

2.IIoT Platform Layer: As the core hub, this layer is responsible for handling the requests of the industrial scenario interaction layer and coordinating the IIoT perception layer. Its core functions include cloud data processing (for real-time data processing of visual modules), device data integration (intelligent manipulator, Bluetooth beacon, etc.), intelligent contract interaction (support for blockchain based evidence storage) and hybrid encryption technology (using SM4+CP-ABE to

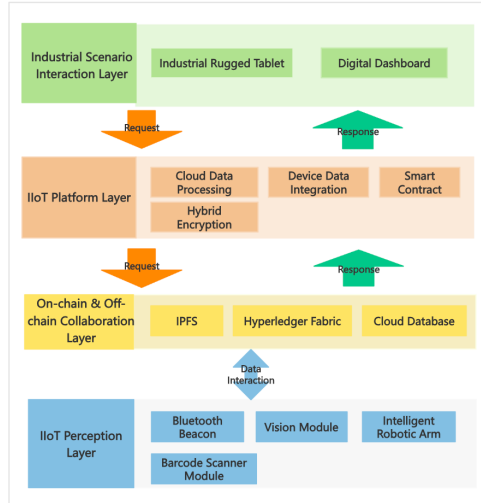


Fig. 1. System Architecture.

achieve data security). This layer ensures cross module collaboration and business process coordination.

3.On-chain and Off-chain Collaboration Layer: This layer adopts a collaborative storage architecture combining Hyperledger Fabric, IPFS, and cloud databases. The blockchain stores the hash values and index information of energy efficiency identification data, ensuring tamper-proof integrity of the data; IPFS stores encrypted original images, enabling distributed backup; and the cloud database stores structured business data, supporting efficient queries.

4.IIoT Perception Layer: This layer integrates Bluetooth beacons, YOLO vision modules, smart robotic arms, barcode scanner modules, and other IIoT devices. It enables multi-dimensional industrial data sensing—including personnel identity verification, product energy efficiency labeling detection, equipment status monitoring, and material barcode recognition—providing comprehensive data input for the Platform Layer across all operational scenarios.

Through systematic innovations in the four aspects mentioned above, this paper addresses the core challenges in industrial scenarios—such as low data credibility, difficulties in technology integration, and incomplete security mechanisms—and has provided a complete solution for IIoT data acquisition and control that combines theoretical significance with engineering feasibility.

3.2 System Function Design

The platform comprises six core functional modules, as illustrated in Figure 2.

1. Data acquisition module: includes the following five modules:

(1) Bluetooth beacon personnel identification: The device periodically scans the target UUID device at an interval of 500 milliseconds to realize the rapid identification of visitors/employees, and

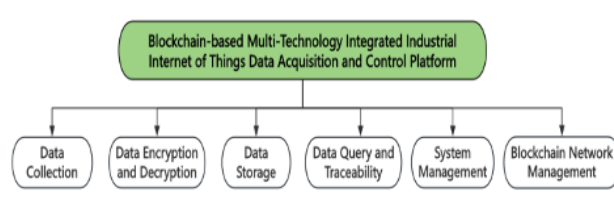


Fig. 2. Functional Structure of the System.

refresh the number of visitors on the data dashboard.

(2) YOLOv8 Energy Efficiency Label Recognition: By uploading the pictures collected by the visual module to the cloud for recognition, combined with Tencent cloud server and YOLOv8 model, multi label recognition from level 1 to level 5 energy efficiency levels is realized.

(3) Dual-mode control for intelligent robotic arm: The system uses STM32F103C8T6 as the main controller, with HC-05 Bluetooth module and LD3320 voice chip. It supports both native commands (#001P1500T1000!) and voice commands (using the wake-up word "Xiaoshan").

(4) Web label printing: Generate CODE128 barcodes with JsBarcode, supporting manual or automatic printing.

(5) Smart product inventory management: Using the Python pyzbar library to decode barcode information, it efficiently extracts key data like product types and timestamps.

2. Data encryption and decryption module: Generate dynamic SM4 key to encrypt sensitive information, such as energy efficiency identification images. The CP-ABE scheme is used to encrypt the dynamic SM4 secret key, and the access policy is designed according to the user attributes (administrator, operator, visitor). Only users with matching attributes can decrypt data.

3. Data Storage Module: Structured business data is stored in cloud database. The encrypted sensitive information such as energy efficiency identification images is stored in IPFS and indexed. The index information, data hash value and access strategy of energy efficiency identification data are then recorded in the Hyperledger Fabric. Synchronization mechanism ensures data consistency between cloud database and blockchain.

4. Data Query and Trace Module: Supports multi-condition queries based on product ID and time range. Authorized users can decrypt data credentials and keys through attribute verification to access raw data. It provides full-process data traceability, displaying key information such as collection devices, processing nodes, and storage time.

5. System Management Module: Provides device management, user permission configuration, and certificate management. It supports device status monitoring and user attribute adjustment to ensure stable platform operation.

6. Blockchain Network Management Module: Built on Hyperledger Fabric, this private blockchain network handles node management, smart contract deployment, and transaction monitoring, while supporting multi-node consensus and data synchronization.

3.3 Data Design

Core business data, including personnel management, product quality inspection, equipment control, and blockchain evidence data, is stored in JSON format. The core data structure is as follows:

- (1) Personnel management data: {visitor ID, group ID, device SN, personnel type, collection time}.
- (2) Product quality inspection data: {product ID, group ID, inspection device, energy efficiency rating, encrypted hash}.
- (3) Device control data: {device ID, group ID, control command, running status, device fault status, operation time}.
- (4) Blockchain evidence data: {transaction ID, data hash value, IPFS index, block number, blockchain timestamp}.

3.4 Business Process Design

The platform's core business process implements a closed-loop data cycle of collection-encryption-storage-query-traceability, with the following steps:

- (1) System initialization: Deploy the Hyperledger Fabric network and initialize smart contract parameters and encryption algorithms.
- (2) Data collection: Industrial data is gathered through Bluetooth beacons, vision modules, robotic arms, and rugged industrial tablets, then transmitted to the business logic layer.
- (3) Hybrid encryption: SM4 encrypts sensitive data, while CP-ABE encrypts the SM4 key.
- (4) Collaborative storage: Structured business data is stored in a cloud database, while encrypted sensitive data is stored on IPFS. Indexes and hash values are recorded on the blockchain and synchronized with the cloud database.
- (5) Authorized query: The system decrypts and returns data after verifying the attributes of the query request submitted by the user.
- (6) Full-process traceability: The digital dashboard displays complete data chain information and supports tracing abnormal data.

The business process flowchart is shown in Figure 3.

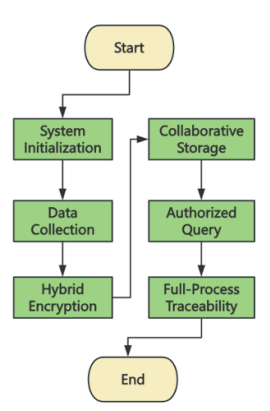


Fig. 3. Business Process Flowchart.

4 System Implementation

4.1 Development Environment

The development environment, including the hardware environment and software environment, is shown in Table 1.

4.2 Implementation of Core Functions

Multi-technology integrated data collection function: The Bluetooth beacon module identifies personnel through UUID filtering, supports dual-role statistics for visitors/staff, and enables real-time updates on the digital dashboard. As shown in Figure 4.

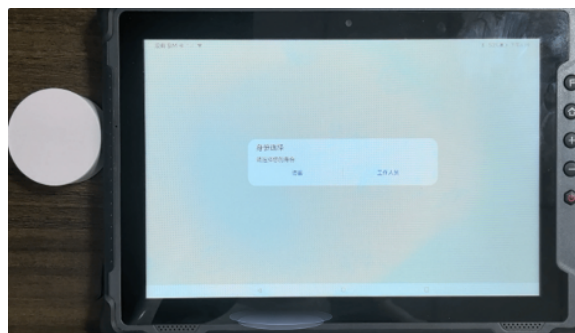


Fig. 4. Bluetooth Visitor Management.

The YOLOv8 module can recognize energy efficiency labels. The visual module collects im-

Table 1: Development Environment

Category	Components & Specifications
Hardware Environment	Industrial rugged tablet: OpenHarmony 4.0 Intelligent robotic arm: STM32F103C8T6 controller YOLOv8 vision module: OpenMV4 H7 Plus Server: Ubuntu22.04-Docker26-LF22 (2 cores, 2GB memory, 40GB SSD cloud disk) Peripherals: Bluetooth beacon, DP30 barcode printer, digital screen
Software Environment	Operating systems: Ubuntu 22.04, Windows 10, OpenHarmony 4.0 Blockchain platform: Hyperledger Fabric 2.5 Development frameworks: Flask 2.3.3, Spring Boot 2.7.0, Vue 3 Algorithm libraries: ultralytics 8.0.196 (YOLOv8), OpenCV 4.8.1, SM4/CP-ABE encryption libraries

ages of energy efficiency labels and sends them to the cloud for detection. The encrypted original images are stored on IPFS, while the index information is stored on the blockchain. As shown in Figure 5.

The key parameters, dataset details, and performance metrics of YOLOv8 are presented in Table II. This table comprehensively presents the experimental configuration and performance of the YOLOv8n model used in industrial energy label detection. Trained on a dataset of 231 images over 150 epochs, the model achieves a precision of 99.77%, with energy label detection mAP@50 at 99.5% and mAP@50-95 at 97.08%, demonstrating its high accuracy and strong robustness in industrial scenarios.

Equipped with an external BT04 BLE module and ASRPRO voice board on the original STM32F103, the intelligent robotic arm supports dual-mode control via Bluetooth and voice. As shown in Figure 6.

Intelligent inventory management product output and inventory information, real-time printing of product barcodes. As shown in Figure 7.

Blockchain-based data storage and retrieval: Deploy smart contracts for data storage to achieve on-chain storage of data hash values and IPFS indexes. During queries, user attributes are verified, and the smart contract retrieves the index to download and decrypt the encrypted data from IPFS for display. As shown in Figure 8.

Visual traceability: The digital dashboard integrates data such as personnel entry statistics, product quality inspection pass rates, and equipment operation status, presented in charts. As shown in Fig 9.



Fig. 5. Energy efficiency label recognition.



Fig. 6. Dual-mode control of intelligent manipulator.

4.3 Test Scheme

The platform undergoes validation across three dimensions: functionality, security, and performance. Functionality testing verifies the integrity of core features including data collection, encryption, storage, querying, and traceability. Security testing simulates attacks such as data tampering and unauthorized access to assess the platform's protective capabilities. Performance testing evaluates response times for data collection, encryption processing duration, storage efficiency, and query latency.

Table 2: YOLOv8 Key Parameters, Dataset, and Performance Metrics

Category	Parameter / Metric	Value / Setting
Dataset Split	Total Samples	231 images
	Training Set	188 images
	Validation Set	43 images
Model Architecture	Model Version	YOLOv8n
	Training Epochs	150
Training Configuration	Batch Size	16
	Optimizer	SGD
	Input Image Size	640x640
Inference Configuration	Confidence Threshold	0.5
	IoU Threshold	0.7
Performance Metrics	Precision	0.9977
	mAP@50	0.995
	mAP@50-95	0.9708



Fig. 7. Real-time printing of product barcodes.

```
root@4481a9d697e5: /opt/gopath/src/github.com/hyperledger/fabric/peer
annel -n bntilo666 --peerAddresses peer0.org1.example.com:7051 --tlsRootCertFile
s /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/or
g1.example.com/peers/peer0.org1.example.com/tls/ca.crt --peerAddresses peer0.org
2.example.com:7051 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fab
ric/peer/crypto/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/
tls/ca.crt --peerAddresses peer0.org3.example.com:7051 --tlsRootCertFiles /opt/g
opath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org3.examp
le.com/peers/peer0.org3.example.com/tls/ca.crt -c '{"function": "InitLedger", "Arg
s": []}' --waitForEvent
2023-12-02 12:51:49.985 UTC 0001 INFO [chaincodeCmd] ClientWait -> txid [930bda6
0742ab5cd889333ef19b37b09ce8a28a28bc94e6c78121ed05521de6a] committed with status
(VVALID) at peer0.org3.example.com:7051
2023-12-02 12:51:49.986 UTC 0002 INFO [chaincodeCmd] ClientWait -> txid [930bda6
0742ab5cd889333ef19b37b09ce8a28a28bc94e6c78121ed05521de6a] committed with status
(VVALID) at peer0.org2.example.com:7051
2023-12-02 12:51:49.987 UTC 0003 INFO [chaincodeCmd] ClientWait -> txid [930bda6
0742ab5cd889333ef19b37b09ce8a28a28bc94e6c78121ed05521de6a] committed with status
(VVALID) at peer0.org1.example.com:7051
2023-12-02 12:51:49.988 UTC 0004 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> C
haincode invoke successful. result: status:200
```

Fig. 8. Smart Contracts on the Blockchain.



Fig. 9. Digital Screen Visualization.

5 Experimental Results and Analysis

5.1 Functional Test Results

The functional tests covered six core scenarios, with all features meeting design specifications: YOLOv8 achieves 99.5% mAP@50 and 97.08% mAP@50-95 in energy label detection, and label printing response process takes only 1.5 seconds. Visitor identification is completed within 5 seconds, with a complete and traceable data chain and smooth operation of the digital display.

5.2 Security Test Results

The platform resists data tampering attacks by preventing mismatched hash values between altered data and blockchain records. Unauthorized users cannot decrypt data due to attribute mismatches. Mechanisms like collision detection and current protection ensure secure device operations, meeting industrial safety standards.

5.3 Performance Test Results

The key performance test indicators are shown in Table 3.

Table 3: Test Results of Smart Contract and Data Functions

Test Specification	Actual Value	Design Goal	Completion Status
Energy label detection mAP@50	99.5%	$\geq 95\%$	reach
Energy label detection mAP@50-95	97.08%	$\geq 90\%$	reach
Robotic arm command recognition rate	95%	$\geq 95\%$	reach
Voice wake-up response rate for robotic arms	99%	$\geq 95\%$	reach
Label print response	1.5 s	≤ 2 s	reach
Visitor identification time	≤ 5 s	5 s	reach
Improved data storage efficiency	$> 99\%$	$\geq 90\%$	reach

The results show that the platform response time meets the industrial real-time requirements, the data storage efficiency is greatly improved compared with the traditional scheme, and the platform can support the trusted management of large-scale industrial data.

6 Conclusions and Prospects

This study presents a Blockchain-based Multi-Technology Integrated Industrial Internet of Things Data Acquisition and Control Platform. The platform effectively addresses the issues of data silos, foreign technology blockades, and the lack of full-process traceability in conventional IIoT systems. It adopts a four-layer architecture: edge data collection, blockchain and cloud database storage, cloud data processing and intelligent identification, and industrial scene interaction. The four-layer architecture integrates multi-technology acquisition modules, while hybrid encryption and collaborative storage strategies ensure end-to-end trusted management of industrial data. Experimental results demonstrate the platform's robust functionality and reliability, achieving 99.5% mAP@50, 97.08% mAP@50-95 in energy label detection, 95% robotic arm command recognition, 99% voice wake-up response rate, ≤ 1.5 s label printing response, and over 99% on-chain data reduction. These capabilities provide critical support for industrial intelligent transformation.

Future work will focus on three key optimization directions: deploying edge computing nodes to reduce cloud load; refining the CP-ABE algorithm for more flexible access control; and expanding device compatibility. In addition, further experimental evaluation will be conducted on critical issues such as the impact of blockchain scale growth on performance, IPFS access latency under high loads, and the complexity of CP-ABE attributes.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (62472252), the Taishan Scholars Program (tsqn202211280), the Quan Cheng Laboratory (QCL20250204), the Shandong Provincial Innovation Capacity Enhancement Project for Science and Technology SMEs (2023TSGC0588) and the Taian Municipal Science and Technology Program (2023NS106, 2022TPY034).

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

- [1] Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. *IEEE internet of things journal*. 2019;6(5):8076-94.
- [2] Hu Y, Jia Q, Yao Y, Lee Y, Lee M, Wang C, et al. Industrial internet of things intelligence empowering smart manufacturing: A literature review. *IEEE Internet of Things Journal*. 2024;11(11):19143-67.
- [3] Li R, Sun L. Network security threat detection model based on large-scale multi-source data analysis and perception fusion. *Neural Computing and Applications*. 2025:1-14.

- [4] Padma A, Ramaiah M. GLSBloT: GWO-based enhancement for lightweight scalable blockchain for IoT with trust based consensus. *Future Generation Computer Systems*. 2024;159:64-76.
- [5] Wang F, Cui J, Zhang Q, He D, Zhong H. Blockchain-based secure cross-domain data sharing for edge-assisted industrial internet of things. *IEEE Transactions on Information Forensics and Security*. 2024;19:3892-905.
- [6] Wijaya R, Radhy A, Mujiyanti SF. A Novel Lo-Ra Based Wireless Communication Module for Industrial Data Acquisition-Telemetry. *IEEE Access*. 2025.
- [7] Lin T, Ren Z, Zhu L, Zhu Y, Feng K, Ding W, et al. A Systematic Review of Multi-Sensor Information Fusion for Equipment Fault Diagnosis. *IEEE Transactions on Instrumentation and Measurement*. 2025.
- [8] Li X, Zhao H, Feng Y, Li J, Zhao Y, Wang X. Research on key technologies of high energy efficiency and low power consumption of new data acquisition equipment of power Internet of Things based on artificial intelligence. *International Journal of Thermofluids*. 2024;21:100575.
- [9] Chen Y, Lu Y, Bulysheva L, Kataev MY. Applications of blockchain in industry 4.0: A review. *Information Systems Frontiers*. 2024;26(5):1715-29.
- [10] Vasantha B, Bhavana K, Kavya K, Varshini M. Blockchain System with Credit-Based Consensus Mechanism for Industrial Internet of Things: An Application of Industry 4.0. *JETT*. 2024;15(5):250-64.
- [11] Sizan NS, Dey D, Layek MA, Uddin MA, Huh EN. Evaluating blockchain platforms for iot applications in industry 5.0: A comprehensive review. *Blockchain: Research and Applications*. 2025:100276.