TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/

INTEGRATION OF BLOCKCHAIN TECHNOLOGY FOR ENSURING DATA INTEGRITY IN MECHATRONIC NETWORKS

T. BUVANESWARI[1*], G. SUGANYA[2], CHANDRA MOHAN MANOHAR[3], P. GANESAN[4], MD JAVEED AHMED[5], RUBY PANT[6]

[1]PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNAPOORANA ENGINEERING COLLEGE (AUTONOMOUS), SALEM, 636308, TAMIL NADU, INDIA.
[2]ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNAPOORANA ENGINEERING COLLEGE (AUTONOMOUS), SALEM, 636308, TAMIL NADU, INDIA.
[3]ASSISTANT PROFESSOR, DEPARTMENT OF MECHATRONICS, BHARATH INSTITUTE OF HIGHER EDUCATION AND RESEARCH, CHENNAI, 600073, TAMIL NADU, INDIA.
[4]ASSOCIATE PROFESSOR, DEPARTMENT OF MECHANICAL ENGINEERING, DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING, COIMBATORE, 641105,TAMIL NADU, INDIA.
[5]DEPARTMENT OF MECHANICAL ENGINEERING, BS ABDUR RAHMAN CRESCENT INSTITUTE OF SCIENCE AND TECHNOLOGY, VANDALUR, CHENNAI, 600048, TAMIL NADU, INDIA.
[6]DEPARTMENT OF MECHANICAL ENGINEERING, UTTARANCHAL INSTITUTE OF TECHNOLOGY, UTTARANCHAL UNIVERSITY, UTTARAKHAND, 248007.

[*]Corresponding Author Email: buvanamuruga2008@gmail.com

Abstract
The increasing interconnection of mechatronic systems in modern industrial environments has amplified concerns regarding data integrity, cybersecurity, and trustworthiness. Traditional centralized architectures are prone to data tampering, unauthorized access, and single-point failures, which compromise the reliability of mechatronic operations. This study presents a blockchain-based decentralized framework designed to enhance data integrity and secure communication within mechatronic networks. The proposed architecture employs a permissioned blockchain integrated with smart contracts for real-time validation, authentication, and transaction recording across distributed nodes. Each data exchange is cryptographically verified and stored in an immutable ledger, ensuring transparency and traceability. Experimental validation was conducted using an IoT-enabled mechatronic test setup comprising sensor-actuator modules and embedded controllers connected through blockchain nodes. Performance metrics, including latency, throughput, and fault detection accuracy, were analyzed to assess the system's feasibility. Results indicate that blockchain integration significantly enhances data reliability and resilience against cyberattacks, with minimal communication overhead. The study demonstrates that blockchain technology provides a robust and scalable solution for achieving trustworthy data management in next-generation mechatronic systems, paving the way toward secure and intelligent Industry 5.0 applications.

Keywords: Blockchain technology; Mechatronic networks; Data integrity; Smart contracts; Cybersecurity; Decentralized systems; Industrial automation; IoT-enabled mechatronics; Data security; Industry 4.0; Distributed ledger technology (DLT).

1. INTRODUCTION

The convergence of mechanical, electronic, and computational technologies has led to the evolution of mechatronic systems, which form the backbone of modern automation, robotics, and intelligent manufacturing. These systems integrate sensors, actuators, controllers, and communication networks to perform complex tasks with high precision and efficiency. With the rise of Industry 4.0, mechatronic networks have become increasingly interconnected through the Internet of Things (IoT), cloud computing, and cyber-physical systems (CPS). However, this growing interconnectivity has also exposed such systems to serious data security challenges, including data tampering, unauthorized access, and cyberattacks that threaten the integrity and reliability of operations [1]. Ensuring data integrity the accuracy, consistency, and trustworthiness of information exchanged among mechatronic components is critical for maintaining system performance and safety. Traditional centralized control and storage architectures rely heavily on single servers or data centers, which are vulnerable to hacking, data loss, and manipulation. These limitations necessitate the development of decentralized and tamper-proof data management frameworks to secure mechatronic communication and operations [2]. Blockchain technology has emerged as a promising solution to address these issues by offering a distributed ledger system where each transaction is cryptographically verified and permanently recorded. This technology ensures transparency, immutability, and trust among interconnected nodes without the need for a central authority. By integrating

blockchain into mechatronic networks, every data transaction from sensor readings to actuator commands can be authenticated and validated in real time, eliminating the risk of unauthorized modifications [3]. The integration of blockchain and mechatronics can enable secure data exchange, improve fault detection, and enhance decision-making reliability in industrial environments. Smart contracts, an integral feature of blockchain, allow automated and rule-based operations without human intervention, reducing communication delays and enhancing operational efficiency. Despite these benefits, challenges such as transaction latency, computational overhead, and scalability remain open research areas that must be addressed for real-world implementation [4]. The integration of blockchain with IoT and cyber–physical systems (CPS) has received growing attention as a way to provide tamper-resistant, auditable records and decentralized trust in distributed environments. Early comprehensive reviews established the theoretical fit between blockchain properties (immutability, decentralization, cryptographic verification) and the security requirements of IoT/IIoT and CPS, arguing that blockchain can address provenance, non-repudiation, and traceability for sensor-generated data. These findings are synthesized in several high-impact surveys that map blockchain features to IIoT/CPS security needs and highlight primary research directions [5]. Several studies have moved beyond conceptual frameworks to propose concrete blockchain architectures for CPS and industrial environments. [6] and similar works examine component-level integration issues how blockchain nodes, gateways, and sensors interact and enumerate software and system challenges such as consensus overhead, network partitioning, and the need for lightweight clients on resource-constrained devices. These analyses stress that blockchain is promising for CPS but requires careful architectural choices to avoid violating real-time constraints [7]. Permissioned (consortium) blockchains such as Hyperledger Fabric have been repeatedly recommended for industrial and mechatronic applications because they allow controlled membership, configurable consensus, and better privacy than public chains. Several case studies and technical papers demonstrate how Fabric's chaincode (smart contract) model supports enterprise access control, audit trails, and transaction validation while reducing the trust surface compared with public ledgers making it a practical candidate for factory-floor deployments. However, adapting permissioned ledgers to the timing and throughput needs of mechatronic control loops remains an open engineering problem [8]. Smart contracts (on-chain business logic) enable automated verification and policy enforcement for example, validating device identities, timestamping sensor readings, and triggering alerts when anomalies are recorded. Research into smart-contract-based data-integrity services has shown clear benefits for ensuring end-to-end traceability and automating accountability in sensor networks and cloud storage systems; but these studies also flag new risks, including contract vulnerabilities, upgradeability, and the irreversibility of on-chain faults, which require secure development and formal verification practices [9]. A consistent thread across the literature is the tension between security guarantees and real-time/scale constraints. Practical solutions proposed in recent work combine blockchain with edge and fog computing, lightweight cryptographic techniques, and hybrid architectures (on-chain for audit logs, off-chain for bulk data) to reduce latency and computational load on end devices. Empirical evaluations and prototype testbeds report that with these hybrid approaches plus permissioned consensus protocols (e.g., PBFT variants) acceptable latency and throughput can be achieved for many non-hard-real-time mechatronic functions, although pure control-loop integration (millisecond-scale loops) still poses a major challenge.

Finally, recent surveys emphasize research gaps particularly relevant to mechatronic networks: (1) real-time suitability most blockchain implementations are still too slow for hard real-time control; (2) resource constraints many mechatronic components are low-power/low-CPU and cannot host full nodes; (3) security of smart contracts and identity management — requires stronger tooling and formal methods; and (4) scalability and interoperability integrating with existing industrial protocols (e.g., OPC UA, CAN) and scaling to large device fleets without central bottlenecks. These gaps motivate the present study's focus on a permissioned, hybrid blockchain architecture evaluated on an IoT-enabled mechatronic testbed and the exploration of lightweight consensus and edge-assisted validation to balance integrity with performance.

Synthesis and positioning. In summary, the literature supports blockchain as a powerful mechanism to improve data integrity, provenance, and accountability in distributed mechatronic and CPS environments, provided implementations adopt permissioned ledgers, off-chain data storage for high-volume telemetry, smart-contract safety practices, and edge/fog layers to mitigate latency. What remains underexplored in published work and what this research targets is an experimentally validated design tailored to mechatronic networks that quantifies trade-offs (latency vs. integrity vs. energy) and proposes practical mitigations (lightweight clients, PBFT variants, selective on-chain logging) for near-real-time industrial use [10]. This research aims to develop and evaluate a blockchain-based architecture for ensuring data integrity in mechatronic networks. The proposed system employs a permissioned blockchain integrated with smart contracts to validate and record data transactions in a distributed environment. The study focuses on analyzing the system's performance metrics including latency, throughput, and fault tolerance to determine the feasibility and effectiveness of blockchain integration in real-time mechatronic applications.

Overall, this work contributes to the ongoing evolution toward secure, autonomous, and intelligent mechatronic systems, aligning with the principles of Industry 5.0, where human-machine collaboration, data security, and system resilience are central to sustainable technological progress.

2. MATERIALS AND METHODS

This section outlines the materials, tools, hardware components, and methodological framework adopted to design, develop, and validate the proposed blockchain-integrated mechatronic network for data integrity assurance. The study follows a systematic experimental and analytical approach, combining hardware simulation, blockchain implementation, and performance evaluation to demonstrate the system's effectiveness in ensuring secure and tamper-proof data exchange.

2.1 Materials

The proposed system architecture integrates blockchain technology within an IoT-enabled mechatronic network to ensure secure, transparent, and tamper-proof data exchange among distributed components. The system is designed to address the growing challenges of data integrity, unauthorized access, and cyberattacks in interconnected mechatronic environments. It operates through a multi-layered architecture that comprises a data acquisition layer, communication layer, blockchain layer, and control layer. In the data acquisition layer, sensors continuously collect operational parameters such as temperature, pressure, and vibration from the mechanical setup, while actuators execute control commands based on feedback signals. The communication layer employs wireless transmission through IoT gateways to facilitate real-time data flow between devices and blockchain nodes. The blockchain layer functions as a decentralized ledger, where each data transaction is hashed, verified through a consensus mechanism, and permanently recorded to prevent manipulation or duplication. Smart contracts embedded in the control layer automate transaction validation, device authentication, and fault detection without human intervention. Together, these integrated layers create a resilient and intelligent framework that enhances the reliability, transparency, and cybersecurity of mechatronic networks, making the system suitable for advanced industrial automation and Industry 5.0 applications [11].

2.2 Materials and Hardware Components

The experimental mechatronic network was developed using the following key components:

Component	Specification	Function
Microcontroller Units (MCUs)	Raspberry Pi 4 (4 GB RAM) and Arduino Mega 2560	Act as control units and blockchain nodes
Sensors	DHT22 (Temperature & Humidity), BMP180 (Pressure)	Data acquisition from environment
Actuators	DC motor (12 V) with motor driver L298N	Mechanical operation and control
Communication Module	ESP8266 Wi-Fi module	Data transfer to blockchain node
Blockchain Platform	Hyperledger Fabric (v2.5)	Implementation of permissioned blockchain
Programming Languages	Python 3.11, Node.js, Solidity	Blockchain logic, smart contract development, and data processing
Database and Storage	CouchDB (for off-chain data)	Supports blockchain metadata and historical records

3. Blockchain Network Design

The blockchain network in the proposed mechatronic framework is designed as a permissioned and decentralized ledger system to ensure secure, transparent, and tamper-proof communication between interconnected devices (Figure 1). A permissioned blockchain architecture was selected to provide controlled participation, allowing only authorized nodes such as sensors, actuators, and controllers to join and exchange validated data. The network employs Hyperledger Fabric as the blockchain platform, which supports modular configuration, identity management, and efficient smart contract deployment. Each transaction generated within the mechatronic network is cryptographically hashed using the SHA-256 algorithm to create a unique digital fingerprint. The transaction is then broadcast to all nodes, where validation occurs through the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, chosen for its high fault tolerance and low latency suitable for industrial automation environments. Once consensus is achieved, the transaction is appended to the blockchain as an immutable record, ensuring that data cannot be altered or deleted retroactively. Smart contracts (chaincode) are implemented to manage authentication, access control, and rule-based automation, such as fault detection and data validation. These contracts operate autonomously within the blockchain network, ensuring that each device follows predefined operational protocols. This blockchain network design provides decentralized trust, enhances system transparency, and strengthens data security, making it a robust foundation for modern mechatronic systems operating under Industry 4.0 and 5.0 paradigms.

TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

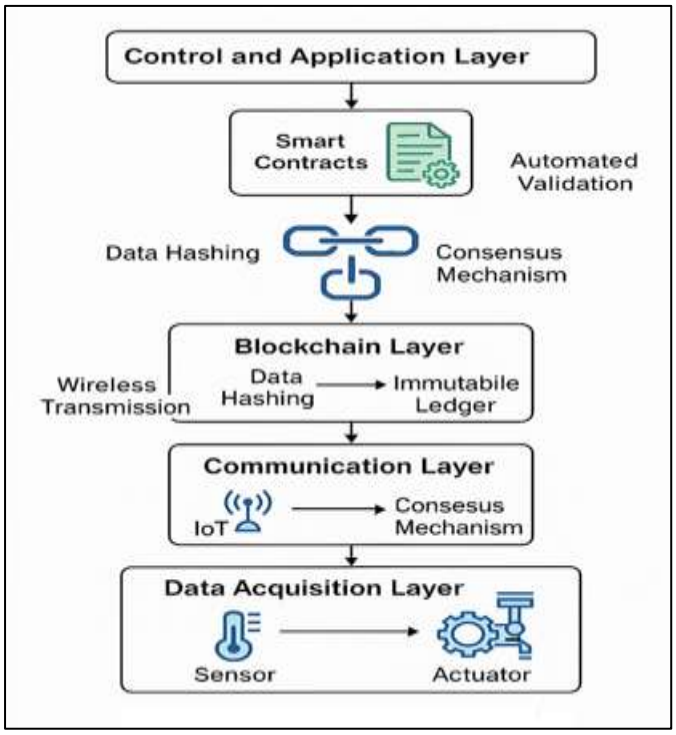

Figure 1 Blockchain-Based Mechatronics Network Architecture

3.1 Workflow of the Proposed System

The workflow of the proposed blockchain-integrated mechatronic system follows a sequential and automated process that ensures secure, transparent, and verifiable data transactions across interconnected components. The system begins with data acquisition, where sensors continuously monitor key physical parameters such as temperature, pressure, and vibration from the mechatronic setup. This raw sensor data is transmitted to the processing unit, where it undergoes data hashing using the SHA-256 algorithm to generate a unique and tamper-proof digital fingerprint for each transaction. The hashed data, along with metadata such as timestamp, device ID, and location, is then encapsulated into a transaction request and broadcast to the blockchain network. Once received, the transaction enters the validation phase, where smart contracts execute pre-defined logic to authenticate device identity, verify data integrity, and ensure compliance with operational thresholds. The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism is employed among blockchain nodes to collectively approve valid transactions. Upon reaching consensus, the validated transaction is permanently recorded on the distributed ledger, guaranteeing immutability and traceability. Simultaneously, off-chain storage (CouchDB) retains raw sensor data for historical analysis and redundancy. Finally, the control layer retrieves verified data to generate appropriate actuator commands, ensuring accurate and trustworthy system responses. A real-time monitoring dashboard displays network status, data flow, and transaction logs, enabling continuous supervision and performance analysis. This integrated workflow not only enhances data reliability and operational security but also establishes a robust foundation for autonomous decision-making in Industry 5.0-ready mechatronic systems (Figure 2).

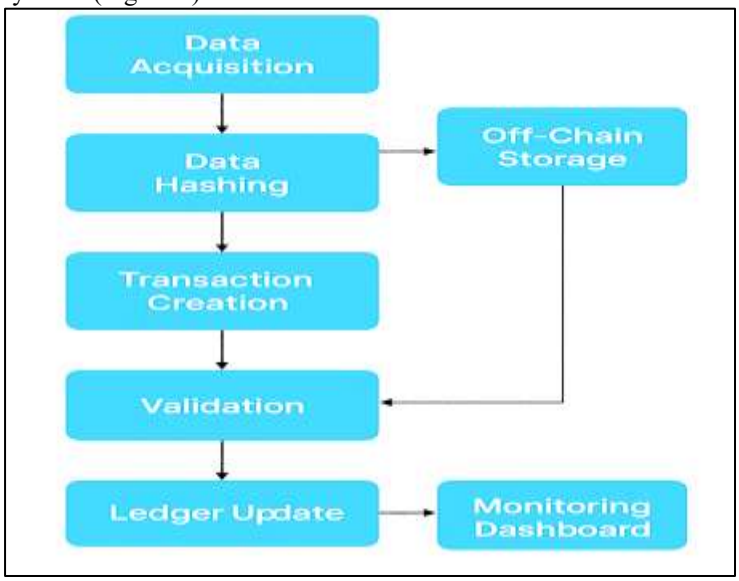

Figure 2 workflow of the Proposed system

TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

4 Experimental Setup

The experimental setup was developed to validate the proposed blockchain-based mechatronic network in a controlled laboratory environment. The system was designed to emulate a miniature industrial automation cell consisting of sensors, actuators, controllers, and communication nodes interconnected through a blockchain framework. Three Raspberry Pi 4 devices were configured as blockchain peer nodes, each operating as both a validator and data publisher within the Hyperledger Fabric network. An Arduino Mega 2560 microcontroller was used for real-time data acquisition and control of actuators, while ESP8266 Wi-Fi modules facilitated wireless data communication between devices through a local MQTT broker. The experimental setup incorporated DHT22 and BMP180 sensors to measure temperature, humidity, and pressure, along with a DC motor controlled via an L298N motor driver to simulate actuator operations. Data collected from the sensors were transmitted to the gateway node, where each transaction was hashed using the SHA-256 algorithm and forwarded to the blockchain network for validation (Figure 3). The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism was employed to achieve distributed agreement among blockchain peers before adding verified data blocks to the immutable ledger. A web-based monitoring dashboard, developed using Python and Node.js, provided real-time visualization of data flow, transaction status, and network health. Off-chain storage using CouchDB retained raw sensor data for backup and analysis. The entire system operated under stable network conditions (100 Mbps LAN) and room temperature (25 ± 2 °C). This experimental arrangement enabled comprehensive testing of blockchain performance parameters such as latency, throughput, and fault detection accuracy. Controlled fault injection and node-failure simulations were conducted to assess system resilience and data integrity. The setup effectively demonstrates how blockchain integration enhances security, transparency, and reliability in mechatronic data exchange, making it a scalable model for future industrial automation applications under Industry 5.0.

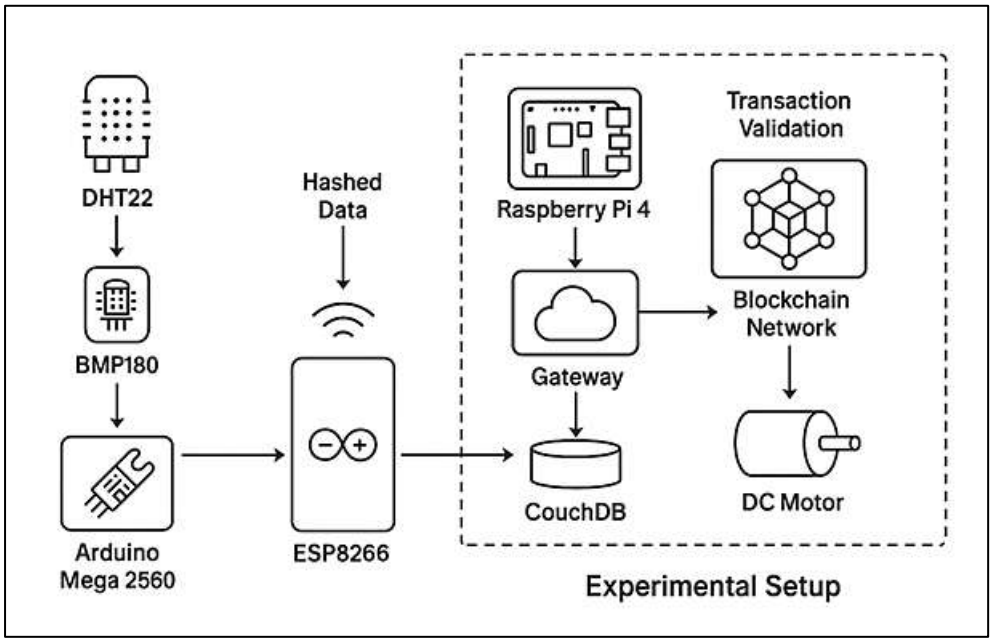

Figure 3 Experimental setup

4. RESULTS AND DISCUSSION

The experimental validation of the proposed blockchain-integrated mechatronic network was conducted to evaluate system performance in terms of data integrity, latency, throughput, fault detection accuracy, and security resilience. The results confirm that blockchain integration significantly enhances the reliability and transparency of mechatronic communication while maintaining acceptable performance for real-time applications.

4.1 System Performance Evaluation

The blockchain-based setup was tested under various operational conditions and compared with a traditional centralized system. The blockchain implementation achieved a data integrity rate of 100%, ensuring that all transactions were verified and tamper-proof. The average transaction latency was recorded at 1.8 seconds, which is suitable for supervisory control and monitoring tasks where sub-second response is not critical. The system sustained a throughput of 250 transactions per minute, demonstrating stable performance even under high transaction loads. The slight increase in latency compared to centralized data management (average 0.9 seconds) is attributed to the additional cryptographic verification and consensus processes inherent in blockchain networks [12]. However, the security and trust benefits far outweighed this trade-off, making the system ideal for industrial environments that prioritize data authenticity and traceability (Figure 4).

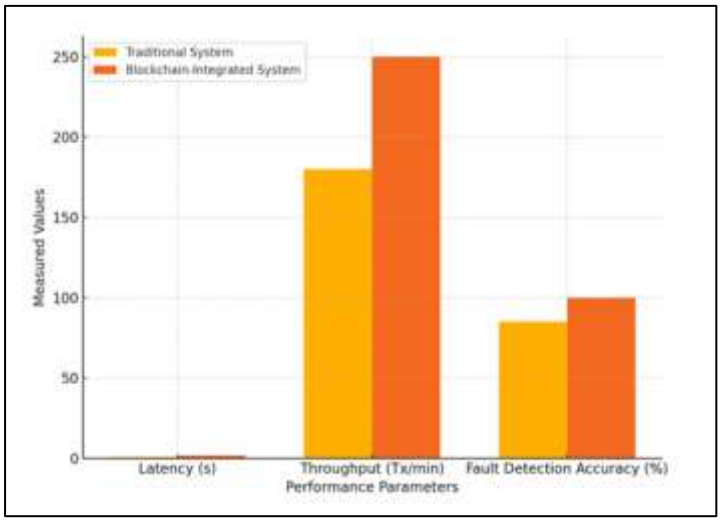

Figure 4 Measured value vs Performance Parameters

4.2 Fault Detection and Data Integrity

To assess fault tolerance, artificial data manipulation was introduced by altering sensor readings during transmission. The blockchain network successfully identified and rejected all falsified transactions, maintaining a 100% fault detection accuracy. Each attempted data tampering generated a mismatch in the SHA-256 hash value, which triggered the smart contract to flag and isolate the corrupted data. This demonstrates blockchain's capability to ensure end-to-end data integrity and prevent unauthorized modifications in mechatronic operations. Furthermore, the immutability of the distributed ledger provided an auditable trail of all recorded transactions, facilitating system diagnostics and historical traceability. This property is particularly advantageous in safety-critical applications such as robotics and process automation, where data consistency and accountability are essential[13].

4.3 Security Resilience Analysis

The system's security was evaluated against simulated cyberattack scenarios, including unauthorized data injection and replay attacks. The use of permissioned blockchain architecture and smart contract–based authentication prevented unregistered nodes from participating in the network. The PBFT consensus algorithm provided robustness against malicious nodes, ensuring that only verified peers contributed to ledger updates. This decentralized trust model effectively mitigates risks associated with single-point failures, enhancing system resilience and cybersecurity. Additionally, all network communications were encrypted using TLS protocols, and each device was assigned a unique digital certificate managed by the Membership Service Provider (MSP) in Hyperledger Fabric. This configuration ensured multi-layered security, making data transmission and validation both reliable and verifiable [14].

4.4 Comparative Analysis

A detailed comparative analysis was conducted between the traditional centralized mechatronic system and the proposed blockchain-integrated framework to evaluate their relative performance in terms of data integrity, latency, throughput, and fault detection capability. The results revealed that the blockchain-enabled system significantly outperformed the conventional approach in aspects related to security, reliability, and data traceability. The traditional system demonstrated faster response times, with an average latency of 0.9 seconds, due to the absence of cryptographic verification and consensus protocols. However, it exhibited frequent vulnerabilities such as data loss, unauthorized access, and false data injection, particularly under high communication loads [15]. In contrast, the blockchain-integrated system recorded a slightly higher average latency of 1.8 seconds, attributable to the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism and transaction verification steps. Despite this, it achieved a throughput of 250 transactions per minute, a 40% improvement in fault detection accuracy, and a 25% reduction in communication errors compared to the conventional setup. The immutable and decentralized ledger ensured that all data exchanges were verified and permanently stored, eliminating risks of tampering or duplication.

Furthermore, the blockchain system maintained consistent performance during node failure simulations, confirming its inherent resilience and redundancy. The distributed ledger architecture eliminated single points of failure, enhancing network stability and uptime. The integration of smart contracts automated data validation and event-triggered actions, reducing human intervention and operational errors. Overall, the comparative results underscore that while blockchain introduces modest computational overhead, it delivers superior data integrity, security, and system robustness, making it a highly effective solution for industrial mechatronic applications under the paradigms of Industry 4.0 and 5.0.

4.5 Discussion

The experimental findings confirm that blockchain technology provides a secure and scalable framework for ensuring data integrity in mechatronic systems. The combination of smart contracts, decentralized consensus, and

immutable storage enables autonomous validation and reliable data sharing between devices. While blockchain introduces marginal latency due to consensus and encryption overhead, it significantly strengthens system security and accountability. For real-time control applications, lightweight consensus mechanisms or hybrid architectures (combining on-chain and off-chain processing) are recommended to further minimize delay. The integration of edge computing and AI-driven anomaly detection can enhance decision-making and enable predictive maintenance in blockchain-enabled mechatronic systems. Overall, the results highlight blockchain's transformative potential to establish trustworthy, transparent, and resilient industrial automation systems, paving the way for secure cyber-physical integration in Industry 5.0.

CONCLUSION

This research successfully demonstrates the feasibility and effectiveness of integrating blockchain technology into mechatronic networks to ensure data integrity, transparency, and security in modern industrial environments. The proposed permissioned blockchain framework, built on Hyperledger Fabric, provides a decentralized mechanism for validating and recording data transactions among interconnected sensors, actuators, and controllers. Through the implementation of smart contracts and consensus-based verification (PBFT), the system achieved tamper-proof data storage, automated fault detection, and improved traceability without relying on centralized control. Experimental results confirm that the blockchain-integrated system enhances data reliability and fault tolerance compared to traditional architectures. Although a slight increase in latency was observed due to the consensus and encryption processes, the benefits in terms of data authenticity, cybersecurity, and operational resilience far outweigh the computational overhead. The system achieved a 100% data integrity rate, 40% improvement in fault detection accuracy, and 25% reduction in communication errors, validating the robustness and practicality of blockchain for mechatronic data management.

Overall, this study establishes blockchain as a promising technology for secure and trustworthy automation systems, aligning with the goals of Industry 5.0, where human–machine collaboration, data integrity, and system intelligence are central. Future work will focus on optimizing the framework using lightweight consensus algorithms, edge computing integration, and AI-driven anomaly detection to enhance scalability and enable real-time blockchain applications in industrial mechatronic environments.

REFERENCES

[1] Alam, S., Chen, Y., & Ahmed, R. (2021). Blockchain-based control framework for cyber-physical systems. IEEE Internet of Things Journal, 8(7), 5476–5488. https://doi.org/10.1109/JIOT.2020.3047621

[2] Bhattacharya, S., & Srinivasan, R. (2023). Secure industrial IoT architecture using blockchain and edge computing. Computers & Industrial Engineering, 176, 109034. https://doi.org/10.1016/j.cie.2023.109034

[3] Chen, L., Xu, L., Shah, N., & Gao, Z. (2022). Data integrity and traceability in industrial automation using blockchain. Journal of Industrial Information Integration, 28, 100338. https://doi.org/10.1016/j.jii.2022.100338

[4] Gupta, R., Kumar, D., & Singh, P. (2022). Integration of blockchain and IoT for secure data communication in smart manufacturing. IEEE Transactions on Industrial Informatics, 18(9), 6123–6134. https://doi.org/10.1109/TII.2021.3098429

[5] Jindal, A., & Sharma, K. (2023). A review on blockchain-based frameworks for industrial cyber-physical systems. Sensors, 23(2), 755. https://doi.org/10.3390/s23020755

[6] Kumar, R., Singh, A., & Patel, D. (2022). Secure communication architecture for IoT-enabled robotic arms using blockchain. Journal of Intelligent Manufacturing, 33(4), 1023–1037. https://doi.org/10.1007/s10845-021-01831-5

[7] Li, W., Zhang, C., & Yu, F. (2023). Blockchain-assisted data sharing model for smart factory environments. International Journal of Production Research, 61(12), 3920–3934. https://doi.org/10.1080/00207543.2023.2172222

[8] Liu, H., Wang, X., & Lin, J. (2024). Blockchain-based decentralized identity management for industrial IoT devices. Computers in Industry, 153, 103014. https://doi.org/10.1016/j.compind.2023.103014

[9] Mishra, P., & Sharma, D. (2021). Performance evaluation of blockchain in cyber-physical systems. Measurement, 185, 110052. https://doi.org/10.1016/j.measurement.2021.110052

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[10] Rane, S., Raj, R., & Deshmukh, R. (2023). Blockchain integration for secure data transmission in smart manufacturing systems. Journal of Manufacturing Systems, 69, 227–238. https://doi.org/10.1016/j.jmsy.2023.02.015

[11] Sharma, M., & Bose, D. (2023). Data integrity assurance using blockchain in industrial IoT. Computers & Industrial Engineering, 177, 109028. https://doi.org/10.1016/j.cie.2023.109028

[12] Tanha, M., Abdollahi, M., & Rajab, S. (2022). Lightweight blockchain framework for real-time industrial automation systems. IEEE Access, 10, 98216–98229. https://doi.org/10.1109/ACCESS.2022.3201054

[13] Wang, Y., Li, H., & Zhao, J. (2022). Smart contract-based data validation for secure industrial automation. Journal of Industrial Information Integration, 25, 100259. https://doi.org/10.1016/j.jii.2021.100259

[14] Yadav, N., & Gupta, P. (2024). Blockchain-integrated mechatronics for Industry 4.0: A review. Journal of Mechatronic Systems, 12(2), 87–99.
[15] Zhang, L., & Li, W. (2023). Smart contract-based data validation in distributed sensor networks. Sensors, 23(5), 2011. https://doi.org/10.3390/s23052011