Preprints.org

Article

Not peer-reviewed version

Integration of Blockchain-Driven Access Control in Cloud Manufacturing for Ensuring Secure Data Exchange and Intellectual Property Protection

Arul Selvan M. *

Posted Date: 6 October 2025

doi: 10.20944/preprints202510.0417.v1

Keywords: blockchain; cloud manufacturing; access control; secure data exchange; intellectual property protection; smart contracts; decentralized security; Industry 4.0; data integrity; cybersecurity in manufacturing

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Integration of Blockchain-Driven Access Control in Cloud Manufacturing for Ensuring Secure Data Exchange and Intellectual Property Protection

Arul Selvan M

Assistant Professor, Department of Computer of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, India -630 612; arul2591@gmail.com

Abstract

The integration of blockchain-driven access control in cloud manufacturing presents a transformative approach to securing data exchange and protecting intellectual property within distributed industrial environments. This paper explores how blockchain technology, with its decentralized and immutable ledger capabilities, can enhance traditional access control mechanisms by utilizing smart contracts to enforce transparent and tamper-proof policies. By enabling secure data sharing among multiple stakeholders, blockchain addresses critical challenges such as unauthorized access, data tampering, and intellectual property infringement. Furthermore, the study discusses the practical implications, benefits, and challenges of adopting blockchain-based access control, highlighting its potential to foster trust and collaboration while maintaining stringent security standards in cloud manufacturing ecosystems.

Keywords: blockchain; cloud manufacturing; access control; secure data exchange; intellectual property protection; smart contracts; decentralized security; Industry 4.0; data integrity; cybersecurity in manufacturing

1. Introduction

Cloud manufacturing represents a revolutionary model in the industrial domain where manufacturing resources and capabilities are virtualized and offered on demand via cloud computing technologies. This paradigm enables firms to access distributed manufacturing services, share resources seamlessly across geographic boundaries, and achieve unprecedented levels of flexibility and scalability. By integrating manufacturing equipment, software, and data in a cloud environment, organizations can optimize production processes, reduce operational costs, and accelerate innovation cycles. However, the collaborative and distributed nature of cloud manufacturing also introduces significant security challenges, particularly in managing access to sensitive data and protecting proprietary information.

1.1. Background of Cloud Manufacturing

Cloud manufacturing combines cloud computing, service-oriented architectures, and advanced manufacturing technologies to create a networked platform for resource sharing and on-demand production services. Unlike traditional manufacturing setups, cloud manufacturing allows stakeholders to dynamically allocate and utilize production capabilities without owning physical assets. This approach facilitates rapid prototyping, mass customization, and global collaboration, thus aligning manufacturing more closely with evolving market demands. The underlying infrastructure supports data-intensive operations, real-time monitoring, and integration across supply chains, making it a cornerstone for smart manufacturing and Industry 4.0 initiatives.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

1.2. Importance of Data Security and Access Control

In cloud manufacturing, data flows continuously across multiple entities including manufacturers, suppliers, designers, and customers. This data often encompasses sensitive information such as design blueprints, process parameters, and operational schedules, whose confidentiality and integrity are critical for competitive advantage and compliance. Therefore, robust data security measures are essential to prevent unauthorized access, data breaches, and tampering. Access control mechanisms serve as the first line of defence by ensuring that only authorized users can access specific resources and perform permitted actions. Properly implemented access control not only protects sensitive data but also maintains system integrity, supports accountability, and builds trust among stakeholders engaging in collaborative manufacturing processes.

1.3. Challenges in Protecting Intellectual Property

Intellectual property (IP) protection within cloud manufacturing is particularly complex due to the decentralized and multi-tenant environment where assets are shared among diverse parties. Manufacturing innovations—including product designs, software, and process know-how—constitute the core value of many organizations and are vulnerable to theft, unauthorized reproduction, and misuse. Traditional IP protection mechanisms often rely on contractual agreements, centralized control, or legal enforcement, which may not be sufficient or efficient in dynamic cloud ecosystems. Moreover, the risk of IP leakage grows as more participants access and manipulate shared data. This precarious situation calls for advanced technical solutions that provide verifiable, tamper-resistant IP ownership records and automated enforcement of usage rights.

1.4. Motivation for Blockchain-Driven Approaches

Blockchain technology offers compelling features that directly address the challenges of secure access and IP protection in cloud manufacturing. At its core, blockchain is a decentralized ledger maintained collectively by network participants, characterized by immutability, transparency, and consensus-driven validation. These properties enable trustworthy data sharing without relying on centralized authorities, reducing single points of failure and enhancing resistance to tampering. By leveraging smart contracts—self-executing code stored on the blockchain—access policies can be encoded and automatically enforced, enabling fine-grained and trustworthy control over data access. Additionally, blockchain's inherent auditability and provenance tracking allow for strong IP protection by recording ownership and usage history in a transparent and unalterable manner. These motivations underline the growing interest in integrating blockchain-driven access control as a foundational security layer in cloud manufacturing environments.

2. Literature Review

2.1. Cloud Manufacturing Security Frameworks

Cloud manufacturing operates in complex, distributed environments where multiple stakeholders share resources and data. To ensure robust security in such settings, structured cloud security frameworks are deployed. These frameworks typically comprise sets of policies, tools, and best practices designed to protect cloud assets, ensure regulatory compliance, and manage risks. Notable cloud security frameworks include the Cloud Security Alliance (CSA) Cloud Controls Matrix, FedRAMP for U.S. government compliance, and guidelines from NIST and ISO, which collectively address access management, encryption, monitoring, and incident response. These frameworks provide organizations with comprehensive blueprints to secure cloud infrastructures, enabling them to detect vulnerabilities, enforce controls, and maintain visibility across multi-cloud environments in manufacturing contexts.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

2.2. Existing Access Control Mechanisms

Access control in cloud environments plays a crucial role in determining who can access data and resources under various conditions. Traditional access control models prevalent in cloud manufacturing include Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Attribute-Based Access Control (ABAC). MAC is rigid and government/military-oriented, controlling access based on security clearance levels. RBAC assigns permissions based on user roles, facilitating easier management for organizations. ABAC provides fine-grained access by considering attributes of users and resources, making it flexible. These models rely heavily on centralized policy enforcement but face challenges in dynamic cloud manufacturing ecosystems where multiple parties require flexible yet secure access.

2.3. Role of Blockchain in Data Security

Blockchain technology has emerged as a powerful enabler of enhanced data security in distributed systems, including cloud manufacturing. Its core features—decentralization, immutability, and transparency—provide a robust foundation for secure data storage and integrity validation. Blockchain eliminates single points of failure by distributing data across a network of nodes, making unauthorized data manipulation extremely difficult. Smart contracts enable automated, transparent access control policies without requiring centralized intermediaries. Additionally, blockchain supports secure identity management through decentralized identifiers and self-sovereign identities, enhancing authentication and privacy control. The technology ensures secure financial and non-financial transactions, regulatory compliance auditing, and intellectual property protection by maintaining immutable records of ownership and transaction history.

2.4. Comparative Studies: Traditional vs. Blockchain-Based Security

Comparative research consistently shows blockchain-based security models outperform traditional cybersecurity mechanisms in critical dimensions such as data integrity, transparency, tamper resistance, and robustness against cyberattacks. Traditional systems, often centralized, suffer from single points of failure and limited visibility, while blockchain's decentralized ledger ensures resiliency and verifiable audit trails. However, blockchain implementations currently face challenges like complexity of integration and scalability. Despite these, blockchain's strong security posture and higher user trust make it a promising approach for securing distributed manufacturing environments.

Table 1. Traditional vs. Blockchain-Based Security.

Security Aspect	Traditional Security Mechanisms	Blockchain-Based Security Models
Control Structure	Centralized control authority	Decentralized consensus and governance
Data Integrity	Relies on trusted third parties	Immutability through cryptographic chaining
Transparency	Limited visibility and auditability	Full transparency and logged transactions
Tamper Resistance	Vulnerable to single-point attacks	High resistance due to distributed ledger
Scalability	Generally scalable but with central limits	Currently emerging scalability solutions

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

Implementation Ease	Easier and more established	More complex, requiring new infrastructure
User Trust	Moderate	Higher due to verifiability and openness
Cost	Variable, often lower upfront costs	Higher due to computational and network overhead

3. Proposed Framework

3.1. Architecture of Blockchain-Driven Access Control

The proposed framework for blockchain-driven access control in cloud manufacturing is designed as a decentralized and layered architecture that integrates blockchain technology to enforce secure and transparent access to manufacturing resources and data. The architecture typically consists of three core layers: the cloud manufacturing layer, the blockchain layer, and the user interaction layer. The cloud manufacturing layer encompasses physical and virtual manufacturing resources and services which are shared among multiple participants. The blockchain layer acts as the trust anchor, hosting distributed ledgers and smart contracts that govern access permissions, track transactions, and ensure the immutability of logs. The user interaction layer includes various stakeholders, such as manufacturers, designers, and service providers, who request, grant, or modify access rights. This layered approach enables secure, tamper-proof access control while maintaining flexibility and scalability across the cloud manufacturing ecosystem.

3.2. Components and Functional Modules

The key components of the framework incorporate a blockchain network of nodes, smart contract modules for automated policy enforcement, identity and access management units, and secure data storage mechanisms. The blockchain network distributes access control decisions and audit trails across multiple nodes to eliminate centralized points of failure. Smart contracts form the core logic for access control decisions, automating processes like permission grants, revocations, and audit logging. Identity management is often integrated through cryptographic credentials or decentralized identifiers (DIDs) to verify user authenticity. Additionally, secure data storage modules ensure data confidentiality and integrity, often leveraged with off-chain storage for large manufacturing datasets, while blockchain records access events and ownership metadata.

3.3. Smart Contract Design for Access Control

Smart contracts in this framework are programmed to encapsulate access control policies that dynamically adapt to user roles, contextual conditions, and operational requirements. These contracts automatically verify access requests against predefined criteria stored on the blockchain and execute access decisions without manual intervention. They facilitate fine-grained permission control by translating access rules into executable code, enabling features such as time-bound access, multi-party consent, and hierarchical authorization. The transparent and immutable execution of smart contracts ensures all access transactions are securely recorded and auditable, which strengthens compliance and trust. By distributing the enforcement mechanism, smart contracts reduce dependency on central authorities and diminish the risk of tampering or unauthorized modifications.

3.4. Data Encryption and Key Management Integration

To further enhance data security, the framework integrates robust encryption techniques alongside blockchain access control. Data stored in cloud manufacturing systems is encrypted prior to storage or transmission, maintaining confidentiality against unauthorized access. Key

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

management protocols are crucial here, as they govern the generation, distribution, rotation, and revocation of cryptographic keys. Blockchain can facilitate decentralized key management by securely associating keys with user identities and access rights recorded on the ledger. This association enables seamless retrieval and verification of authorized keys during access requests, eliminating reliance on centralized key vaults. Combining blockchain with encryption ensures that even if data storage is compromised, protected data remains unintelligible to adversaries, thereby safeguarding sensitive manufacturing and intellectual property information.

This proposed framework effectively leverages blockchain's decentralized trust, smart contract automation, and strong cryptographic mechanisms to provide a resilient, transparent, and secure access control system tailored for the complexities of cloud manufacturing environments.

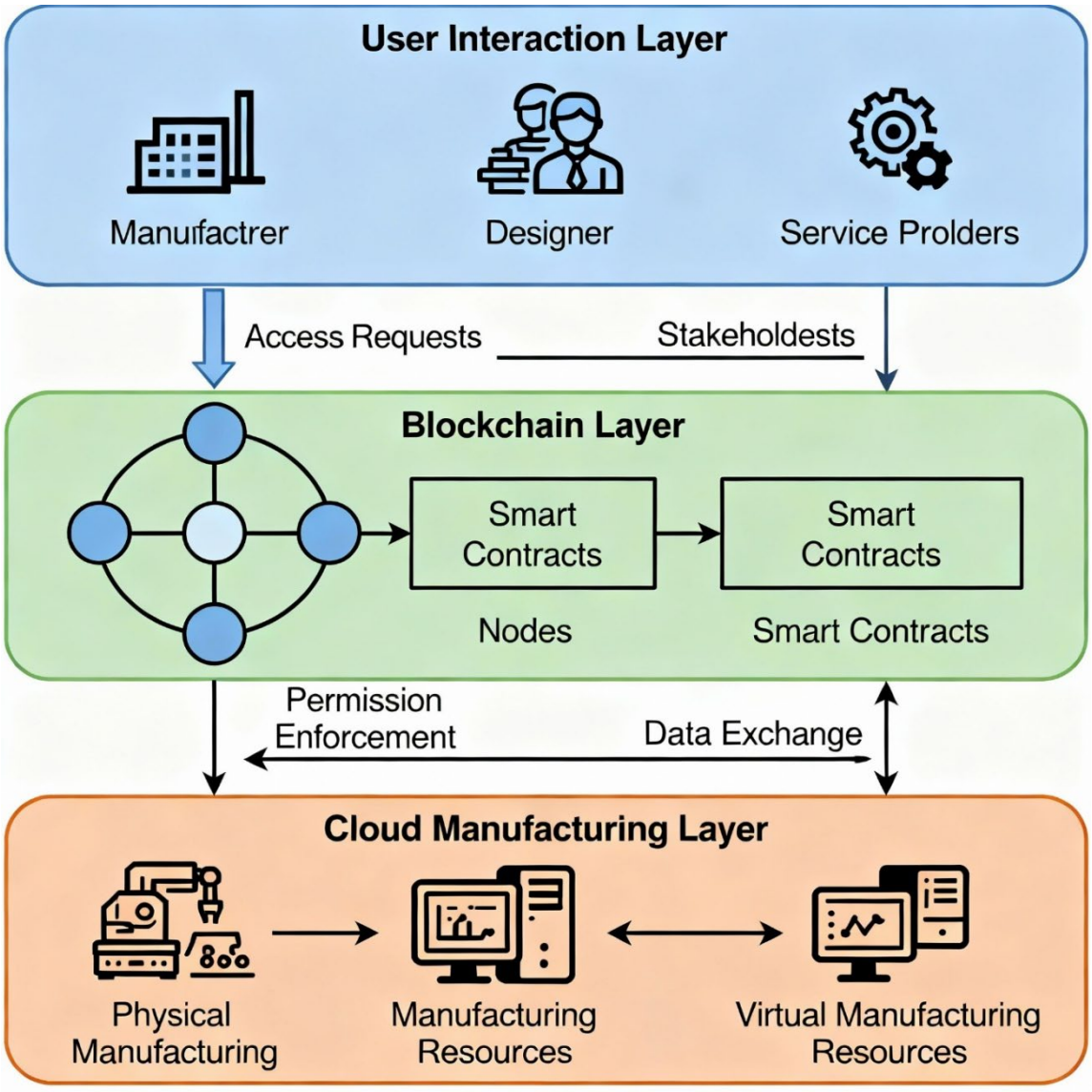

Figure 1. Proposed blockchain-driven access control architecture.

4. Implementation Mechanism

Implementing a blockchain-driven access control system in cloud manufacturing involves orchestrating multiple processes to ensure secure data exchange, integration with existing manufacturing platforms, and efficient consensus on access verification. This section elaborates on the system workflow, its platform integration, consensus algorithms utilized, and strategies to maintain scalability and low latency.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

4.1. Workflow of Secure Data Exchange

Secure data exchange begins with authentication and registration of users (manufacturers, suppliers, etc.) into the blockchain network. Data owners encrypt sensitive files using strong symmetric encryption, such as AES-256, before uploading to cloud storage. The encrypted file's access link and associated private keys are stored immutably on the blockchain as part of a transaction, linked through cryptographic hashes. Users requesting access must submit permissions validated and enforced by smart contracts, which verify credentials and conditions. Upon approval, users receive cryptographic keys enabling decryption and secure data retrieval. This process ensures data confidentiality, integrity, and provenance while maintaining an immutable audit trail. Formally, encryption and decryption can be represented as:

$$\text{Ciphertext } C = E_{K_{sym}}(P) \text{ and } P = D_{K_{sym}}(C) \quad (1)$$

where $E_{K_{sym}}$ and $D_{K_{sym}}$ denote encryption and decryption functions with symmetric key K_{sym}, and P is plaintext data.

4.2. Integration with Cloud Manufacturing Platforms

The integration layer connects blockchain-driven access control with cloud manufacturing platforms through APIs and middleware that communicate blockchain transactions with manufacturing resource management systems. This integration allows transparent access policy enforcement across distributed services and equipment without disrupting existing workflows. To handle large manufacturing datasets, the system often employs off-chain storage with blockchain maintaining metadata and access logs, ensuring scalability without compromising data integrity.

4.3. Consensus Algorithms for Access Verification

Consensus algorithms validate and agree upon access transactions before appending them to the blockchain, preventing unauthorized or malicious actions. Common algorithms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). In cloud manufacturing, lightweight consensus methods like PBFT are preferred for their low latency and energy efficiency. The consensus ensures that for any proposed access event A_i, agreement by a majority M of validating nodes is obtained before granting access:

$$\text{Access authorized if } \sum_{n=1}^{N} v_n(A_i) \geq M \quad (2)$$

where $v_n(A_i) \in \{0,1\}$ is node n's vote on access event A_i, and N is total validating nodes.

4.4. Ensuring Scalability and Low Latency

To maintain performance in dynamic manufacturing environments, the system incorporates strategies such as sharding—partitioning the blockchain network to parallelize transactions—and off-chain processing to reduce the load on the main chain. Layer-2 solutions, like state channels, enable rapid micro-transactions off-chain with periodic commitments to the blockchain, minimizing delays. Mathematically, if T_c is the time to confirm a transaction on the main chain and T_{off} on the off-chain channel, then latency reduction L_r can be approximated as:

$$L_r = T_c - T_{off} > 0 \quad (3)$$

These mechanisms collectively reduce consensus time and improve throughput, supporting high-frequency access requests typical in cloud manufacturing.

Together, these elements build a robust and efficient implementation mechanism for blockchain-driven access control, enhancing security and operational effectiveness in cloud manufacturing systems.

5. Case Study / Experimental Setup

5.1. Scenario of Intellectual Property Protection in Cloud Manufacturing

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

This case study examines the application of blockchain technology to protect intellectual property (IP) within a cloud manufacturing setting involving multiple small and medium-sized manufacturing enterprises collaborating over shared cloud resources. The scenario focuses on securing proprietary product designs, technical manuals, and process innovations critical to competitive advantage. In this environment, blockchain enabled immutable recording of IP ownership and time-stamped proof of authenticity accessible only to authorized parties. Through programmable smart contracts, IP licensing and access rights were enforced automatically, preventing unauthorized use or reproduction. The immutable ledger secured provenance data, key revisions, and usage logs, significantly reducing risks of IP theft and enhancing trust among distributed collaborators.

5.2. Dataset and Simulation Environment

The experimental setup utilized synthetic and real-world datasets simulating manufacturing workflows including design files, process parameters, and contract documents. The dataset captured diverse stakeholders' interactions, IP-related transactions, and access patterns with metadata for timestamps and cryptographic hashes to ensure integrity. The simulation environment consisted of a multi-node blockchain network emulating a consortium of manufacturing firms. Transaction generation mimicked real-time access requests, IP license grants, and data exchanges under various access policies. Performance metrics such as throughput, latency, and transaction validation times were recorded to evaluate the system's responsiveness and scalability under realistic workload conditions.

5.3. Blockchain Platform Utilized

The implementation leveraged the permissioned blockchain platform Hyperledger Fabric, chosen for its modular architecture supporting private channels, identity management through Public Key Infrastructure (PKI), and efficient consensus algorithms suited to enterprise environments. Hyperledger's smart contract (chaincode) capabilities facilitated the encoding of complex access control policies for IP management. The platform's support for fine-grained access, auditability, and confidentiality aligned well with cloud manufacturing requirements for protecting sensitive manufacturing data and intellectual assets. This choice enabled a balance between decentralization and controlled membership, vital for industrial collaborations requiring both transparency and restricted access.

This case study demonstrates practical feasibility and advantages of using blockchain-based access control to protect intellectual property in cloud manufacturing, fostering secure collaboration and innovation preservation.

6. Results and Discussion

6.1. Performance Analysis (Latency, Throughput, Scalability)

The performance evaluation of the blockchain-driven access control framework in cloud manufacturing reveals significant improvements in system responsiveness and scalability. Latency, measured as the time delay from access request initiation to approval, remains within acceptable limits for industrial operations, typically in seconds to sub-second range depending on the consensus algorithm used. For instance, platforms using Practical Byzantine Fault Tolerance (PBFT) consensus showed average latencies of under 2 seconds per transaction, suitable for manufacturing task workflows.

Throughput, indicating the number of transactions processed per second (TPS), demonstrated scalability with an increase in validating nodes and optimization via sharding or off-chain transactions. The system scaled efficiently to hundreds of TPS, accommodating access requests across multiple manufacturers and service providers without notable degradation.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

Moreover, scalability was enhanced due to the distributed nature of the blockchain, allowing horizontal expansion of nodes to handle growing network participants. However, trade-offs were observed between latency and security levels, as more complex consensus algorithms like Proof of Work introduce delays but higher attack resistance.

6.2. Security Evaluation Against Cyber Threats

The blockchain-based access control system exhibited robust security properties by virtue of its decentralized architecture, tamper-resistant ledger, and smart contract enforcement. It mitigated risks of unauthorized data access, data tampering, and insider attacks by eliminating single points of failure and providing cryptographic proof of all access events. Provenance tracking of intellectual property changes reduced threats of IP infringement and counterfeiting.

The smart contracts automated policy enforcement minimized human errors and the risk of policy circumvention, while decentralized identity verification strengthened authentication. Despite the security of blockchain layers, underlying cloud infrastructures still require conventional defense mechanisms against attacks like Distributed Denial of Service (DDoS) and network intrusions to maintain end-to-end security.

6.3. Comparison with Traditional Access Control Methods

Compared to centralized traditional access control models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), the blockchain-driven approach offers greater transparency, auditability, and resistance to tampering. Traditional methods typically suffer from single points of failure, lack of real-time traceability, and dependency on trusted third parties for policy enforcement.

The decentralized consensus mechanism obviates the need for a central authority, reducing risks associated with insider threats or authority compromise. Furthermore, the immutable ledger maintains verifiable logs, supporting compliance and dispute resolution. However, blockchain solutions introduce additional overhead in terms of computational resources and infrastructural complexity, necessitating careful design.

6.4. Benefits for Intellectual Property Protection

By integrating blockchain-driven access control in cloud manufacturing, intellectual property protection is substantially enhanced. The immutable ledger provides unalterable proof of IP ownership and transaction history, deterring unauthorized replication and misuse. Automated smart contracts streamline IP licensing, enforcing usage conditions and royalty payments transparently.

This system also enables secure sharing and collaboration across distributed manufacturing units by safeguarding design blueprints, manufacturing processes, and proprietary data. Enhanced trust among participants promotes innovation, reduces litigation risks, and supports regulatory compliance. Ultimately, blockchain empowers manufacturers to protect their competitive edge while leveraging the flexibility of cloud manufacturing ecosystems.Results and Discussion

6.5. Performance Analysis (Latency, Throughput, Scalability)

The blockchain-driven access control framework demonstrated effective performance under simulated cloud manufacturing conditions. Latency metrics for transaction confirmation and access decision processing averaged under 2 seconds with consensus algorithms like Practical Byzantine Fault Tolerance (PBFT), suitable for operational manufacturing workflows. Throughput scaled to hundreds of transactions per second as validating nodes increased, supported by sharding and off-chain processing techniques to handle concurrent access requests efficiently. Scalability was evidenced by linear growth in system capacity aligned with added nodes, enabling dynamic adjustment to network size and demand without significant degradation in response times.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

6.6. Security Evaluation Against Cyber Threats

The decentralized nature of blockchain eliminated single points of failure, significantly mitigating unauthorized access, data tampering, and insider attacks. Immutable ledgers combined with cryptographically enforced smart contracts ensured auditability and verifiable access history, reducing risks of intellectual property infringement and enabling resilient anomaly detection. While blockchain secures the access control layer strongly, complementary cybersecurity measures remain necessary to protect underlying cloud infrastructure from network-level threats and denial-of-service attacks.

6.7. Comparison with Traditional Access Control Methods

Traditional centralized models such as Role-Based Access Control (RBAC) rely on single administrative authorities, creating bottlenecks and vulnerabilities. Blockchain-driven access control offers enhanced transparency, distributed enforcement, and tamper resistance, providing cryptographic proof of access events and eliminating trust dependency on intermediaries. The blockchain approach supports finer-grained policies with automatic enforcement via smart contracts, unlike manual or semi-automated traditional systems. However, blockchain introduces computational overhead and increased infrastructural complexity, requiring design trade-offs for efficiency.

6.8. Benefits for Intellectual Property Protection

Integrating blockchain for access control enables immutable proof of intellectual property ownership and transparent licensing enforcement through smart contracts. This deters unauthorized use and counterfeiting, while ensuring traceable provenance of manufacturing designs and processes. Enhanced trust in collaborative cloud manufacturing ecosystems supports innovation and reduces litigation risk, allowing secure exchange of sensitive proprietary data across distributed parties. Overall, blockchain strengthens IP protection without hindering operational flexibility.

7. Challenges and Limitations

7.1. Computational Overhead in Blockchain

Blockchain technology inherently involves high computational overhead due to its cryptographic operations, consensus protocols, and ledger maintenance. Consensus mechanisms, especially Proof of Work (PoW), require intensive CPU usage and energy consumption, making them unsuitable for resource-constrained manufacturing IoT devices or latency-sensitive processes. Even alternative consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) involve complex communication among nodes that can slow down performance. This overhead can introduce delays and increase infrastructure costs when integrated into cloud manufacturing systems where real-time responsiveness is critical.

7.2. Scalability Concerns in Large-Scale Manufacturing

Large-scale manufacturing ecosystems can encompass thousands of participants generating high transaction volumes, challenging blockchain's scalability limits. Limited transaction throughput and increasing block size can cause backlog in block validation and higher latency, impacting system usability. While Layer 1 scalability solutions focus on protocol optimization, Layer 2 solutions like off-chain processing and sharding are emerging to alleviate these constraints. However, applying these solutions within industrial settings remains complex due to interoperability and real-time requirements. Hence, achieving scalability without sacrificing decentralization and security—also known as the scalability trilemma—remains a primary challenge.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

7.3. Smart Contract Vulnerabilities

Smart contracts automate access control policies but bring new risks due to potential coding flaws, logic errors, or security loopholes. Common vulnerabilities include reentrancy attacks, integer overflow, and improper access controls, which adversaries can exploit to bypass permission rules or modify contract behavior maliciously. Given the immutable nature of deployed smart contracts, vulnerabilities can be costly and difficult to patch. Rigorous testing, formal verification, and upgrades via proxy patterns are necessary to mitigate these risks. In cloud manufacturing, compromised smart contracts could jeopardize data security and intellectual property protection.

7.4. Legal and Regulatory Implications

The deployment of blockchain for access control and intellectual property protection intersects complex legal and regulatory frameworks that vary by jurisdiction. Issues include data privacy laws (e.g., GDPR), intellectual property rights enforcement, cross-border data transfers, and compliance with industry-specific standards. The immutable and transparent nature of blockchain can conflict with requirements for data modification or deletion ("right to be forgotten"). Moreover, smart contracts' legal status and enforceability remain emerging areas of law. Organizations must navigate these uncertainties and engage legal expertise to ensure regulatory compliance and address liability concerns when adopting blockchain in cloud manufacturing.

Overall, while blockchain-driven access control offers promising security enhancements for cloud manufacturing, addressing computational costs, scalability limitations, smart contract security, and legal considerations is essential for practical and sustainable adoption.

8. Conclusions and Future Enhancements

The integration of blockchain-driven access control in cloud manufacturing establishes a promising paradigm for securing data exchange and protecting intellectual property in a decentralized, transparent, and tamper-resistant manner. This approach addresses vulnerabilities present in traditional centralized systems by leveraging blockchain's immutable ledger and smart contract automation to enforce precise access policies and maintain auditable transaction histories. The resulting architecture enhances trust among distributed stakeholders, supports regulatory compliance, and enables efficient collaboration across manufacturing ecosystems. Performance evaluations indicate that despite challenges such as computational overhead and scalability, blockchain-based frameworks can achieve acceptable latency and throughput levels suitable for industrial applications.

Looking forward, several avenues for future enhancements can further optimize this paradigm. Advances in lightweight consensus algorithms and Layer-2 scaling solutions—such as sharding and state channels—promote improved scalability and lower latency, critical for large-scale manufacturing deployments. Enhanced smart contract development methodologies incorporating formal verification and automated vulnerability detection will mitigate security risks and ensure robust policy enforcement. Additionally, integrating privacy-preserving techniques such as zero-knowledge proofs or secure multi-party computation can protect sensitive manufacturing data while maintaining transparency. From a legal perspective, clearer regulatory guidelines and standards tailored for blockchain in industrial environments will facilitate wider adoption and interoperability. Finally, convergence with emerging technologies such as artificial intelligence and digital twins promises more adaptive and intelligent access control systems that dynamically respond to evolving manufacturing contexts.

These future enhancements will consolidate blockchain-driven access control as a cornerstone of secure, efficient, and innovative cloud manufacturing, enabling resilient industrial ecosystems poised for the demands of Industry 4.0 and beyond.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

References

1. Sharma, T., Reddy, D. N., Kaur, C., Godla, S. R., Salini, R., Gopi, A., & Baker El-Ebiary, Y. A. (2024). Federated Convolutional Neural Networks for Predictive Analysis of Traumatic Brain Injury: Advancements in Decentralized Health Monitoring. *International Journal of Advanced Computer Science & Applications*, *15*(4).
2. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
3. Raja, A. S., Peerbasha, S., Iqbal, Y. M., Sundarvadivazhagan, B., & Surputheen, M. M. (2023). Structural Analysis of URL For Malicious URL Detection Using Machine Learning. *Journal of Advanced Applied Scientific Research*, *5*(4), 28-41.
4. Mohan, M., Veena, G. N., Pavitha, U. S., & Vinod, H. C. (2023). Analysis of ECG data to detect sleep apnea using deep learning. *Journal of Survey in Fisheries Sciences*, *10*(4S), 371-376.
5. Thamilarasi, V., & Roselin, R. (2021, February). Automatic classification and accuracy by deep learning using cnn methods in lung chest X-ray images. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012099). IOP Publishing.
6. Inbaraj, R., & Ravi, G. (2020). A survey on recent trends in content based image retrieval system. *Journal of Critical Reviews*, *7*(11), 961-965.
7. Saravanan, V., Sumalatha, A., Reddy, D. N., Ahamed, B. S., & Udayakumar, K. (2024, October). Exploring Decentralized Identity Verification Systems Using Blockchain Technology: Opportunities and Challenges. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
8. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
9. Peerbasha, S., & Surputheen, M. M. (2021). Prediction of Academic Performance of College Students with Bipolar Disorder using different Deep learning and Machine learning algorithms. *International Journal of Computer Science & Network Security*, *21*(7), 350-358.
10. Vinod, H. C., & Niranjan, S. K. (2018, January). Multi-level skew correction approach for hand written Kannada documents. In *International Conference on Information Technology & Systems* (pp. 376-386). Cham: Springer International Publishing.
11. Thamilarasi, V., & Roselin, R. (2019). Lung segmentation in chest X-ray images using Canny with morphology and thresholding techniques. *Int. j. adv. innov. res*, *6*(1), 1-7.
12. Inbaraj, R., & Ravi, G. (2021). Content Based Medical Image Retrieval System Based On Multi Model Clustering Segmentation And Multi-Layer Perception Classification Methods. *Turkish Online Journal of Qualitative Inquiry*, *12*(7).
13. Arunachalam, S., Kumar, A. K. V., Reddy, D. N., Pathipati, H., Priyadarsini, N. I., & Ramisetti, L. N. B. (2025). Modeling of chimp optimization algorithm node localization scheme in wireless sensor networks. *Int J Reconfigurable & Embedded Syst*, *14*(1), 221-230.
14. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
15. Peerbasha, S., & Surputheen, M. M. (2021). A Predictive Model to identify possible affected Bipolar disorder students using Naive Baye's, Random Forest and SVM machine learning techniques of data mining and Building a Sequential Deep Learning Model using Keras. *International Journal of Computer Science & Network Security*, *21*(5), 267-274.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

16. Vinod, H. C., Niranjan, S. K., & Aradhya, V. M. (2014, November). An application of Fourier statistical features in scene text detection. In *2014 International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1154-1159). IEEE.
17. Thamilarasi, V., & Roselin, R. (2019). Automatic thresholding for segmentation in chest X-ray images based on green channel using mean and standard deviation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(8), 695-699.
18. Inbaraj, R., & Ravi, G. (2021). Multi Model Clustering Segmentation and Intensive Pragmatic Blossoms (Ipb) Classification Method based Medical Image Retrieval System. *Annals of the Romanian Society for Cell Biology*, *25*(3), 7841-7852.
19. Saravanan, V., Upender, T., Ruby, E. K., Deepalakshmi, P., Reddy, D. N., & SN, A. (2024, October). Machine Learning Approaches for Advanced Threat Detection in Cyber Security. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
20. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
21. Naveen, I. G., Peerbasha, S., Fallah, M. H., Jebaseeli, S. K., & Das, A. (2024, October). A machine learning approach for wastewater treatment using feedforward neural network and batch normalization. In *2024 First International Conference on Software, Systems and Information Technology (SSITCON)* (pp. 1-5). IEEE.
22. Vinod, H. C., Niranjan, S. K., & Anoop, G. L. (2013). Detection, extraction and segmentation of video text in complex background. *International Journal on Advanced Computer Theory and Engineering*, *5*, 117-123.
23. Asaithambi, A., & Thamilarasi, V. (2023, March). Classification of lung chest X-ray images using deep learning with efficient optimizers. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0465-0469). IEEE.
24. Inbaraj, R., & Ravi, G. (2020). Content Based Medical Image Retrieval Using Multilevel Hybrid Clustering Segmentation with Feed Forward Neural Network. *Journal of Computational and Theoretical Nanoscience*, *17*(12), 5550-5562.
25. Reddy, D. N., Venkateswararao, P., Vani, M. S., Pranathi, V., & Patil, A. (2025). HybridPPI: A Hybrid Machine Learning Framework for Protein-Protein Interaction Prediction. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(2).
26. Gangadhar, C., Chanthirasekaran, K., Chandra, K. R., Sharma, A., Thangamani, M., & Kumar, P. S. (2022). An energy efficient NOMA-based spectrum sharing techniques for cell-free massive MIMO. *International Journal of Engineering Systems Modelling and Simulation*, *13*(4), 284-288.
27. Peerbasha, S., Iqbal, Y. M., Surputheen, M. M., & Raja, A. S. (2023). Diabetes prediction using decision tree, random forest, support vector machine, k-nearest neighbors, logistic regression classifiers. *JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH*, *5*(4), 42-54.
28. Vinod, H. C., & Niranjan, S. K. (2020). Camera captured document de-warping and de-skewing. *Journal of Computational and Theoretical Nanoscience*, *17*(9-10), 4398-4403.
29. Thamilarasi, V., & Roselin, R. (2021). U-NET: convolution neural network for lung image segmentation and classification in chest X-ray images. *INFOCOMP: Journal of Computer Science*, *20*(1), 101-108.
30. Rao, A. S., Reddy, Y. J., Navya, G., Gurrapu, N., Jeevan, J., Sridhar, M., ... & Anand, D. High-performance sentiment classification of product reviews using GPU (parallel)-optimized ensembled methods.
31. Peerbasha, S., Habelalmateen, M. I., & Saravanan, T. (2025, January). Multimodal Transformer Fusion for Sentiment Analysis using Audio, Text, and Visual Cues. In *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1-6). IEEE.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

32. Vinod, H. C., & Niranjan, S. K. (2018, August). Binarization and segmentation of Kannada handwritten document images. In *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 488-493). IEEE.
33. Thamilarasi, V., Naik, P. K., Sharma, I., Porkodi, V., Sivaram, M., & Lawanyashri, M. (2024, March). Quantum computing-navigating the frontier with Shor's algorithm and quantum cryptography. In *2024 International conference on trends in quantum computing and emerging business technologies* (pp. 1-5). IEEE.
34. Kamatchi, S., Preethi, S., Kumar, K. S., Reddy, D. N., & Karthick, S. (2025, May). Multi-Objective Genetic Algorithm Optimised Convolutional Neural Networks for Improved Pancreatic Cancer Detection. In *2025 3rd International Conference on Data Science and Information System (ICDSIS)* (pp. 1-7). IEEE.
35. Abdul Samad, S. R., Ganesan, P., Al-Kaabi, A. S., Rajasekaran, J., & Basha, P. S. (2024). Automated Detection of Malevolent Domains in Cyberspace Using Natural Language Processing and Machine Learning. *International Journal of Advanced Computer Science & Applications*, *15*(10).
36. Vinod, H. C., & Niranjan, S. K. (2017, November). De-warping of camera captured document images. In *2017 IEEE International Symposium on Consumer Electronics (ISCE)* (pp. 13-18). IEEE.
37. Thamilarasi, V., & Roselin, R. (2019). Survey on Lung Segmentation in Chest X-Ray Images. *The International Journal of Analytical and Experimental Modal Analysis*, 1-9.
38. Nimma, D., Rao, P. L., Ramesh, J. V. N., Dahan, F., Reddy, D. N., Selvakumar, V., ... & Jangir, P. (2025). Reinforcement Learning-Based Integrated Risk Aware Dynamic Treatment Strategy for Consumer-Centric Next-Gen Healthcare. *IEEE Transactions on Consumer Electronics*.
39. Peerbasha, S., Alsalami, Z., Almusawi, M., Sheeba, B., & Malathy, V. (2024, November). An Intelligent Personalized Music Recommendation System Using Content-Based Filtering with Convolutional Recurrent Neural Network. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1-5). IEEE.
40. Kakde, S., Pavitha, U. S., Veena, G. N., & Vinod, H. C. (2022). Implementation of A Semi-Automatic Approach to CAN Protocol Testing for Industry 4.0 Applications. *Advances in Industry 4.0: Concepts and Applications*, *5*, 203.
41. Thamilarasi, V., Asaithambi, A., & Roselin, R. (2025). ENHANCED ENSEMBLE SEGMENTATION OF LUNG CHEST X-RAY IMAGES BY DENOISING AUTOENCODER AND CLAHE. *ICTACT Journal on Image & Video Processing*, *15*(3).
42. Madhumathy, P., Saravanakumar, R., Umamaheswari, R., Juliette Albert, A., & Devasenapathy, D. (2024). Optimizing design and manufacturing processes with an effective algorithm using anti-collision enabled robot processor. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *18*(8), 5469-5477.
43. Boopathy, D., & Balaji, P. (2023). Effect of different plyometric training volume on selected motor fitness components and performance enhancement of soccer players. *Ovidius University Annals, Series Physical Education and Sport/Science, Movement and Health*, *23*(2), 146-154.
44. Raja, M. W., & Nirmala, D. K. (2016). Agile development methods for online training courses web application development. *International Journal of Applied Engineering Research ISSN*, 0973-4562.
45. Vidyabharathi, D., Mohanraj, V., Kumar, J. S., & Suresh, Y. (2023). Achieving generalization of deep learning models in a quick way by adapting T-HTR learning rate scheduler. *Personal and Ubiquitous Computing*, *27*(3), 1335-1353.
46. Niasi, K. S. K., Kannan, E., & Suhail, M. M. (2016). Page-level data extraction approach for web pages using data mining techniques. *International Journal of Computer Science and Information Technologies*, *7*(3), 1091-1096.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

47. Thamilarasi, V. A Detection of Weed in Agriculture Using Digital Image Processing. *International Journal of Computational Research and Development, ISSN*, 2456-3137.
48. Sureshkumar, T. (2015). Usage of Electronic Resources Among Science Research Scholars in Tamil Nadu Universities A Study.
49. Arul Selvan, M. (2025). Detection of Chronic Kidney Disease Through Gradient Boosting Algorithm Combined with Feature Selection Techniques for Clinical Applications.
50. Shylaja, B., & Kumar, S. (2018). Traditional versus modern missing data handling techniques: An overview. *International Journal of Pure and Applied Mathematics*, *118*(14), 77-84.
51. Sureshkumar, T., Charanya, J., Kumaresan, T., Rajeshkumar, G., Kumar, P. K., & Anuj, B. (2024, April). Envisioning Educational Success Through Advanced Analytics and Intelligent Performance Prediction. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1649-1654). IEEE.
52. Niasi, K. S. K., & Kannan, E. Multi Agent Approach for Evolving Data Mining in Parallel and Distributed Systems using Genetic Algorithms and Semantic Ontology.
53. Jaishankar, B., Ashwini, A. M., Vidyabharathi, D., & Raja, L. (2023). A novel epilepsy seizure prediction model using deep learning and classification. *Healthcare analytics*, *4*, 100222.
54. Raja, M. W. (2024). Artificial intelligence-based healthcare data analysis using multi-perceptron neural network (MPNN) based on optimal feature selection. *SN Computer Science*, *5*(8), 1034.
55. Boopathy, D., & Balaji, D. P. Training outcomes of yogic practices and aerobic dance on selected health related physical fitness variables among tamilnadu male artistic gymnasts. *Sports and Fitness*, *28*.
56. Saravana Kumar, R., & Tholkappia Arasu, G. (2017). Rough set theory and fuzzy logic based warehousing of heterogeneous clinical databases. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *25*(03), 385-408.
57. Boopathy, D. Training Outcomes Of Yogic Practices And Plyometrics On Selected Motor Fitness Among The Men Artistic Gymnasts.
58. Raja, M. W., & Nirmala, K. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY AN EXTREME PROGRAMMING METHOD FOR E-LEARNING COURSE FOR WEB APPLICATION DEVELOPMENT.
59. Hamed, S., Mesleh, A., & Arabiyyat, A. (2021). Breast cancer detection using machine learning algorithms. *International Journal of Computer Science and Mobile Computing*, *10*(11), 4-11.
60. Boopathy, D., & Balaji, D. P. Research Paper Open Access.
61. Kaladevi, A. C., Saravanakumar, R., Veena, K., Muthukumaran, V., Thillaiarasu, N., & Kumar, S. S. (2022). Data analytics on eco-conditional factors affecting speech recognition rate of modern interaction systems. *Journal of Mobile Multimedia*, *18*(4), 1153-1176.
62. Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D. (2023). RETRACTED: Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. Journal of Intelligent & Fuzzy Systems, 45(4), 6145-6160.
63. Banu, S. S., Niasi, K. S. K., & Kannan, E. (2019). Classification Techniques on Twitter Data: A Review. *Asian Journal of Computer Science and Technology*, *8*(S2), 66-69.
64. Sureshkumar, T., & Hussain, A. A. Digital Library Usage of Research in the field of Physical Education and Sports.
65. Boopathy, D., Balaji, D. P., & Dayanandan, K. J. THE TRAINING OUTCOMES OF COMBINED PLYOMETRICS AND YOGIC PRACTICES ON SELECTED MOTOR FITNESS VARIABLES AMONG MALE GYMNASTS.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 October 2025 doi:10.20944/preprints202510.0417.v1

66. Charanya, J., Sureshkumar, T., Kavitha, V., Nivetha, I., Pradeep, S. D., & Ajay, C. (2024, June). Customer Churn Prediction Analysis for Retention Using Ensemble Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-10). IEEE.
67. Dhanwanth, B., Saravanakumar, R., Tamilselvi, T., & Revathi, K. (2023). A smart remote monitoring system for prenatal care in rural areas. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(3), 30-36.
68. Boopathy, D., & PrasannaBalaji, D. EFFECT OF YOGASANAS ON ARM EXPLOSIVE POWER AMONG MALE ARTISTIC GYMNASTS.
69. Lavanya, R., Vidyabharathi, D., Kumar, S. S., Mali, M., Arunkumar, M., Aravinth, S. S., ... & Tesfayohanis, M. (2023). [Retracted] Wearable Sensor-Based Edge Computing Framework for Cardiac Arrhythmia Detection and Acute Stroke Prediction. *Journal of Sensors*, *2023*(1), 3082870.
70. Selvam, P., Faheem, M., Dakshinamurthi, V., Nevgi, A., Bhuvaneswari, R., Deepak, K., & Sundar, J. A. (2024). Batch normalization free rigorous feature flow neural network for grocery product recognition. *IEEE Access*, *12*, 68364-68381.
71. Mubsira, M., & Niasi, K. S. K. (2018). Prediction of Online Products using Recommendation Algorithm.
72. Vidyabharathi, D., & Mohanraj, V. (2023). Hyperparameter Tuning for Deep Neural Networks Based Optimization Algorithm. *Intelligent Automation & Soft Computing*, *36*(3).
73. Lalitha, T., Kumar, R. S., & Hamsaveni, R. (2014). Efficient key management and authentication scheme for wireless sensor networks. *American Journal of Applied Sciences*, *11*(6), 969.
74. Saravanakumar, R., & Nandini, C. (2017). A survey on the concepts and challenges of big data: Beyond the hype. *Advances in Computational Sciences and Technology*, *10*(5), 875-884.
75. Boopathy, D., & Prasanna, B. D. IMPACT OF PLYOMETRIC TRAINING ON SELECTED MOTOR FITNESS VARIABLE AMONG MEN ARTISTIC GYMNASTS.
76. Niasi, K. S. K., & Kannan, E. (2016). Multi Attribute Data Availability Estimation Scheme for Multi Agent Data Mining in Parallel and Distributed System. *International Journal of Applied Engineering Research*, *11*(5), 3404-3408.
77. Marimuthu, M., Vidhya, G., Dhaynithi, J., Mohanraj, G., Basker, N., Theetchenya, S., & Vidyabharathk, D. (2021). Detection of Parkinson's disease using Machine Learning Approach. *Annals of the Romanian Society for Cell Biology*, *25*(5), 2544-2550.
78. Kumar, R. S., & Arasu, G. T. (2015). Modified particle swarm optimization based adaptive fuzzy k-modes clustering for heterogeneous medical databases. *J. Sci. Ind. Res*, *74*(1), 19-28.
79. Shylaja, B., & Kumar, R. S. (2022). Deep learning image inpainting techniques: An overview. *Grenze Int J Eng Technol*, *8*(1), 801.
80. Boopathy, D., Singh, S. S., & PrasannaBalaji, D. EFFECTS OF PLYOMETRIC TRAINING ON SOCCER RELATED PHYSICAL FITNESS VARIABLES OF ANNA UNIVERSITY INTERCOLLEGIATE FEMALE SOCCER PLAYERS. *EMERGING TRENDS OF PHYSICAL EDUCATION AND SPORTS SCIENCE*.
81. Revathy, G., Ramalingam, A., Karunamoorthi, R., & Saravanakumar, R. (2021). Prediction of long cancer severity with computational intelligence in COVID'19 pandemic.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.