Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4 (2025)

The Convergence of IoT and Blockchain in Supply Chain Monitoring: A Holistic Approach to Data Integrity, Automation, and Cybersecurity

Dr. Kakarlamudi V S Sudhakar[1]
[1]Associate Professor, Computer Science and Engineering, Keshav Memorial Engineering College, Osmania University Hyderabad, Telangana
sudhakarkvs20@gmail.com

Irshadullah Asim Mohammed[2]
[2]Supply Chain Project Manager at FuelCell Energy Inc., USA.
asim434@icloud.com

Dr. P. Nithya[3]
[3]Assistant Professor, School of Commerce, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India - 600062
drnithyap@veltech.edu.in

Dr. Asim Ray[4]
[4]Professor, Department of Management Studies, G L Bajaj Group of Institutions, Mathura
asim.ray2012@gmail.com

Dr. Christabell Joseph[5]
[5]Associate Professor, School of Law, Christ (Deemed to be University), Bangalore.
christabell.joseph@christuniversity.in

Dr. Aaquil Bunglowala[6]
[6]Professor and Director, Sri Aurobindo Institute of technology Indore, Madhya Pradesh, India
aaquilbun@gmail.com

Abstract:

The introduction of the Internet of Things (IoT) and the Blockchain technology is a ground-breaking paradigm of the contemporary supply chain management. In this paper, the convergence is discussed in a holistic way, focusing on its potential to become synergistic and providing an undisputable basis of data integrity, provide trust less automation, using smart contracts, and improve the cybersecurity postures significantly. As the IoT devices create large, real-time streams of data about the location, condition, and status of goods, blockchain offers a decentralized and tamper-evident registry to store this information, and thus establish its validity and establish a single source of truth within multi-party and multi-faceted networks. The research design that is used in this study is an empirical study design because it investigates the effectiveness of this fusion in solving the perennial supply chain challenges, which include: being opaque, fraud, inefficient and prone to cyber-attacks. In addition, it explores the new role of Artificial Intelligence (AI) and machine learning as the enabling factors that streamline IoT data analytics and blockchain functions. The discussion then generalizes the research on architectural paradigms, performance measures and implementation obstacles, and concludes that the IoT-Blockchain-AI triad is needed to create resilient, transparent, and intelligent supply chains that can self-operate and demonstrate compliance. Nevertheless, issues concerning the scalability, interoperability, energy usage, and the alignment with the regulatory requirements have to be tackled systematically to be widely adopted.

Keywords: Internet of Things (IoT), Blockchain, Supply Chain Management, Data Integrity, Smart Contracts, Cybersecurity, Decentralized AI, Automation, Trustless Systems.

Introduction:

Global supply chains have become complex systems that involve many jurisdictions and participants, including suppliers of raw materials or final consumers. This complexity brings severe vulnerabilities: absence of transparency, vulnerability to counterfeiting and fraud, manual work is inefficient, and there are high risks of cybersecurity attacks (Sharma, Srivastva, and Fatima, 2023). There is an inherent tendency in traditional centralized systems of data management to form information silos, distrust between stakeholders, and single points of failure, which are subject to manipulation or attack.

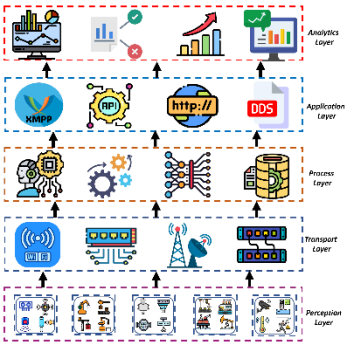

Fig 1. Blockchain in IoT Cybersecurity

The answer to this dilemma lies in the concurrent development of two disruptive technologies the Internet of Things (IoT) and Blockchain. The IoT enables the omnipresent sensing and digitalization of the physical world in which the sensors provide real-time data related to such parameters as temperature, humidity, shock, and position (Singh et al., 2025). However, IoT ecosystems have security and scaling problems. A blockchain is a decentralized and distributed ledger technology that is impossible to audit, transparent, and cross-examine because of cryptographic hashing and consensus algorithms (Chavali et al., 2024). The second invention it is based on is the power to believe without believing. The symbiotic relationship between the IoT and blockchain is very high. IoT provides the physical world with verifiable and time-stamped data to the blockchain and blockchain secures that data, providing a trusted history that all are allowed to view. It is the premise of so-called trustless automation of smart contracts, a self-executable code that is executed when preconditions are met by the IoT data (Shinde, Seth, and Kadam, 2023). In the next generation of monitoring the supply chain, the paper assumes an all-encompassing solution to integrating IoT and blockchain should also be provided. It goes further than just the idea of technology juxtaposition to imply a system whose design is its own data integrity, automated process automation and cyber resiliency. The article presents its study using literature review, empirical methodology, detailed analysis using models and equations, implications discussion, and conclusion synthesis. It also incorporates the much-needed element of the Artificial Intelligence (AI) to act as an intelligent interface to crunch the IoT data, enhance the blockchain functionality, and advance the predictive capability (Zuo, 2024; Hussain and Al-Turjman, 2021) with.

Literature Review:

The academic literature about the IoT, blockchain and supply chains is diverse and complex. Initial studies were based on the standalone use of the technologies. The functions of IoT in logistics relating to asset tracking and monitoring of their condition are not novel (Rane, 2023), and the opportunities of blockchain in provenance tracing in such industries as food and pharmaceuticals are discussed many times already (Kumar et al., 2022).

The recent literature has changed to their integration. Shinde, Seth, and Kadam (2023) offer an extensive overview of the integration of blockchain with AI, ML, and IoT, with the examples of supply chain, healthcare, and smart cities. They single out the data integrity and automated settlements as core advantages. Likewise, Zuo (2024) views the two-way synergy, i.e. AI optimizes blockchain and blockchain optimizes AI. One of the important ones is the improvement of cybersecurity. Meduri (2024) studies the application of fraud detection in the banking industry, which is applicable to unearthing anomalies in the supply chain financial deals made on-chain. Particularly, Venkatesan and Rahayu (2024) suggest using hybrid consensus mechanisms and machine learning to enhance the security of blockchain against such attacks as 51 per cent attacks. Vedula, Venkatakrishnan, and Gupta (2023) touch upon the issue of transaction reordering attacks (MEV) which is a subtle security risk in blockchain systems that may affect the equitability of supply chain transactions.

The enabling layer of AI and Machine Learning (ML) is important. Sarker (2022) describes the AI-based modelling methods of constructing automation and intelligent systems. This can be applied in supply chains to predictive analytics in demand forecasting, dynamic routing and predictive asset maintenance (Khanal et al., 2023). Decentralized or blockchain-based concept of AI is on the rise to eliminate the threat of centralization. Lo et al. (2022) suggest accountability and fairness solution in Federated Learning systems as a blockchain-based architecture, which can be applied to collaborative, privacy-preserving supply chain analytics. Alsagheer et al., (2023) and Gaddam (2024) address the governance and opportunities, along with challenges of decentralized machine learning, and the importance of trusted and transparent AI models in the context of multi-stakeholder, such as supply chain.

Besides, studies have also explored the barriers of implementation. Interpretive Structural Modeling (ISM) is used by Chavali et al. (2024) to examine the obstacles to blockchain in finance and construction, respectively, with technological complexity, regulatory unpredictability, and high initial costs being identified. The results have a direct implication on the application of IoT-blockchain integration in supply chains.

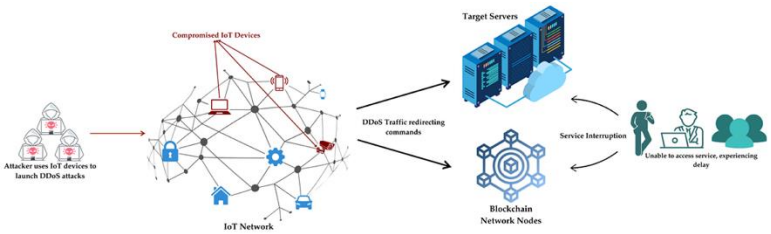

Fig 2. Blockchain-Enabled Supply Chain Management

In the marketing and customer viewpoint, the analytics on secured IoT information, which is AI-powered, can transform interaction. Islam, Shawon, and Sumsuzoha (2023) and Thirumagal et al. (2024) cover personalized marketing with the help of ML that can be optimized with high-integrity supply chain data to better predict the consumer demand. Haque, Islam, and Mohtasim (2024) and Tabianan, Velu, and Ravi (2022) discuss customer-focused analytics and smart segmentation, which is based on reliable streams of data that can be offered by a blockchain-supported IoT system.Ussatova et al. (2022) apply ML algorithms to the classification of DDoS attacks in the context of cybersecurity, which is a threat applicable to the IoT network as well as blockchain nodes. Saleh (2024) gives an overview of blockchain to secure and decentralized AI in cybersecurity, forming a vision that will be highly useful in securing supply chain cyber-physical systems. Thus, Alabdulatif et al. (2023) and Le, Truong, and Le (2024) introduce frameworks in e-health and the metaverse, respectively, where blockchain keeps data safe and AI gives insights, which is a blueprint that may be adjusted to supply chain monitoring.This review affirms that the triad of IoT, Blockchain, and AI is considered potent; however, the overall study of its concerted implementation to the end-to-end monitoring of the supply chain, including data integrity, automation, and cybersecurity, as the pillars of a case, is considered to be a relevant research area.

Methodology:

This paper will follow empirical research design because it aims to explore the overlap of IoT and Blockchain in monitoring the supply chain. An empirical approach is selected to base the research in an observable evidence, practical architectures and quantifiable performance measures based on established implementations, pilot projects and simulated studies reported in literature.

The methodology can be divided into the following three stages:

Systematic Evidence Collection: A systematic review of academic literature, white papers in the industry, and case studies was carried out to obtain empirical data of existing or planned IoT-blockchain systems (Meenal, 2025). This involved the examination of reported results on the accuracy of data, process efficiency improvement, decrease in fraud cases, and security improvement.

Architectural and Model Analysis: Generalized, holistic, architectural model of IoT- blockchain supply chain integration was derived on the basis of evidence that has been obtained. This phase was comprised of breaking down successful implementations in order to acquire common components, data streams and consensus algorithms. Besides, analytical and machine learning models that can be applied to the framework of system performance were also reviewed, which led to the creation of the necessary equations to implement integrity assurance and predictive analytics that can support the functioning of the system.

Comparative Performance Evaluation: The empirical data of different studies collected were put in comparative tables. The factors that are put into consideration in these tables are the suitability of different consensus algorithms to the limitations of an IoT-blockchain, the suitability of different AI/ML models to the supply chain data, and a qualitative evaluation of the obstacles to implementation and its strength. This tripartite approach allows making multi-dimensional analysis, and the ontological architecture is replaced by the quantitative modelling and realistic evaluation of challenges.

Analysis:

Holistic Architectural Model:

An integrated IoT-Blockchain-AI architecture of monitoring supply chains includes four layers:

Physical/IoT Layer: It contains RFID tags, GPS sensors and environmental as temperature sensors on the assets/packages. They gather and relay real time data to the gateway devices.

Blockchain & Security Layer: IoT data are cryptographically signed and submitted to a blockchain network by oracles, which are typically gateway devices or dedicated nodes as it is common to use permissioned, asHyperledger Fabric, when enterprise supply chains are involved. This layer allows the business logic to be encoded in smart contracts as"if temperature exceed 10C and take more than 1 hour, send an alert and pause payment.

AI & Analytics Layer: This layer subscribes to on-chain and off-chain streams of data. ML models are used to perform analytics asspoilage prediction, demand forecasting (Hoque et al., 2024), as well as logistics optimization (Ristimaki, 2022). The training of models with distributed data can be implemented by using federated learning (Lo et al., 2022).

Application & Interface Layer: Offers stakeholder dashboards that the stakeholders (suppliers, logistics providers, retailers, regulators) can use to see the provenance, condition, and compliance of goods in close real-time with verifiable evidence.

Consensus Mechanism	Suitability for IoT/Supply Chain	Key Advantages	Key Drawbacks
Proof of Work (PoW)	Low	High security, decentralization.	Extremely high energy cost, slow throughput, unsuitable for IoT device participation.
Proof of Stake (PoS)	Medium	Lower energy consumption, faster than PoW.	Potential for centralization; wealth-based influence.
Practical Byzantine Fault Tolerance (PBFT)	High	High throughput, low latency, finality. Efficient for permissioned networks.	Scalability issues with large node count; communication overhead.
Proof of Authority (PoA)	High	Very fast, low resource consumption. Ideal for trusted enterprise consortiums.	Centralized trust in validators; not fully permission less.
Delegated Proof of Stake (DPoS)	Medium-High	Scalable, energy-efficient.	Relies on a small set of elected delegates, semi-centralized.

Table 1: Comparison of Consensus Mechanisms for IoT-Blockchain Supply Chains

(Source: Self-developed)

Equation 1: Data Integrity Assurance Score

The security level of the data trail of an asset can be specified as a result of the indelibility of its records. A basic measurement can be stipulated:

$$I\_asset = \Sigma (w\_i * H(T\_i || D\_i || H\_prev))$$

Where:

- I asset = Integrity score of asset history.
- w i = weight of the ith event recorded ascustom clearance weight more than a routine ping of the location p.
- H() = Cryptographic hash asSHA-256.
- T i, D i T i, D i Timestamp and Data of event i.
- H a: H a: Hash of the last block/event, the link in the chain.
- The concept behind this equation is that the hashing of blockchain would form a tamper evident chain; any hashes would drastically impact I_asset because any modification will change all further hashes.

Role of AI and Machine Learning:

The intellect of this system is AI.

Predictive Analytics: Time-series forecasting algorithms asProphet, XGBoost can be used to forecast Estimated Times of Arrival (ETAs) or possible delay (Khanal et al., 2023). The downstream sales information can also be used by AI in predicting demand spikes (secured on-chain), and this allows it to proactively manage inventory (Meenal, 2025).

Anomaly Detection: Sensor data streams can also be analyzed through unsupervised learning models asIsolation Forest, Autoencoders to identify anomalies that reveal the presence of theft asunusual route selection, spoilage as insensible temperature change, and tampering (Meduri, 2024). These exceptions may automatically cause smart contract provisions.

Optimization: Reinforcement Learning has the ability to optimize dynamic parameters such as the transportation path, warehouse choice, and carrier assortment based on the current circumstances and economical restrictions (Sarker, 2022).

Supply Chain Function	AI/ML Model Examples	Purpose	Data Source
Demand Forecasting	SARIMA, Prophet, LSTM Networks	Predict product demand at different nodes.	Historical sales data (on-chain), market trends.
Predictive Maintenance	Regression Models, CNNs on vibration/audio data	Predict failure of vehicles or storage equipment.	IoT sensor data from assets.
Fraud & Anomaly Detection	Isolation Forest, K-means Clustering, Supervised Classifiers	Identify counterfeit goods, false documentation, route deviations.	IoT GPS/temperature logs, document hash records on BC.
Personalized Marketing	Collaborative Filtering, Association Rule Mining (Market Basket Analysis)	Recommend products, optimize promotions (Thirumagal et al., 2024; Hoque et al., 2024).	Customer purchase history (with privacy protocols).
Dynamic Pricing & Procurement	Reinforcement Learning	Optimize pricing strategies and supplier selection based on real-time demand and supply ledger data.	On-chain inventory levels, supplier performance history.

Table 2: Application of AI/ML Models in Integrated Supply Chain (Source: Self-developed)

Equation 2: Anomaly Detection Threshold for Sensor Data

An example expression of the simplified model of triggering an alert of an IoT sensor stream can be stated as:

$$Alert\_triggered\ IF: |(X\_t - \hat{Y}\_t)| / \sigma\_residual > \tau$$

Where:

- X_t = Actual sensor reading at time t.
- $\hat{Y}$_t = Predicted value at time t from a time-series ML model asARIMA, LSTM.
- σ_residual = Standard deviation of the model's historical prediction residuals.
- τ = A configurable threshold (as 3 for a "3-sigma" rule). If true, this event (Alert_triggered) and the associated sensor data X_t are signed and written to the blockchain as an immutable incident record.

Cybersecurity Enhancement:

The convergence is something that enhances cybersecurity in a natural way:

Data Integrity and Non- Repudiation: The Cryptographic hashing guarantees that the information cannot be modified in the past. Signing is done on each transaction giving non-repudiation.

Decentralization: Removes points of failure. The network is not compromised when one node is attacked using a DDoS attack (Ussatova et al., 2022).

Secure Identity Management: Decentralized identifiers (DID) can be placed on the blockchain on devices and participants, which minimizes identity spoofing.

AI to Threat Detection: ML models may analyze the blockchain network (especially smart contract exploitation attempts, suspicious transaction flows, etc.) (Venkatesan and Rahayu, 2024; Saleh, 2024).

Barrier Category	Specific Challenges	Potential Mitigations
Technological	Scalability & Throughput of BC; IoT-BC Interoperability; AI Model Complexity & Integration.	Use of hybrid/off-chain architectures assidechains; Standardized APIs & protocols; MLOps and "Blockchain for AI" frameworks (Le et al., 2024).
Financial & Operational	High Initial Capital & Operational Costs; Energy Consumption of certain BC protocols; Lack of ROI clarity.	Consortium-based cost-sharing; Adoption of energy-efficient consensus (PoA, PoS); Pilot projects to demonstrate ROI in fraud reduction.
Organizational & Regulatory	Lack of Standardization & Governance; Regulatory Uncertainty; Resistance to Change & Skill Gaps.	Development of industry-specific consortia and standards asIBM Food Trust; Engagement with regulators; Training and phased implementation.

Table 3: Assessment of Implementation Barriers (Source: Self-developed)

The discussion shows that IoT, Blockchain, and AI are a synergistic supply chain architecture. IoT offers physical information in real-time, blockchain guarantees its integrity and allows automated smart contracts, and AI derives predictive information. The main points are that the best consensus mechanisms such as PBFT or PoA are applicable to the enterprise, the ML models can be used to predict and investigate anomalies, and decentralized models and cryptographic auditing can be utilized to improve cybersecurity. Nevertheless, there are still major obstacles on the way

to adoption that are mostly related to technological scalability, system interoperability, and organizational resistance, which is why hybrid architectures and industry consortia are the only possible ways to implement them.

Discussion:

The discussion has confirmed the fact that the concerted effort of employment of IoT, Blockchain, and AI refines a supply chain environment that is bigger than the summation of its components. The audit trail that blockchain provides cannot be changed, thus make the IoT data more than a piece of information and it becomes reality, which the competitors within the network cannot duplicate. Smart contracts automatize paper-based complex operations, reducing administrative burdens and decreasing the settlement time to a matter of minutes.AI integration works with one of the primary drawbacks of raw blockchain; the system is a great system of record but not a system of insight (Gaddam, 2024). The information extracted with the help of AI/ML models recognizes predictive and prescriptive intelligence in the secured data and enables proactive management rather than reactive management. This is per the aspiration of autonomous supply chains. And yet there are hard battles in this integration.The IoT scenarios of producing large volumes of data increase scalability trilemma of blockchain (decentralization, security, scalability). Maintaining all sensor measurements on-chain is not viable. Hybrid systems, including storing exclusively vital hashes and alterations of the state on-chain and bulk data on off-chain secure storage will be required (Shinde et al., 2023). The greatest problem is the interoperability, which requires data format standardization, communication protocols among heterogeneous IoT devices and other blockchain platforms, and cross-chain communication among supply chains of multi-ecosystem.

Though being an advantage of the decentralized AI paradigm, its privacy and the ability to ensure trust is a favorable characteristic of the model, but there is a disadvantage of complexity when it was applied to govern the model, training, and ensure performance of the model consistency across nodes (Alsagheer et al., 2023). Moreover, the regulatory climate is not developed. Problems with legal admissibility of blockchain records, liability of smart contracts bugs, and data privacy regulations that are not compatible with blockchain immutability shall be addressed (Chavali et al., 2024).The architecture considers a majority of the traditional threats with respect to cybersecurity, but it brings in new attack vectors. They include the risk of the smart contract code, the attack on the IoT gateway as an oracle (providing the chain with false data), and the consensus mechanism breach with permissioned networks (Venkatesan and Rahayu, 2024). It must have the defence in depth approach, which implies the inherent safety of blockchain and AI-enhanced intrusion detection and the hardening of hardware security of the IoT (Zuo, 2024).

Lastly, transformation must rely on a psychological shift in the distribution of competitive secrecy in favour of a competitive openness. These systems can only be effective in the establishment of industry associations that co-evolves the forms of governance, cost sharing and agreeing on standards to convert the technological potential into practicable, industry-wide utility.

Conclusion:

This paper has presented the detailed discussion about the convergence of IoT and Blockchain to supply chain monitoring which is augmented with the significant capabilities of Artificial Intelligence. The empirical research demonstrates that the triad can address the most urgent problems of the modern supply chains: it is capable of building an unbreakable chain of custody when it comes to the data integrity, can be effectively used in trustless and automated processes with the help of smart contracts, and is capable of building a stronger cybersecurity framework to combat fraud and manipulation.

The proposed integration can not only be limited to tracking to enable truly intelligent and self-directed supply chain operations. The application of the AI models structured on the received proved data base helps to provide more accurate predictive estimation, real-time optimization of logistics, and customer interaction. However, the path to success lies with the extent that it will be able to address the significant technological challenges of scale and interoperability, the problems of governance and cooperation in organizations, and create a positive regulatory climate.Potential research would include lightweight, energy efficient, consensus-based protocols to be executed with an IoT network, cross-platform interoperability standards, and general legal systems of enforcing smart contracts in the future. Moreover, the more advanced forms of decentralization AI such as the secure multi-party computation using the federated learning based on blockchains to ensure the maximum utility of the data gathered and ensure privacy will have to be pursued.

In sum, convergence of IoT, blockchain and AI are not a new upgrade to gain in the supply chain, but a paradigm shift towards transparent, efficient, secure and smart supply chains. Companies who will strategically approach the integration issues and ensure the holistic approach will be able to achieve the previously unimaginable operating resilience, trust and competitive advantage among stakeholders of the world market place. The physically-digitally-cryptographically seamless integration of the physical, digital, and cryptographic worlds is the future of the supply chain management.

Reference List:

1. Alabdulatif, A., Al Asqah, M., Moulahi, T. and Zidi, S., 2023. Leveraging artificial intelligence in blockchain-based e-health for safer decision making framework. Applied Sciences, 13(2), p.1035. https://www.mdpi.com/2076-3417/13/2/1035
2. Alsagheer, D., Xu, L. and Shi, W., 2023. Decentralized machine learning governance: Overview, opportunities, and challenges. IEEE Access, 11, pp.96718-96732. https://ieeexplore.ieee.org/abstract/document/10238468/
3. Chavali, K., VV, A.K., Mavuri, S., Tiwari, C.K. and Pal, A., 2024. Investigation and Modelling of Barriers in Adoption of Blockchain Technology for Accounting and Finance: An ISM Approach. *Journal of Global Information Management (JGIM)*, *32*(1), pp.1-23. https://www.igi-global.com/viewtitle.aspx?titleid=353960
4. Gaddam, S.K., 2024, November. Bridging Decentralized AI and Blockchain: Challenges and Solutions. In 2024 19th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP) (pp. 8-13). IEEE. https://ieeexplore.ieee.org/abstract/document/10859075/
5. Hammad, A. and Abu-Zaid, R., 2024. Applications of AI in Decentralized Computing Systems: Harnessing Artificial Intelligence for Enhanced Scalability, Efficiency, and Autonomous Decision-Making in Distributed Architectures. Applied Research in Artificial Intelligence and Cloud Computing, 7, pp.161-187. https://scholar.googleusercontent.com/scholar?q=cache:EgB0_tHyBs8J:scholar.google.com/+Decentralized+AI:+Leveraging+Blockchain+for+Trustworthy+Machine+Learning+Models+&hl=en&as_sdt=0,5&as_ylo=2021
6. Hoque, E.M.J., Islam, M.S. and Mohtasim, S.A., 2024. Optimizing decision-making through customer-centric market basket analysis. *Journal of Operational and Strategic Analytics*, *2*(2), pp.72-83.https://www.researchgate.net/profile/Engr-Md-Jiabul-Hoque/publication/380218474_Optimizing_Decision-Making_Through_Customer-Centric_Market_Basket_Analysis/links/665e8a5ad59c846ad430187c/Optimizing-Decision-Making-Through-Customer-Centric-Market-Basket-Analysis.pdf
7. Hussain, A.A. and Al-Turjman, F., 2021. Artificial intelligence and blockchain: A review. Transactions on emerging telecommunications technologies, 32(9), p.e4268. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4268
8. Islam, M.R., Shawon, R.E.R. and Sumsuzoha, M., 2023. Personalized marketing strategies in the US retail industry: leveraging machine learning for better customer engagement. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), pp.750-774.https://www.researchgate.net/profile/Saqib-Luqman/publication/385720670_Personalized_Marketing_Strategies_in_the_US_Retail_Industry_Leveraging_Machine_Learning_for_Better_Customer_Engagement/links/6732c6a668de5e5a30739b6a/Personalized-Marketing-Strategies-in-the-US-Retail-Industry-Leveraging-Machine-Learning-for-Better-Customer-Engagement.pdf
9. Khanal, I., Dhakal, O.P., Guragain, M.K., Karki, P. and Pandey, B., 2023. Comparative Analysis of Time Series Forecasting Models for Predicting PM2. 5 level in Kathmandu: SARIMA, Prophet and XGBoost.http://conference.ioe.edu.np/publications/ioegc14/IOEGC-14-170-PS2-001-138.pdf
10. Kumar, R., Arjunaditya, Singh, D., Srinivasan, K. and Hu, Y.C., 2022, December. AI-powered blockchain technology for public health: a contemporary review, open challenges, and future research directions. In *Healthcare* (Vol. 11, No. 1, p. 81). MDPI.https://www.mdpi.com/2227-9032/11/1/81
11. Le, H.D., Truong, V.T. and Le, L.B., 2024. Blockchain-empowered metaverse: Decentralized crowdsourcing and marketplace for trading machine learning data and models. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10530265
12. Lo, S.K., Liu, Y., Lu, Q., Wang, C., Xu, X., Paik, H.Y. and Zhu, L., 2022. Toward trustworthy ai: Blockchain-based architecture design for accountability and fairness of federated learning systems. IEEE Internet of Things Journal, 10(4), pp.3276-3284. https://ieeexplore.ieee.org/abstract/document/9686048
13. Meduri, K., 2024. Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive*, *11*(2), pp.915-925.https://www.researchgate.net/profile/Karthik-Meduri/publication/379600459_Cybersecurity_threats_in_banking_Unsupervised_fraud_detection_analysis/links/66106c542034097c54f97ae8/Cybersecurity-threats-in-banking-Unsupervised-fraud-detection-analysis.pdf
14. Meenal, B., 2025. Forecasting Customer Invoice Settlement with behavioural analytics.https://www.researchsquare.com/article/rs-5858261/latest.pdf
15. Rane, N., 2023. Enhancing customer loyalty through Artificial Intelligence (AI), Internet of Things (IoT), and Big Data technologies: improving customer satisfaction, engagement, relationship, and experience. *Internet of Things (IoT), and Big Data Technologies: Improving Customer Satisfaction, Engagement, Relationship, and Experience (October 13, 2023)*.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4616051
16. Ristimäki, M., 2022. PRICING VARIABLES SPECIFICATION AND EFFECT ON THE TOTAL PRICE CONTRIBUTION IN SUBCONTRACTING.https://trepo.tuni.fi/bitstream/handle/10024/142555/RistimakiMikko.pdf?sequence=2

17. Saleh, A.M.S., 2024. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain: Research and Applications, p.100193. https://www.sciencedirect.com/science/article/pii/S209672092400006X
18. Sarker, I.H., 2022. AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. *SN computer science*, *3*(2), p.158.https://link.springer.com/article/10.1007/s42979-022-01043-x
19. Sharma, P., Sharma, M., Vijayanand, N., Prabhakaran, J., Sahu, D.N. and Choudhary, S., 2022. Category Management's Effects on Retail Business Profitability and Operations. *NeuroQuantology*, *20*(10), pp.4401-4413.https://www.researchgate.net/profile/Preeti-Sharma-78/publication/370264563_Category_Management's_Effects_on_Retail_Business_Profitability_and_Operations/links/6448b7b9d749e4340e388df9/Category-Managements-Effects-on-Retail-Business-Profitability-and-Operations.pdf
20. Sharma, R., Srivastva, S. and Fatima, S., 2023. E-commerce and digital transformation: Trends, challenges, and implications. *Int. J. Multidiscip. Res.(IJFMR)*, *5*, pp.1-9.https://pdfs.semanticscholar.org/9090/1ca619de45cfc8df70b1804923d497e8058e.pdf
21. Shinde, N.K., Seth, A. and Kadam, P., 2023. Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications. Machine Learning and Optimization for Engineering Design, pp.85-119. https://link.springer.com/chapter/10.1007/978-981-99-7456-6_7
22. Singh, A.R., Sujatha, M.S., Kadu, A.D., Bajaj, M., Addis, H.K. and Sarada, K., 2025. A deep learning and IoT-driven framework for real-time adaptive resource allocation and grid optimization in smart energy systems. *Scientific Reports*, *15*(1), p.19309.https://www.nature.com/articles/s41598-025-02649-w
23. Song, Y.X., Yang, X.D., Luo, Y.G., Ouyang, C.L., Yu, Y., Ma, Y.L., Li, H., Lou, J.S., Liu, Y.H., Chen, Y.Q. and Cao, J.B., 2023. Comparison of logistic regression and machine learning methods for predicting postoperative delirium in elderly patients: a retrospective study. CNS Neuroscience & Therapeutics, 29(1), pp.158-167.https://onlinelibrary.wiley.com/doi/pdf/10.1111/cns.13991
24. Tabianan, K., Velu, S. and Ravi, V., 2022. K-means clustering approach for intelligent customer segmentation using customer purchase behavior data. *Sustainability*, *14*(12), p.7243.https://www.mdpi.com/2071-1050/14/12/7243/pdf
25. Thirumagal, P.G., Bhattacharjee, K., Dorbala, R., Palav, M.R. and Mahajan, V., 2024, April. Application of Machine Learning Algorithms in Personalized Marketing. In 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) (pp. 165-170). IEEE.https://www.researchgate.net/profile/Rajesh-Dorbala/publication/382011085_Application_of_Machine_Learning_Algorithms_in_Personalized_Marketing/links/669788e4cb7fbf12a457808c/Application-of-Machine-Learning-Algorithms-in-Personalized-Marketing.pdf
26. Tian, B., He, L., Xu, Y., Fu, J. and Wu, H., 2025. Critical Success Factors for Blockchain Implementation in the AEC Industry: An Integrated ISM and DEMATEL Approach. *Engineering Management Journal*, pp.1-17. https://www.researchgate.net/profile/Yongshun_Xu/publication/389437962_Critical_Success_Factors_for_Blockchain_Implementation_in_the_AEC_Industry_An_Integrated_ISM_and_DEMATEL_Approach/links/67c25ad48311ce680c788405/Critical-Success-Factors-for-Blockchain-Implementation-in-the-AEC-Industry-An-Integrated-ISM-and-DEMATEL-Approach.pdf
27. Ural, O. and Yoshigoe, K., 2023. Survey on Blockchain-Enhanced Machine Learning. IEEE Access, 11, pp.145331-145362. https://ieeexplore.ieee.org/abstract/document/10366252
28. Ussatova, O., Zhumabekova, A., Begimbayeva, Y., Matson, E.T. and Ussatov, N., 2022. Comprehensive DDoS Attack Classification Using Machine Learning Algorithms. Computers, Materials & Continua, 73(1).https://www.academia.edu/download/101914029/pdf.pdf
29. Vedula, A., Venkatakrishnan, S.B. and Gupta, A., 2023. Masquerade: Simple and Lightweight Transaction Reordering Mitigation in Blockchains. *arXiv preprint arXiv:2308.15347*. https://arxiv.org/pdf/2308.15347
30. Venkatesan, K. and Rahayu, S.B., 2024. Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports*, *14*(1), p.1149.https://www.nature.com/articles/s41598-024-51578-7
31. Vinay, S.B., 2024. Identifying research trends using text mining techniques: A systematic review. *International Journal of Data Mining and Knowledge Discovery (IJDMKD)*, *1*(1), pp.1-11. https://lib-index.com/index.php/IJDMKD/article/view/IJDMKD_01_01_001/1278
32. Zuo, Y., 2024. Exploring the Synergy: AI Enhancing Blockchain, Blockchain Empowering AI, and their Convergence across IoT Applications and Beyond. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10769427