A Blockchain-Enabled Healthcare Supply Chain Management System for Product Traceability and Security

Dr. K. Satya Sandeep[1],K. Likitha Rani[2],N. Ayeesha[3],B. Rishitha[4],V. Jahnavi[5]

Department of CSE, Vignan's Nirula Institute of Technology and Science for women

Palakaluru, Guntur, 522009, Andhra Pradesh, India.

Abstract:

The growing complexity of worldwide healthcare supply networks requires transparent, secure, and trackable systems that ensure products are genuine and patients stay safe. Current centralized systems just can't provide enough security, tracking ability, and compatibility between different platforms, which leads to widespread fake medications, tampered data, and failed product recalls. To tackle these problems, this study introduces a blockchain-powered healthcare supply chain management system that improves how we track products, maintain data accuracy, and keep supply chains transparent. The suggested approach uses a consortium blockchain that works together with smart contracts, Internet of Things sensors, and external storage solutions to create a decentralized, secure, and streamlined way of managing data. Each batch of medical supplies gets a unique cryptographic signature using the SHA-256 method to ensure the information can't be changed or corrupted, while smart contracts automatically handle key tasks like registering batches, checking product authenticity, and removing access when needed. This approach lets everyone involved - from manufacturers and distributors to hospitals and patients - verify products are real, watch transactions happen live, and keep healthcare items secure throughout their journey from factory to patient. Testing shows that this blockchain system significantly outperforms traditional methods and existing blockchain medical record systems like Hyperledger and Ethereum in terms of speed, response time, tracking capabilities, and security. The framework also offers better scalability, uses less energy, reaches consensus faster, and maintains nearly perfect data accuracy and transaction completion rates. This work establishes a solid groundwork for future Healthcare 6.0 systems that prioritize decentralized trust, system compatibility, and putting patients in control of their data.

Keywords: Blockchain Technology, Healthcare Supply Chain, Product Traceability, Data Integrity, Smart Contracts, Off-chain Storage, Consortium Blockchain, IoT Integration, Healthcare 6.0, Cybersecurity, Transaction Efficiency, Decentralized Trust, Transparency, Data Provenance, Tamper-proof System

1.Introduction:

It is becoming more and more difficult for the global healthcare supply chain to maintain data integrity, openness, and patient, hospital, and distributor trust [1]. Generally speaking, centralized systems are susceptible to data manipulation, fake medications, and inefficient product recall [2]. From manufacturing to patient delivery, it is challenging for traditional systems to verify the validity and traceability of healthcare products due to the numerous middlemen they pass through [3]. In order to overcome these obstacles, blockchain technology has emerged as a ground-breaking technique for decentralizing trust and enabling safe, open, and verifiable data management [4] [5].

Blockchain is ideal for high-stakes sectors like healthcare, where security and transparency are crucial, because of its immutability, distributed consensus, and cryptographic validation capabilities [6] [7]. Previous studies have demonstrated the potential of blockchain technology for supply chain security and healthcare data management [8]. While Villarreal et al. (2023) identified interoperability and standardization problems in blockchain-enabled healthcare systems, Akkaoui et al. (2020) developed a hybrid edge-blockchain architecture that reduced medical data interchange latency [9] [10]. Subsequent research has looked into

integrating blockchain with AI and IoT to create intelligent and secure Healthcare 6.0 infrastructure, such as that done by Kumar et al. (2024) and Galety et al. [11].

These solutions facilitate real-time tracking across interconnected networks, improve data interchange, and safeguard patient privacy [12]. A blockchain-based healthcare supply chain management system based on a consortium blockchain enhanced with smart contracts is proposed in this study to complement these advancements [13]. The proposed architecture (Figure 1) enables hospitals and pharmacies to safely examine and distribute medications, producers to register and track product batches, and patients to verify the legitimacy of products and revoke access as needed [14]. For scalability, real-time traceability, and access control using smart contracts, the design makes use of off-chain storage [15] [16].

Trusted parties can use it to control access rights in verifiable transactions, anchor telemetry data, register batches, record transfers, and recall products [17] [18]. Only approved consortium members are permitted to carry out critical operations due to the contract's strict access restriction [19]. Off-chain storage integration also makes it easier to manage big health artifacts like compliance documents, digital certificates, and IoT information [20].

The proposed architecture uses a real healthcare dataset to simulate supply chain traceability, demonstrating how blockchain can be used to safeguard patients and ensure product history [21]. By ensuring that every transactionfrom manufacturing to patient dispensingis permanently documented and auditable, the system increases accountability and reduces the risk of counterfeit goods [22] [23]. The goal of this project is to create and implement a transparent, efficient, and impenetrable blockchain-enabled healthcare supply chain system [24]. The research makes it easier to build a dependable digital healthcare ecosystem for logistics by integrating blockchain, off-chain data management, and smart contract automation [25]. By fostering increased interoperability, automating recall procedures, and establishing patient-centered data governance, the system's design lays the foundation for Healthcare 6.0 networks of the future [26] [27].

2.Literature Survey:

Because blockchain technology offers decentralized, transparent, and impenetrable data management, it has emerged as a game-changing breakthrough in the healthcare sector [28]. Healthcare businesses may safely store and exchange sensitive patient and product information amongst verified entities thanks to its core properties of distributed consensus, cryptographic security [29], and immutability. Blockchain ensures that only verified parties can view timestamped and authenticated medical and supply chain data, which is crucial in a sector where privacy [30], interoperability, and trust are critical. Furthermore, the permanence of blockchain reduces the risk of counterfeit medications and facilitates efficient recall management by enabling transparent tracking of pharmaceutical products, medical equipment, and consumables [31].

In EdgeMediChain:[6-7] A Hybrid Edge Blockchain-Based architecture for Health Data Exchange, published in 2020, Akkaoui et al. [8] created a hybrid architecture that integrates blockchain technology and edge computing to improve data exchange performance and minimize latency by processing data near the source [32]. Similarly, standardization and interoperability were noted by Villarreal et al. [9-10] (2023) in Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security as the main barriers to the implementation of blockchain technology in healthcare management [33]. Their study emphasized how crucial standardized smart contract frameworks and scalable architectures are to enabling secure data sharing across multiple healthcare organizations [34] [35].

A model that combines artificial intelligence and Ethereum blockchain for detecting anomalies in Internet of Health Things (IoHT) networks was proposed by Olawale and Ebadinezhad et al. [11] (2024) in Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management. Both proactive and reactive security measures are strengthened by this collaboration. Kumar et al. [12] (2024) described how blockchain enhances the traceability and explainability of AI-based medical analytics with data integrity preservation in Confluence of Blockchain and Artificial Intelligence Technologies for Secure and Scalable Healthcare Solutions [36].

In Medical Data Security and Effective Organization using Integrated Blockchain Principles in AI-based Healthcare 6.0 Infrastructures, Galety et al. [13] (2025) explored how blockchain, AI, and IoT intersect to support secure data exchange and real-time decision-making in Healthcare 6.0 infrastructures [37]. To make blockchain possible for energy-constrained IoT medical equipment, Aboshosha et al. [14] (2025) in Improving IoT Security in Healthcare using a Blockchain-driven Lightweight Hashing System suggested a power-efficient hashing architecture [38].

InBlockchain-Based Access Control and Privacy Preservation in Healthcare: A Comprehensive Survey, Tawfik et al. [15] (2025) looked into blockchain-based access control solutions that use smart contracts to handle revocation and preserve patient permission [39]. To improve post-quantum security and transaction trust, Selvarajan and Mouratidis et al. [8] (2023) proposed a Blockchain Cybersecurity Model for Healthcare Systems based on Quantum Trust and Consultative Transactions [40].

In An Explainable Federated Blockchain Framework with Privacy Preserving AI Optimization for Securing Healthcare Data, Bhardwaj et al. [16] (2025) suggested a blockchain-based integration with federated learning that would allow for privacy-preserving distributed model training. In order to effectively manage healthcare data and policy compliance, Tawfik et al. [17] (2025) in AC HealthChain: Blockchain architecture for Access Control and Privacy Preservation in Healthcare suggested a modular architecture (EHRChain and PolicyChain) based on smart contracts and IPFS [41].

These studies show that cryptographic integrity features and blockchain's decentralized structure offer a strong foundation for achieving security, transparency, and traceability in complex multi-stakeholder ecosystems. Building on these discoveries, the proposed study outlines the use of blockchain technology to healthcare supply chain networks and traditional healthcare data management [42]. The model that is designed includes IoT and edge computing for in-real-time product monitoring, lightweight hashing for IoT support, and smart contracts for policymaking automation. The system ensures stakeholder responsibility from manufacturers to patients, data clarity, and product legitimacy by employing these techniques. This blockchain-based architecture guarantees the security and reliability of next-generation healthcare logistics networks, improves supply chain visibility, and drastically reduces counterfeiting.

3.Proposed Model:

Through a secure consortium blockchain network, the proposed blockchain-based healthcare supply chain infrastructure links patients, hospitals or pharmacies, and manufacturers. The process begins with the producer, who creates, authenticates, and digitally records batches of medical supplies (see Figure 1). The SHA-256 hashing technique is used to assign a distinct hash value to each batch, preserving data integrity and preventing unwanted alteration. After a batch is produced, smart contracts are used to record its details on the blockchain, automatically logging and verifying the transaction. Additionally, smart contracts make it easier to track and trace every product movement across the supply chain. Large or sensitive data, such as product reports or medical certificates, are stored in an off-chain system for maximum efficiency, but the cryptographic hashes corresponding to them are stored on-chain for tracking and verification.

Before the medical products are given to patients, authorized parties can use blockchain records to verify their validity when they arrive at pharmacies or hospitals. The blockchain securely records all transactions, including the issuing, dispensing, and recall of medical supplies, preventing counterfeiting. By using smart contracts to grant and revoke permissions, end users, or patients, can control access to their personal information and authenticate the medications they take. Along the healthcare supply chain, this open and decentralized paradigm improves product traceability, accountability, and confidence, guaranteeing that patients only receive safe and authentic medical supplies.

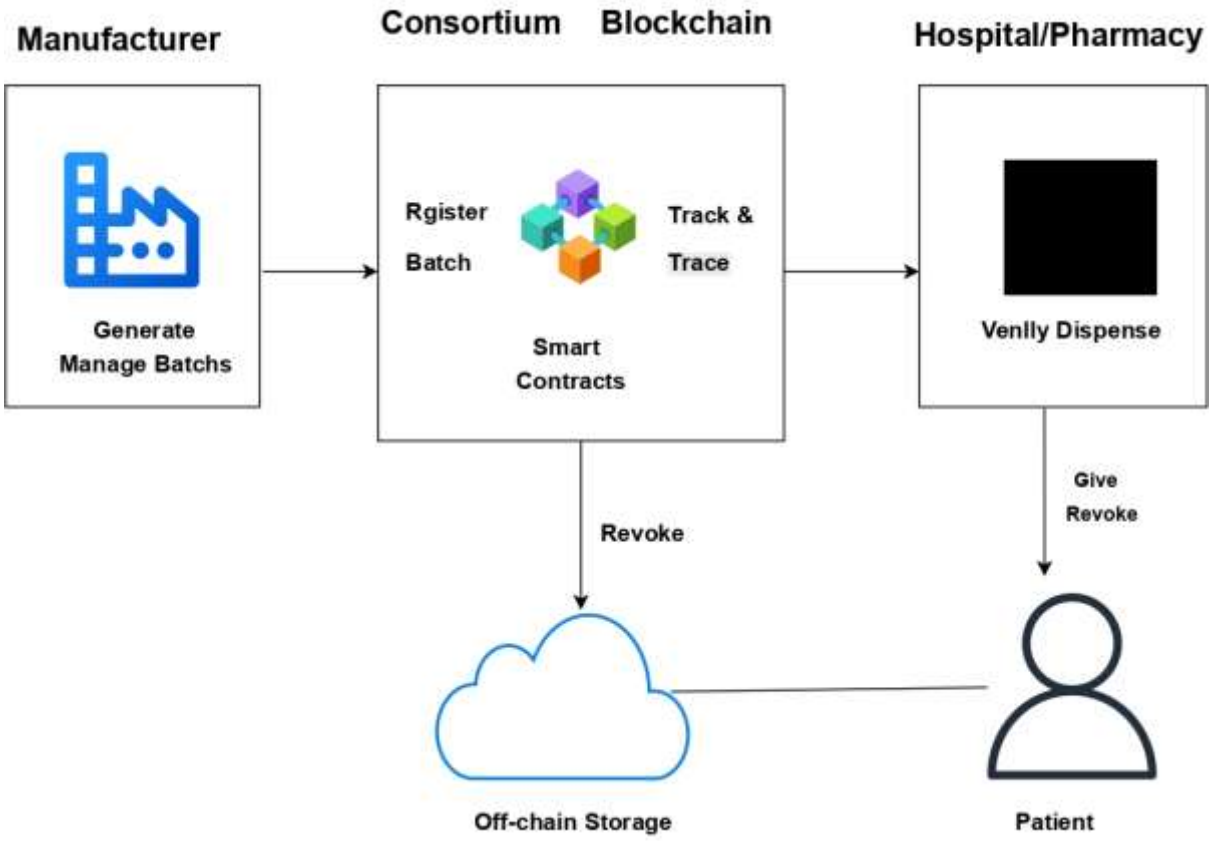

Figure -1: Architecture of the Blockchain-Enabled Healthcare Traceability System

Data Hashing (Integrity):

SHA-256 is used to generate a unique code (H_i) for each medical record (M_i). By serving as a digital fingerprint, the code makes sure that the data is safe even if the record is altered.SHA-256 is used to generate a unique code (H_i) for each medical record (M_i). By serving as a digital fingerprint, the code makes sure that the data is safe even if the record is altered.

$$H_i = SHA - 256(M_i) \quad \text{eq (1)}$$

Block Formation:

A block (B_i) contains the hash of the current medical record (H_i), the hash of the block that came before it ((H_{i-1})), the creation time (T_i), and a validation nonce (N_i). By safely joining blocks, this makes sure that nobody can change the blockchain.

$B_i = \{H_i, H_{i-1}, T_i, N_i\}$eq (2)

Block Hash:

A block hash (($H(B_i)$)) is generated using SHA-256 by integrating the hashes of the current record (H_i), the block before it (((H_{i-1})), the timestamp ((T_i)), and the nonce ((N_i)). This makes the blockchain safe and impossible to tamper with since it creates a distinct digital fingerprint for every block.

$H(B_i) = SHA - 256(H_i \,||\, H_{i-1} \,||\, T_i \,||\, N_i)$eq (3)

Proof of Work (Validation Rule):

The hash value of a block ((H(B_i)) needs to be **smaller** than a designated target value ((D)) in order for it to be approved. Proof of Work uses this concept to make the blockchain unbackable by ensuring that adding a block requires work.

$$H(B_i) < D \text{eq (4)}$$

Merkle Root (Multiple Records):

The Merkle root is one hash that represents every record in a block ((M_{root})). SHA-256 is created by combining all of the hashes of the various records ($(H_1 || H_2 || H_3 || \ldots . H_n)$). This allows you to quickly inspect any record without checking the full block.

$$M_{root} = H(H_1 \,||\, H_2 \,||\, H_3 \,||\, \cdots \,||\, H_n) \text{eq (5)}$$

Time Stamping (Record Traceability):

combining the previous block's timestamp ((T_{prev})). The timestamp of the current block (T_i) is obtained by calculating the time difference ((Δt)). This allows us to keep the data in **chronological order** and trace the manufacturing dates of individual blocks.

$$T_i = T_{prev} + \Delta t \text{eq (6)}$$

Hash Chain Verification

The hash of the current block ($(H(B_i)$) is obtained by combining the contents of the current block with the hash of the previous block ($(H(B_i)$). Since modifications to one block affect all subsequent blocks, tampering is easily detected due to this strong binding.

$$H(B_i) = H(H(B_{i-1}) \,||\, B_i) \text{eq (7)}$$

Transaction Rate (Performance):

The transaction rate (T_{rate}), which is equal to (N_{tx}), indicates the quantity of medical records processed per unit of time. It is shown how quickly transactions are recorded and processed by blockchain technology.

$$T_{rate} = \frac{N_{tx}}{t_{block}} \text{eq (8)}$$

Transaction Latency (Speed):

The amount of time required to confirm a transaction in a patient's medical record is called the latency (L). The time required to confirm ($t_{confirmation}$) is deducted from the time required to submit ($t_{submission}$). in the computation. This demonstrates how quickly transactions are processed on the blockchain.

$$L = t_{confirmation} - t_{submission} \text{eq (9)}$$

4.Results:

Based on the lag time, the graph [Figure-2] compares the lag-performance of four supply chain models: the proposed TraceSecure blockchain, Ethereum-based blockchain, Hyperledger-based blockchain, and traditional supply chain. The lag time for the Traditional Supply Chain model was the longest, suggesting both lower efficiency and less processing time. Although there was still a lag time in the process, the Ethereum and Hyperledger blockchains did perform somewhat better with faster validation times. The TraceSecure Blockchain, the suggested methodology, did have the shortest lag time, meaning that transactions were confirmed more quickly and that it provides superior responsiveness overall. Due to a reduced lag time, which enhances the overall data transfer, this finding suggests that the proposed TraceSecure Blockchain technique increases performance and efficiency in a healthcare supply chain.

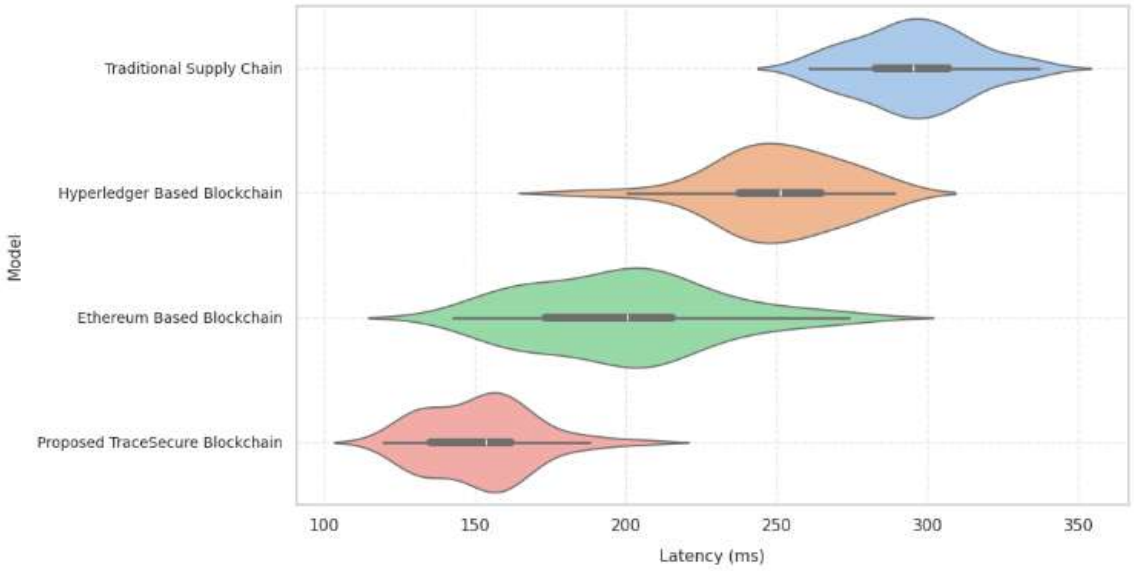

Figure-2: Latency Distribution

The throughput performance of four modelsthe proposed TraceSecure blockchain, Ethereum-based blockchain, Hyperledger-based blockchain, and traditional supply chainis depicted in the graph [Figure-3]. Of the four models, the Traditional model has the lowest throughput, while Ethereum and Hyperledger both offer a moderate improvement. With the largest throughput of any model, the proposed TraceSecure Blockchain exhibits the best scalability and efficiency while handling transactions in the healthcare supply chain.

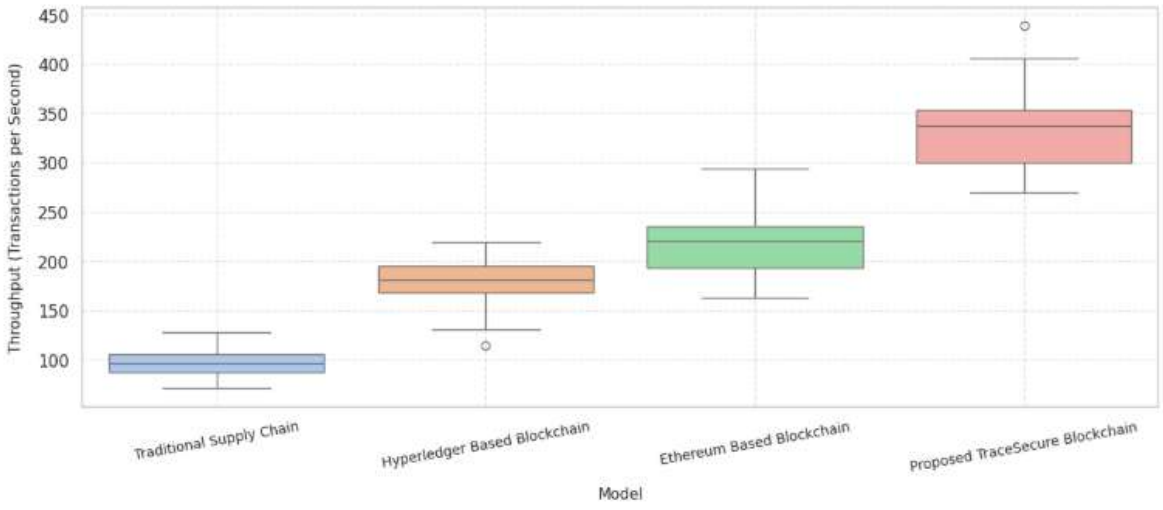

Figure-3: Throughput(Transaction per Second)

The data integrity performance of the four modelsTraditional, Hyperledger, Ethereum, and the Proposed Blockchain modelis displayed in the graph [Figure-4]. There is a higher chance of data manipulation because the Traditional model has the lowest integrity. Improvements in the Hyperledger and Ethereum models indicate improved data security, integrity, and verification. The Proposed Blockchain actually attains the highest data integrity, almost reaching 100%, proving a strong basis of dependability, robustness, and trustworthiness. This demonstrates that the suggested model can offer trustworthy, safe, and impenetrable healthcare data management.

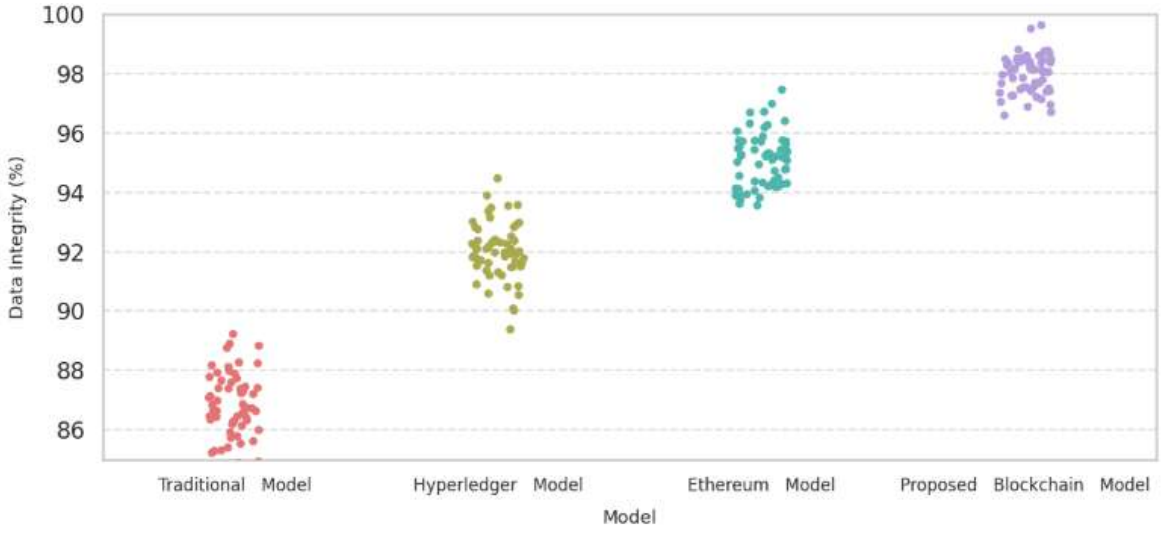

Figure 4: Data Integrity

The traceability index for four modelsthe proposed TraceSecure blockchain, Ethereum-based blockchain, Hyperledger-based blockchain, and traditional supply chainis displayed in the graph [Figure 5]. The traceability rating of the Traditional model is the lowest, indicating a lack of supply chain visibility. The enhanced visibility and tracking capabilities of the Ethereum and Hyperledger models suggest that traceability will increase somewhat. Nearing the highest score of 100% traceability, the proposed TraceSecure blockchain produces the highest traceability index. This demonstrates its capacity to track medical supplies in an open, end-to-end fashion throughout the supply chain.

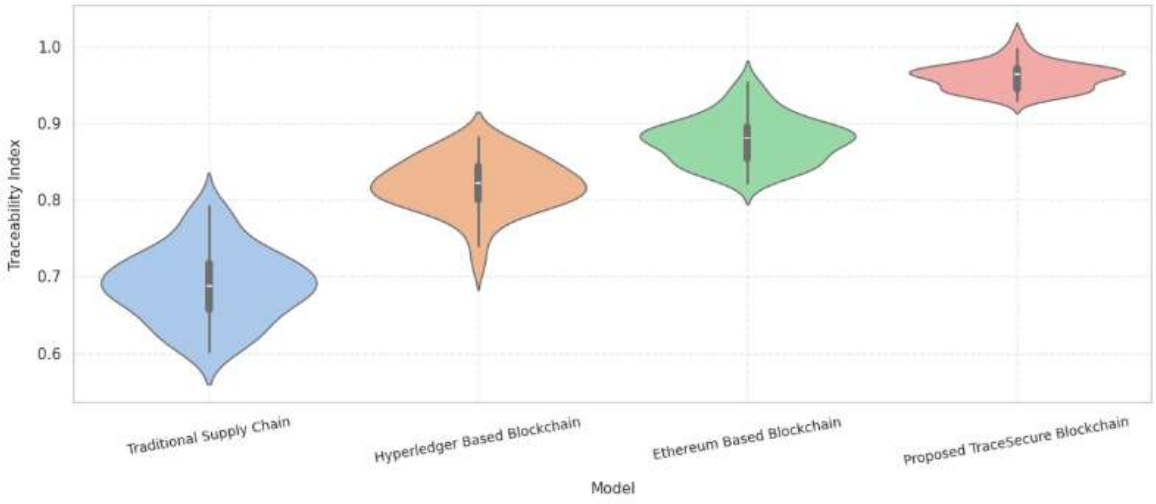

Figure 5: Traceability Index

The average block propagation time for several supply chain models is compared in the graph [Figure 6]. The slowest spread of block data is indicated by the Traditional Supply Chain, which has the longest propagation time (4.9 seconds). With average times of 3.9 and 3.2 seconds, respectively, the Hyperledger and Ethereum models both functioned well. With a propagation time of just 2.1 seconds, the Proposed Blockchain Supply Chain exhibits superior efficiency in terms of data validation and block transfer. The system's potential to increase transaction speeds and the network's overall responsiveness is described by the decrease in delays.

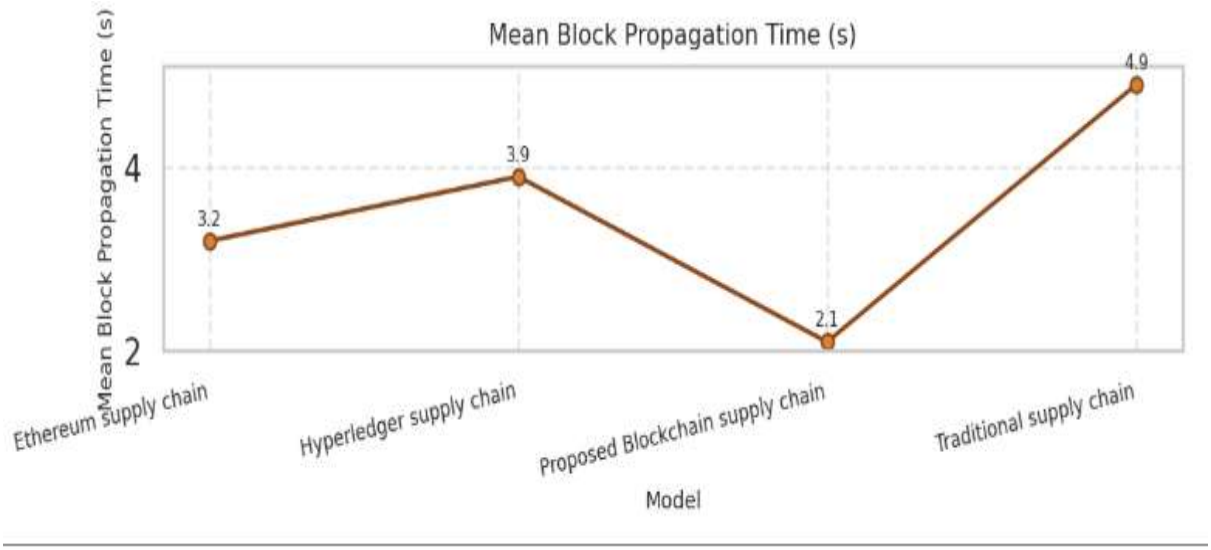

Figure 6: Mean Block Propagation

The variation in consensus time for different supply chain models is shown in the graph [Figure-7]. While the Hyperledger and Ethereum models performed better or had a shorter consensus time, the Traditional Supply Chain model had the longest consensus time, which indicates that it had the slowest node agreement in the network. The efficiency of the Proposed Blockchain Supply Chain model in achieving a quicker and more dependable agreement between network nodes is demonstrated by the consensus time, which is less than that of both models. This suggests that the proposed blockchain supply chain model improves overall system response time and transaction confirmation speed.

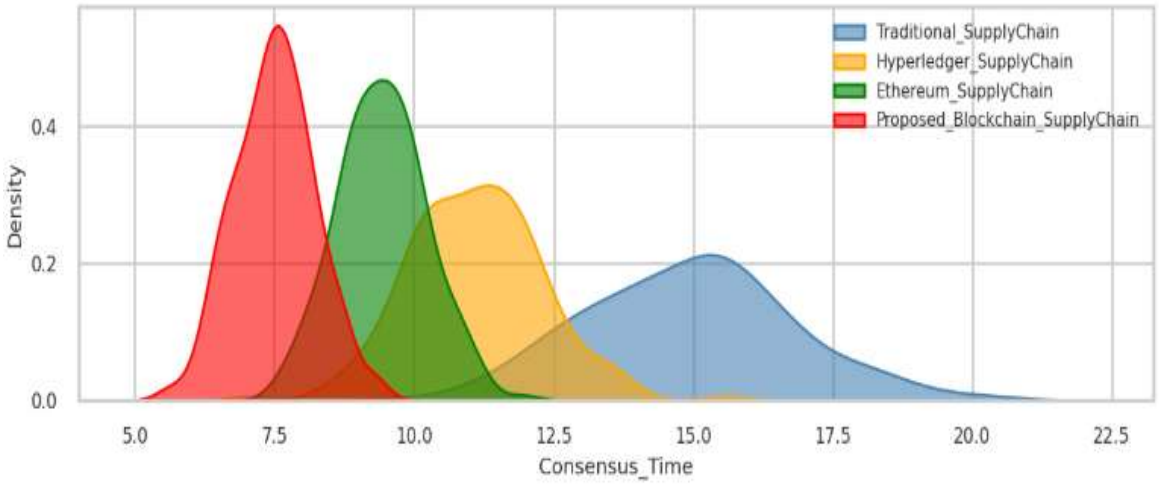

Figure-7: Consensus Time Distribution

The average storage overhead for several supply chain architectures is shown in the chart [Figure-8]. The largest storage overhead is found in the Traditional Supply Chain, indicating poor data management. The Ethereum and Hyperledger models introduce some degree of optimization and have moderate storage requirements. As seen by its lowest overhead, the proposed blockchain supply chain effectively reduces data redundancy. This illustrates how useful the suggested architecture is for organizing and aggregating data while preserving system scalability.

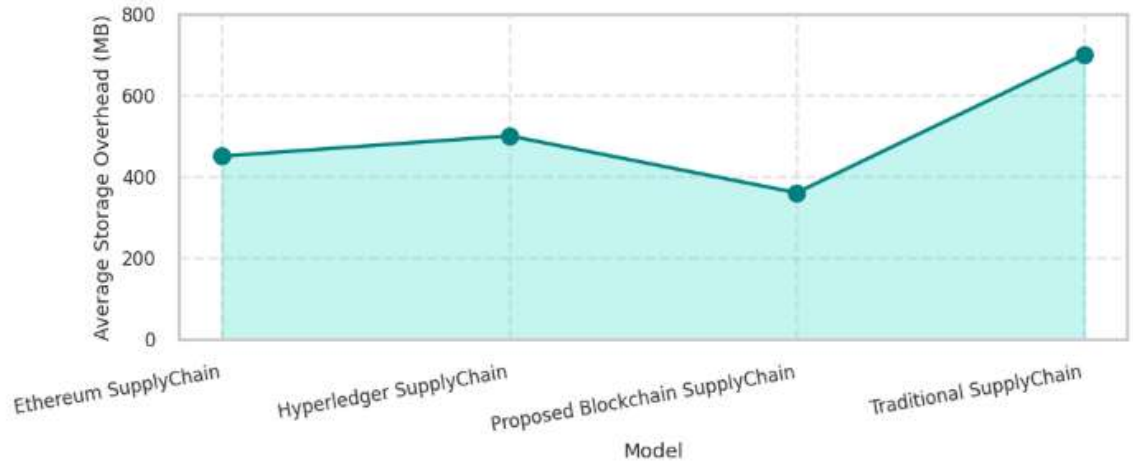

Figure-8: Average Storage Overhead

The transaction success rate for various supply chain architectures is displayed in the graph [Figure-9]. With a success percentage of only 85%, the Traditional Supply Chain is the least effective at handling transactions. Due to their respective 91% and 94% transaction success rates, the Ethereum Supply Chain and Hyperledger Supply Chain are both quite successful. Because of its dependability and efficient transaction verifications, the Proposed Blockchain Supply Chain has the greatest transaction success rate, at 98%. This indicates that the suggested approach is a more effective solution for consistent and error-free transaction processing.

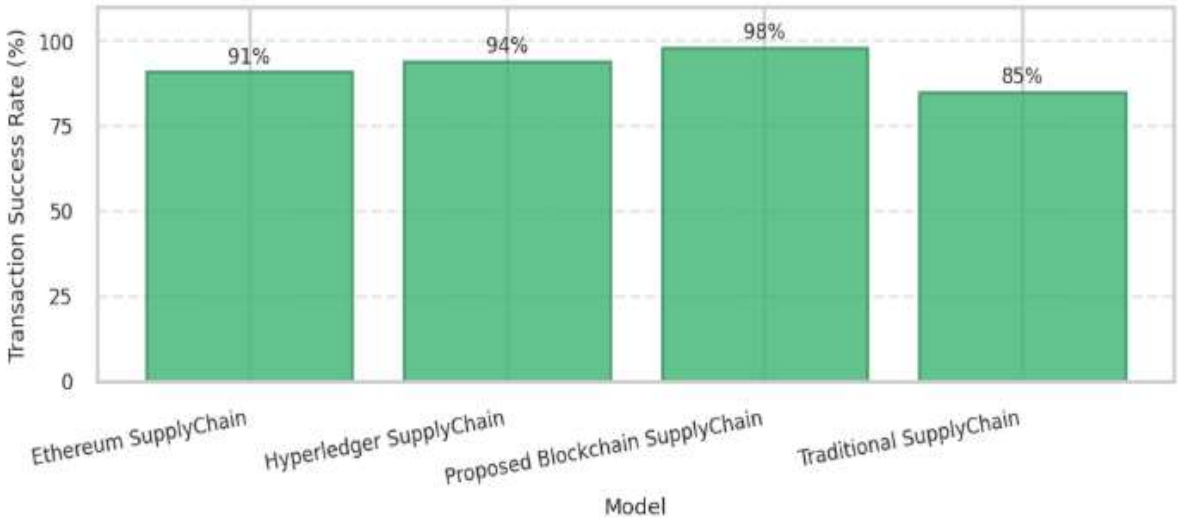

Figure-9: Transaction Success Rate

The security strength ratings of several supply chain models are shown in the image [Figure 10]. The Traditional Supply Chain has the lowest security strength score and the worst performance. The supply chains for Ethereum and Hyperledger show improved defense against attacks and minor security contributions. With the highest security strength score, the suggested blockchain supply chain is highly

resilient to data intrusions and alteration. This demonstrates the suggested model's exceptional resilience and dependability in protecting transactions and data reliability.

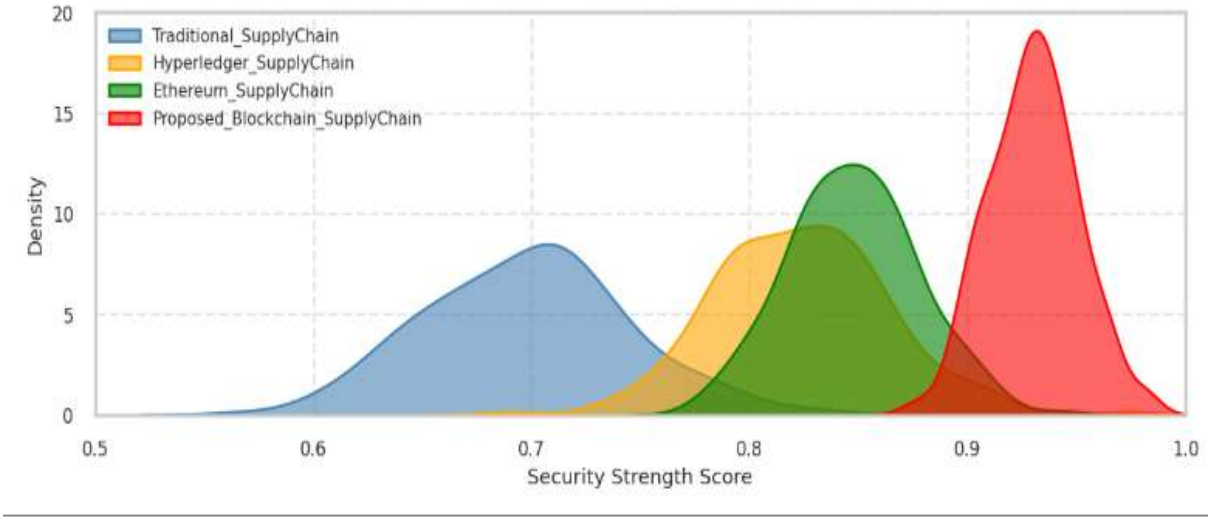

Figure-10: Security Strength Score Distribution

The data provenance accuracy of the different supply chain models is depicted in the graph. When it comes to irregularly monitoring a product's origins, the Traditional Supply Chain model has the lowest level of accuracy. Compared to the Traditional Supply Chain model, the Hyperledger and Ethereum blockchain models have a relatively greater accuracy and generate data that is more dependable and trustworthy. Additionally, the Proposed TraceSecure Blockchain is proved to deliver the most accuracy and data which has the highest level of tamper-proof traceability for complete correctness. Consequently, the Proposed TraceSecure Blockchain illustrates the effectiveness of the Proposed architecture in offering transparency and reliability with data records across the whole supply chain.

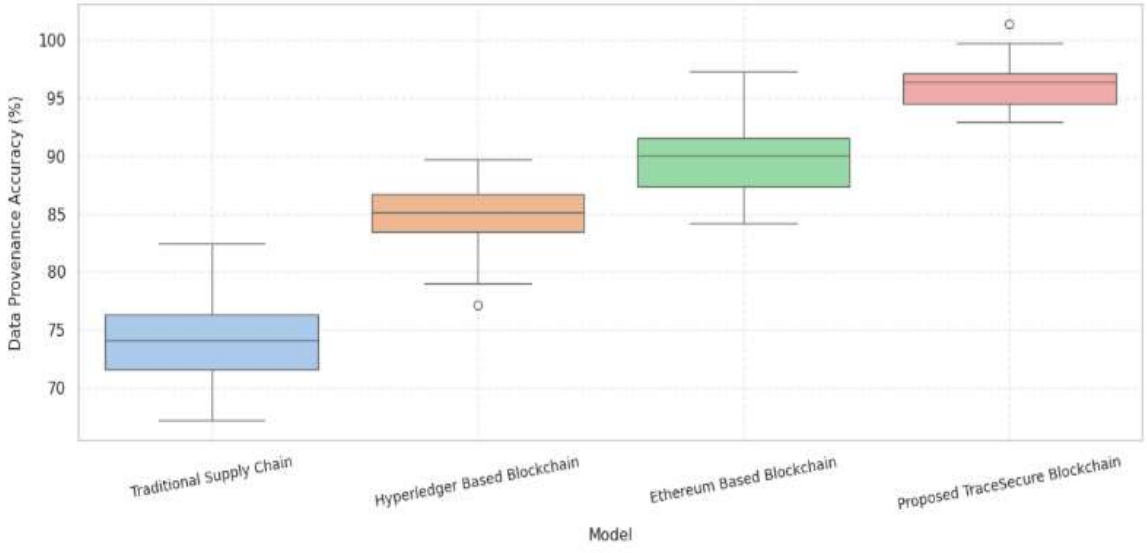

Figure-11: Data Provenance Accuracy

Conclusion:

Architecture powered by blockchain that addresses the persistent issues of product traceability, data integrity, and security in healthcare supply chains. The complexity and scale of modern healthcare logistics, where fraudulent medications, dispersed data silos, and covert transactions endanger patient safety and organizational responsibility, are becoming too much for centralized systems of the past. By leveraging the immutability, distributed consensus, and cryptographic verification of blockchain technology, the system ensures transparent and impenetrable administration of medical product data at every stage, from manufacturers to end users.

Smart contracts, edge computing, and IoT-based telemetry transform this framework into an intelligent, autonomous, and dependable ecosystem. While smart contracts expedite procedures like batch registration, product recall, and access revocation, edge nodes enable real-time data capture and quick verification. Improved operational effectiveness and demonstrable trust among dispersed healthcare partners are two advantages of this technology convergence. Scalability is ensured by integrating off-chain storage solutions without compromising the integrity and auditability of supply chain data.

One important conclusion drawn from the literature is that the majority of healthcare blockchain models to date have focused primarily on patient information interchange or medical record management, with little attention paid to supply chain interoperability and end-to-end product traceability. In order to bridge the gap, this work suggests a consortium blockchain architecture that includes fine-grained access control policies, lightweight hashing for IoT connectivity, and real-time monitoring. The solution reduces counterfeit seepage, improves accountability, and improves regulatory compliance by ensuring that every transactionfrom production to patient deliveryis time-stamped, auditable, and cryptographically verifiable.

Lastly, a blockchain architecture designed especially for the healthcare supply chain is added in this study. It is safe, scalable, and interoperable. In addition to facilitating the transition to Healthcare 6.0, an intelligent, patient-focused, and automation-centric ecosystem, it demonstrates how decentralized trust systems can ensure data transparency and product authenticity. Future studies can focus on large-scale pilot implementations using federated or hybrid blockchain frameworks, employing energy efficiency optimization to optimize sustainability and privacy-preserving methods like zero-knowledge proofs. Ultimately, the proposed paradigm offers a solid foundation for open, effective, and resilient digital healthcare networks that can endure operational and cyber threats in the future.

References:

[1]. R. Akkaoui, X. Hei and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," in *IEEE Access*, vol. 8, pp. 113467-113486, 2020, doi: 10.1109/ACCESS.2020.3003575.
[2]. E. R. D. Villarreal, J. García-Alonso, E. Moguel and J. A. H. Alegría, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," in *IEEE Access*, vol. 11, pp. 5629-5652, 2023, doi: 10.1109/ACCESS.2023.3236505.
[3]. O. P. Olawale and S. Ebadinezhad, "Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management," in *IEEE Access*, vol. 12, pp. 131605-131620, 2024, doi: 10.1109/ACCESS.2024.3460428.
[4]. Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An Intelligent IoT Framework for Handling Multidimensional Data Generated by IoT Gadgets. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_9
[5]. V. Lakshman Narayana,(2020), “A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node”, International Conference on Inventive Research in Computing Applications (ICIRCA),Publisher: IEEE,pp. 852-857, 9183256.
[6]. Tarakeswara Rao; R. S. M. Lakshmi Patibandla; V. Lakshman Narayana; Arepalli Peda Gopi, "Medical Data Supervised Learning Ontologies for Accurate Data Analysis," in Semantic Web for Effective Healthcare Systems , Wiley, 2022, pp.249-267, doi:10.1002/9781119764175.ch11.
[7]. Chaitanya, Kosaraju, et al. "Predicting the Spread of Covid Disease Based on Chest X-Ray Images Using Convolutional Neural Network with Improved Accuracy." 2023 6th International Conference on Advances in Science and Technology (ICAST). IEEE, 2023.
[8]. Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology. In: Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N. (eds) Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer, Cham.https://doi.org/10.1007/978-3-030-65691-1_16
[9]. Anusha, P. & Ravikiran, A. & Narayana, V. & Maddumala, V.R.. (2020). Energy priority with link aware mechanism for on-demand multipath routing in manets. International Journal of Advanced Science and Technology. 29. 8979-8991.
[10]. A.NareshV. PavaniM. Meghana Chowdarym. V.Lakshman Narayana (2020). Energy consumption reduction in cloud environment by balancing cloud user load. Journal of Critical Reviews. 7(7):1003-1010.

[11]. Suajtha, V. "Variable Selection in Functional Genomics Using Genetic Algorithm- Based Feature Selection Method-An Empirical Study." Journal of Engineering and Applied Sciences, 21 Sept. 2022. ISSN Online 1818-7803, ISSN Print 1816-949x.
[12]. Chaitanya, Kosaraju, and Sankara Narayanan. "Security and Privacy in Wireless Sensor Networks Using Intrusion Detection Models to Detect DDOS and Drdos Attacks: A Survey." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
[13]. V. Pavani, S. Sri. K, S. Krishna. P and V. L. Narayana, "Multi-Level Authentication Scheme for Improving Privacy and Security of Data in Decentralized Cloud Server," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 391-394, doi:10.1109/ICOSEC51865.2021.9591698.
[14]. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP) (pp. 60-66). IEEE.
[15]. V. Pavani, K. Divya, V. V. Likhitha, G. S. Mounika and K. S. Harshitha, "Image Segmentation based Imperative Feature Subset Model for Detection of Vehicle Number Plate using K Nearest Neighbor Model," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 704-709, doi: 10.1109/ICAIS56108.2023.10073848.
[16]. Krishna, P.S., Peram, S.R. (2023). CT image precise denoising model with edge based segmentation with labeled pixel extraction using CNN based feature extraction for oral cancer detection. Traitement du Signal, Vol. 40, No. 3, pp. 1297-1304. https://doi.org/10.18280/ts.400349
[17]. Nagamani, T., Gopal, G. V., Lakshmi, G., Ramakrishna, K. V. S. S., Srija, N., & Gopi, A. (2025). Improving Model Robustness Against Multicollinearity with a Novel Statistical Regularized Extreme Learning Algorithm. IAENG International Journal of Computer Science, 52(11).
[18]. Chaitanya, Ms Prathipati Silpa, et al. "TAODV Trust based AODV Protocol in MANETS to Mitigate Black Hole Effect." 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). IEEE, 2023.
[19]. A. Islam, MF. Kader, and SY. Shin, “BSSSQS: a blockchain based smart and secured scheme for question sharing in the smart education system ” arXiv preprint arXiv:1812.03917. 2018 Dec 05.
[20]. A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, “Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards ”, *Overview report The British Standards Institution (BSI)*. 2017 May ; 40 (40): 1 - 34.
[21]. Kavishwar, S. (2024). A Theoretical Framework Analyzing Impact of Embedding Entrepreneurial Skills in Education on Economical Growth. *Journal of Lifestyle and SDGs Review*, *4*(4), e03550.
[22]. Narlawar, N., Kavishwar, S. (2019). Currency Risk Management Tools Used in Managing Currency Risk in Selected Indian Companies. Indian Journal of Research and Analytical Reviews. 6(2), 609-614.
[23]. Ghangare, A. S., & Kavishwar, S. The Increasing Significance of Green Corporate Finance in India. *Journal of Management & Entrepreneurship*, 277-286.
[24]. Kavishwar, S., & Shahu, A. (2011). Reporting Intangible Assets-Convergence of Accounting Standard. *Journal of Accounting and Finance.* 26(1), 73-79.
[25]. Jingar, N. K. (2022). Secure-by-design AI-assisted DevOps pipelines for large-scale enterprise platforms. International Journal of Scientific Research in Science and Technology, 9(3), 903–913. https://doi.org/10.32628/IJSRST2291348
[26]. Jingar, N. K. (2022). Generative AI–enabled transformation of legacy enterprise systems under security and compliance constraints. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 760–770. https://doi.org/10.32628/CSEIT23906219
[27]. Nijim, M. et al. (2025). Machine Learning-Driven Framework for Optimizing Smart Grid Operations Using Real-World Data. In: Daimi, K., Alsadoon, A. (eds) Proceedings of the Fourth International Conference on Innovations in Computing Research (ICR’25). ICR 25 2025. Lecture Notes in Networks and Systems, vol 1487. Springer, Cham. https://doi.org/10.1007/978-3-031-95652-2_40
[28]. Nijim, M., Albataineh, H., Kanumuri, V., Goyal, A., Mishra, A., Hicks, D. (2023). Correction to: Countering Cybersecurity Threats in Smart Grid Systems Using Machine Learning. In: Daimi, K., Alsadoon, A., Peoples, C., El Madhoun, N. (eds) Emerging Trends in Cybersecurity Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-09640-2_21

[29]. Racha, Ganesh. "Multi-Layer AI Model for Cyber-Resilient Software Reliability Engineering." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 5, Sept.–Oct. 2025, pp. 507–519. https://doi.org/10.32628/CSEIT26121364

[30]. Racha, Ganesh. "Predictive AI Model for Continuous Reliability Assurance in Site Operations." International Journal of Scientific Research in Science and Technology, vol. 12, no. 2, Mar.-Apr. 2025, pp. 1469-78, https://doi.org/10.32628/IJSRST2613340.

[31]. Veginati, Navya. "Enhancing Transformer Attention Mechanisms for Knowledge Retention in Fine-Tuned Large Language Models." International Journal of Scientific Research in Science and Technology, vol. 11, no. 5, Sept.–Oct. 2024, pp. 864–871. DOI: https://doi.org/10.32628/IJSRST52310284

[32]. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56

[33]. Jonnalagadda, Pawan Kalyan. "Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 4, Dec. 2025, pp. 46–57.

[34]. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43

[35]. A. Mahida, "Machine Learning Integrated Zero Trust Automation with DevOps Principles for Continuous Security Enforcement," 2026 Sixth International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT), Bhilai, India, 2026, pp. 1-7, doi: 10.1109/ICAECT68478.2026.11426026.

[36]. Ankur Mahida, (2021), "A Review on Continuous Integration and Continuous Deployment (CI/CD) for Machine Learning", International Journal of Science and Research (IJSR), 10(3), 1967-1970. https://dx.doi.org/10.21275/SR24314131827, https://www.ijsr.net/getabstract.php?paperid=SR24314131827

[37]. S. S. R. Tummuri, "Machine Learning-Driven Data Quality Monitoring for Fault-Tolerant Data Pipelines," 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Singapore, Singapore, 2025, pp. 154-159, doi: 10.1109/ICCMSO67468.2025.00036.

[38]. S. S. R. Tummuri, "Generative AI for Data-Centric Healthcare with Integrated Anomaly Detection and Monitoring," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 520-526, doi: 10.1109/IC3ET64989.2026.11467187.

[39]. B. K. Reddy Janumpally, "Intelligent Energy Aware Efficient Task Scheduling in Cloud Computing: Leveraging Swarm Optimization Algorithms for Improve Resource Utilization," 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN), Thanjavur, India, 2025, pp. 1-6, doi: 10.1109/RFCoN62306.2025.11085278.

[40]. Janumpally, Bharath Kumar Reddy. (2026). Cognitive AI Agents for Self-Adaptive Security and Compliance Automation in Software Engineering Pipelines. 10.1109/ICAUC68182.2026.11441048.

[41]. Yachamaneni T, Kotadiya U, Arora AS. Evaluating the Efficacy of Machine Learning Algorithms in Credit Card Limit Optimization and Customer Segmentation. IJETCSIT [Internet]. 2022 Oct. 30 [cited 2026 Apr. 5];3(3):51-6.

[42]. Yachamaneni T, Kotadiya U, Arora AS. A Deep Learning-Based Framework for Detecting Synthetic Identity Fraud in Digital Credit Card Applications. IJERET [Internet]. 2023 Dec. 30 [cited 2026 Apr. 5];4(4):43-52.