International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Medical Supply Blockchain

L.Venkata Jyothsna, KVR. Abhishek, Varanasi Vivek, M. Jaswanth, S. Shahid

Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, A.P., India

---

Abstract - The healthcare supply chain faces challenges such as inefficient procurement, lack of transparency, counterfeit medicines, and poor tracking mechanisms. This paper proposes a blockchain-based solution integrating smart contracts and decentralized storage systems to enhance traceability, security, and efficiency. The system connects stakeholders including manufacturers, distributors, retailers, and healthcare providers through the Ethereum blockchain. Smart contracts automate transactions, while IPFS and Hyperledger Fabric ensure secure and decentralized storage. The proposed framework improves transparency, reduces fraud, and enhances communication across the supply chain. Experimental results demonstrate improved security, cost efficiency, and system reliability.

Key Words: *Blockchain Technology, Healthcare Supply Chain, Smart Contracts, Ethereum, Decentralized Storage, IPFS (InterPlanetary File System), Hyperledger Fabric, Supply Chain Management, Data Security, Traceability, Transparency, Counterfeit Drug Prevention, Distributed Ledger Technology.*

---

1. INTRODUCTION

The healthcare supply chain plays a critical role in ensuring the timely delivery of medicines, medical equipment, and essential healthcare services. However, maintaining the integrity, transparency, and security of this supply chain remains a significant challenge. Traditional healthcare supply chain systems are often centralized, complex, and lack real-time visibility, making them vulnerable to inefficiencies, delays, and fraud. Issues such as counterfeit drugs, lack of traceability, and poor coordination among stakeholders can severely impact patient safety and overall healthcare outcomes. In developing countries, a significant percentage of medicines are reported to be counterfeit or substandard, highlighting the urgent need for a secure and transparent system.

Healthcare supply chains involve multiple stakeholders including manufacturers, distributors, wholesalers, retailers, and healthcare providers. Due to this multi-layered structure, tracking the movement of medical products from production to end consumers becomes difficult. Information is often stored in isolated databases, leading to data silos and lack of synchronization. Once a disruption or vulnerability occurs at any stage, it can propagate throughout the entire system, resulting in supply shortages, delays, or distribution of unsafe products. Additionally, reliance on manual processes and third-party intermediaries increases operational costs and introduces further risks of manipulation and inefficiency.

With the advancement of digital technologies, blockchain has emerged as a promising solution to address these challenges. Blockchain technology provides a decentralized, immutable, and transparent ledger where all transactions are securely recorded and cannot be altered once validated. This ensures data integrity and trust among all participants without requiring a central authority. In a healthcare supply chain context, blockchain enables real-time tracking of products, secure sharing of information, and improved coordination among stakeholders. Each transaction, such as manufacturing, shipping, or delivery, can be recorded on the blockchain, creating a verifiable audit trail.

Smart contracts, a key feature of blockchain platforms such as Ethereum, further enhance the system by automating processes and enforcing predefined rules. These contracts execute automatically when certain conditions are met, eliminating the need for intermediaries and reducing delays. For example, purchase orders, product transfers, and delivery confirmations can be managed through smart contracts, ensuring accuracy and efficiency. However, storing large amounts of data directly on the blockchain can be costly and inefficient, which necessitates the use of decentralized storage solutions.

To overcome this limitation, decentralized storage systems such as InterPlanetary File System (IPFS) and Hyperledger Fabric can be integrated with blockchain. These systems store large files off-chain while maintaining secure references (hashes) on the blockchain, ensuring both efficiency and data security.

This hybrid approach allows for scalable storage while preserving the integrity and authenticity of information. Furthermore, cryptographic techniques and access control mechanisms ensure that only authorized participants can access sensitive data, enhancing privacy and security.

This paper proposes a blockchain-based healthcare supply chain system that integrates Ethereum smart contracts with decentralized storage technologies to provide end-to-end visibility, security, and traceability of medical products. The proposed system enables secure interaction among stakeholders, prevents counterfeit drug distribution, and improves overall efficiency. By leveraging blockchain's inherent properties such as immutability, transparency, and decentralization, the system aims to address the limitations of traditional supply chain models. Ultimately, this approach contributes to building a more reliable, secure, and efficient healthcare ecosystem that ensures safe delivery of medical products to end users.

2. LITERATURE SURVEY

2.1 Blockchain Technology in Supply Chain Management

Blockchain technology has gained significant attention for improving transparency, traceability, and security in supply chain systems. One of the earliest applications of blockchain in supply chains was proposed by Toyoda et al. (2017), who introduced a blockchain-based Product Ownership Management System (POMS) to ensure product authenticity and prevent counterfeiting. Their work demonstrated how distributed ledger technology can maintain immutable ownership records across the supply chain. Malik et al. (2018) further extended this concept through ProductChain, a scalable blockchain framework designed to support data provenance and secure product tracking. Their system emphasized access control and transaction authorization to prevent unauthorized data manipulation.

Wang et al. (2019) proposed a smart contract-based traceability system that enables tracking of products through events generated within blockchain transactions. Their approach improved visibility across supply chain stages but lacked integration with decentralized storage systems. Similarly, large-scale industrial implementations such as the IBM and Maersk blockchain initiative demonstrated the feasibility of blockchain in global logistics by enhancing transparency and reducing paperwork. However, these systems primarily focused on logistics efficiency and did not address domain-specific challenges such as healthcare product safety and counterfeit prevention.

2.2 Blockchain in Healthcare Supply Chain

The application of blockchain in healthcare has been explored to address issues such as counterfeit drugs, lack of traceability, and data security. Kim and Laskowski (2018) proposed an ontology-driven blockchain framework for pharmaceutical supply chains, emphasizing structured data sharing and provenance tracking. Bocek et al. (2017) introduced a blockchain-based solution for monitoring pharmaceutical transportation conditions, particularly temperature-sensitive drugs, ensuring compliance with quality standards during transit.

Further studies by Bryatov and Borodinov (2019) and Haq and Esuka (2018) focused on preventing counterfeit drugs using blockchain-based pharmaceutical supply chains. These works highlighted the importance of immutability and decentralized verification in ensuring product authenticity. However, most of these solutions lacked comprehensive implementation details and did not fully integrate multiple stakeholders or provide end-to-end system validation. Additionally, many systems relied solely on blockchain without incorporating efficient off-chain storage mechanisms, leading to scalability issues.

2.3 Smart Contracts for Automation and Traceability

Smart contracts have emerged as a critical component in blockchain-based systems for automating transactions and enforcing rules without intermediaries. Wang et al. (2019) demonstrated how smart contracts can be used to record product movement and generate event logs for traceability. These contracts ensure that each transaction is validated and executed automatically when predefined conditions are met, reducing human intervention and operational delays.

Other studies have explored the use of smart contracts in managing supply chain workflows, including order processing, shipment tracking, and ownership transfer. Despite these advancements, many existing solutions focus on individual processes rather than providing a unified framework that integrates all stakeholders. Moreover, issues such as high execution costs (gas fees)

and lack of optimized contract design remain challenges in practical implementations.

2.4 Decentralized Storage and Data Security

While blockchain ensures data immutability and transparency, storing large volumes of data directly on-chain is inefficient and costly. To address this limitation, decentralized storage systems such as InterPlanetary File System (IPFS) and Hyperledger Fabric have been proposed. Casino et al. (2019) explored the use of decentralized storage for supply chain systems, highlighting its advantages in scalability and distributed access. However, their approach lacked integration with smart contract-driven workflows and decentralized applications (DApps).

Recent research emphasizes hybrid architectures that combine blockchain with off-chain storage. In such systems, large files are stored in IPFS, while only cryptographic hashes are stored on the blockchain, ensuring both efficiency and data integrity. Hyperledger Fabric further enhances security by enabling permissioned access and encryption mechanisms. Despite these advancements, existing solutions often fail to provide a fully integrated model that combines blockchain, smart contracts, and decentralized storage with strong security guarantees.

2.5 Research Gaps and Motivation

Although significant progress has been made in applying blockchain to supply chain management, several limitations remain. Many existing systems lack complete decentralization, rely on centralized storage components, or fail to integrate smart contracts with decentralized storage solutions. Additionally, most studies do not provide comprehensive evaluation in terms of cost, security, and scalability. As highlighted in the comparative analysis on page 8, several approaches lack decentralized storage or DApp compatibility, limiting their practical applicability.

To address these gaps, there is a need for a unified framework that integrates blockchain technology, smart contracts, and decentralized storage systems to provide secure, scalable, and transparent healthcare supply chain management. The proposed system aims to fulfill these requirements by ensuring end-to-end traceability, preventing counterfeit products, and enhancing stakeholder collaboration.

3. SYSTEM ANALYSIS

3.1 Existing System

Traditional healthcare supply chain systems are primarily centralized and rely on manual record-keeping, fragmented databases, and third-party intermediaries. These systems typically involve multiple stakeholders such as manufacturers, distributors, wholesalers, and healthcare providers, but lack a unified platform for real-time data sharing and verification. Information is stored in isolated systems, leading to inconsistencies, delays, and lack of synchronization across the supply chain.

In the context of security and traceability, existing systems provide limited visibility into the movement of medical products. Once a product leaves the manufacturer, tracking its journey becomes difficult due to the absence of a transparent and tamper-proof mechanism. This creates opportunities for counterfeit drugs to enter the supply chain without detection. Additionally, traditional systems rely heavily on paperwork and manual verification processes, which are prone to human error and manipulation.

Existing supply chain solutions also operate on trust-based relationships between stakeholders rather than verifiable data. This means that once a transaction is recorded in a centralized database, it can potentially be altered or deleted by unauthorized entities. Furthermore, there is no continuous monitoring mechanism to ensure product authenticity, expiry validation, or real-time inventory status. As a result, issues such as supply shortages, delayed deliveries, and distribution of substandard medical products are common.

Another major limitation is the lack of efficient data storage and sharing mechanisms. Large volumes of data, including product details, shipment records, and regulatory documents, are stored in centralized servers, making them vulnerable to cyberattacks and single points of failure. Existing systems also struggle with scalability, as increasing the number of stakeholders leads to higher complexity and reduced system performance. These limitations highlight the need for a secure, transparent, and decentralized solution for healthcare supply chain management.

3.2 Proposed System

The proposed system introduces a blockchain-based healthcare supply chain that integrates Ethereum smart contracts with decentralized storage technologies to ensure secure, transparent, and efficient management of medical products. The system architecture consists of multiple interconnected modules that operate collaboratively to provide end-to-end visibility and control over the supply chain.

The Blockchain Module forms the core of the system, where all transactions are recorded on a distributed ledger. Each stakeholder is assigned a unique Ethereum address, and all interactions such as product creation, order placement, shipment, and delivery are stored as immutable transactions. This ensures that once data is recorded, it cannot be altered, thereby preventing fraud and unauthorized modifications. The blockchain enables real-time tracking of products and provides a verifiable audit trail for all stakeholders.

The Smart Contract Module automates supply chain operations through predefined rules and conditions. The system implements three primary smart contracts: Registration Smart Contract, Purchase Order Smart Contract, and Product Lot Smart Contract. The Registration contract manages stakeholder authentication and access control by maintaining a list of authorized participants. The Purchase Order contract handles order requests, approvals, and confirmations, ensuring seamless coordination between stakeholders. The Product Lot contract tracks detailed information about each product batch, including batch number, quantity, composition, and ownership transfer. These contracts eliminate the need for intermediaries and reduce operational delays by executing transactions automatically.

The Decentralized Storage Module enhances data management by integrating IPFS and Hyperledger Fabric. Large files such as product certificates, images, and regulatory documents are stored off-chain in IPFS, while their corresponding cryptographic hashes are stored on the blockchain. Hyperledger Fabric provides an additional layer of security by storing encrypted hash values and access keys, ensuring that only authorized users can access sensitive data. This hybrid storage approach improves scalability, reduces storage costs, and maintains data integrity.

The Security and Access Control Module ensures that only authorized stakeholders can interact with the system. Cryptographic hashing, encryption techniques, and role-based access control mechanisms are implemented to protect data from unauthorized access. Each transaction is validated through consensus mechanisms, and all data exchanges are secured using blockchain cryptography. This module also prevents cyberattacks such as data tampering, unauthorized modifications, and replay attacks.

The Detection and Monitoring Mechanism continuously tracks supply chain activities, including product movement, order status, and inventory levels. Any discrepancies, such as missing shipments or unauthorized product modifications, can be easily identified through the blockchain ledger. The system also enables real-time notifications and alerts for critical events, improving responsiveness and decision-making among stakeholders.

Overall, the proposed system provides a decentralized, transparent, and secure framework for healthcare supply chain management. By combining blockchain technology, smart contracts, and decentralized storage, it addresses the limitations of traditional systems and ensures efficient, reliable, and tamper-proof operations across the entire supply chain.

Fig 1 :Architecture Diagram

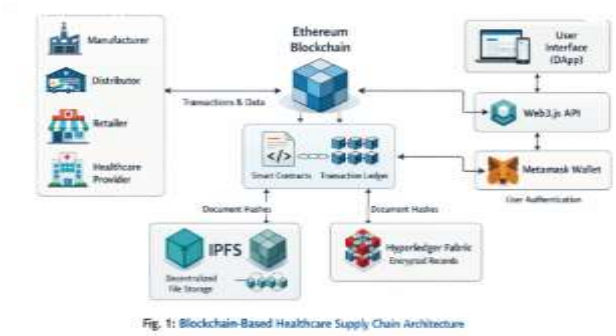

Fig. 1: Blockchain-Based Healthcare Supply Chain Architecture

4. ALGORITHMS AND TECHNIQUES

4.1 Blockchain Transaction and Consensus Mechanism

The proposed system utilizes blockchain technology as the foundational layer for maintaining a distributed and immutable ledger of all supply chain transactions. Each transaction, such as product creation, order placement, shipment, and delivery, is grouped into blocks and appended to the blockchain after validation through a consensus mechanism.

Blockchain ensures data integrity using cryptographic hashing, where each block contains a hash of the previous block, forming a secure chain. Any attempt to

modify data in a block results in a change in its hash, thereby breaking the chain and making tampering easily detectable. The transaction verification process involves validating the authenticity of the sender using digital signatures and ensuring that only authorized stakeholders can perform specific operations.

The immutability property of blockchain ensures that once a transaction is recorded, it cannot be altered or deleted. This is particularly important in healthcare supply chains, where maintaining accurate records of product origin, movement, and ownership is critical. The decentralized nature of the blockchain eliminates the need for a central authority, thereby reducing the risk of single points of failure and improving system reliability.

4.2 Smart Contract Execution Algorithm

Smart contracts are self-executing programs deployed on the Ethereum blockchain that automate supply chain operations. The proposed system implements three primary smart contracts: Registration, Purchase Order, and Product Lot contracts.

The Registration Smart Contract follows an authorization algorithm where each stakeholder is verified before being added to the network. The process includes validating identity credentials, assigning a unique Ethereum address, and storing the stakeholder details on the blockchain. Only authorized entities can invoke this function, ensuring controlled access.

The Purchase Order Smart Contract implements an event-driven workflow algorithm. When a stakeholder initiates an order request, the contract records the request details, including requester address, product type, and quantity. The manufacturer or distributor validates the request and confirms the order, triggering subsequent events such as shipment initiation and delivery confirmation. Each stage is recorded as a transaction, enabling complete traceability.

The Product Lot Smart Contract manages product lifecycle tracking using a state transition model. Each product batch is assigned a unique identifier, and its attributes—such as batch number, composition, and quantity—are stored in the contract. Ownership transfer is handled through function calls that update the current holder of the product, ensuring a transparent and verifiable chain of custody.

4.3 Decentralized Storage and Data Management Technique

To address the limitations of on-chain storage, the system employs a hybrid storage mechanism using IPFS and Hyperledger Fabric. Large data files, including product certificates, images, and regulatory documents, are stored in IPFS, which generates a unique cryptographic hash for each file.

The storage algorithm follows a two-step process:

1. Upload data to IPFS and generate a content-addressable hash.
2. Store the hash on the blockchain through a smart contract transaction.

This approach ensures that the actual data remains off-chain, reducing storage costs and improving scalability, while the hash stored on the blockchain guarantees data integrity and authenticity. Hyperledger Fabric enhances security by storing encrypted hashes and access keys, enabling controlled data sharing among stakeholders. Only users with the correct decryption key can access the stored data, ensuring privacy and confidentiality.

4.4 Access Control and Security Mechanisms

The system incorporates multiple security techniques to ensure safe and authorized interactions within the supply chain. Role-based access control (RBAC) is implemented through smart contracts, where each stakeholder is assigned specific permissions based on their role. For example, only manufacturers can create product lots, while distributors and retailers can initiate purchase orders.

Cryptographic techniques such as hashing and digital signatures are used to secure transactions. Each transaction is signed using the private key of the sender, ensuring authenticity and non-repudiation. Additionally, the system employs encryption mechanisms for protecting sensitive data stored in decentralized storage systems.

Security analysis tools such as SmartCheck and OYENTE are used to detect vulnerabilities in smart contracts, including reentrancy attacks, denial-of-service conditions, and transaction ordering dependencies. These tools analyze the contract code and

ensure that it is free from common security flaws, thereby improving system reliability.

4.5 Supply Chain Monitoring and Traceability Technique

The proposed system implements a real-time monitoring mechanism that tracks the movement of products across the supply chain. Each transaction recorded on the blockchain contributes to a complete audit trail, enabling stakeholders to trace the origin and journey of any product.

The traceability algorithm works by linking all transactions associated with a product lot using its unique identifier. By querying the blockchain, users can retrieve the entire history of the product, including manufacturing details, shipment records, and delivery status. This ensures transparency and helps in identifying discrepancies such as missing shipments or counterfeit products.

Additionally, the system supports event-driven notifications, where stakeholders are alerted about important events such as order confirmation, shipment dispatch, and delivery completion. This improves coordination and decision-making across the supply chain.

5. SOFTWARES AND LIBRARIES

The proposed system is implemented using blockchain technologies combined with modern development tools and decentralized storage frameworks. The architecture follows a modular design, enabling seamless integration between smart contracts, storage systems, and user interfaces. The key software technologies and libraries used in the system are described below.

Solidity serves as the primary programming language for developing smart contracts on the Ethereum blockchain. It is a contract-oriented language specifically designed for writing secure and efficient decentralized applications (DApps). Solidity enables the implementation of business logic such as stakeholder registration, purchase order management, and product tracking. Its strong typing system and support for inheritance allow developers to build scalable and maintainable smart contract architectures.

Ethereum Blockchain is used as the core platform for deploying and executing smart contracts. It provides a decentralized and immutable ledger where all transactions are securely recorded. Ethereum's support for smart contracts enables automation of supply chain operations without the need for intermediaries. Each transaction executed on the network consumes gas, which represents the computational cost of executing operations, ensuring efficient resource utilization.

Remix IDE is a web-based development environment used for writing, testing, and deploying smart contracts. It provides features such as syntax highlighting, debugging tools, and real-time error detection, making it suitable for rapid development and testing. Remix also allows developers to simulate transactions and analyze execution costs (gas usage), which is essential for optimizing smart contract performance.

InterPlanetary File System (IPFS) is used as a decentralized storage solution for handling large data files such as product certificates, images, and regulatory documents. IPFS uses a content-addressable storage mechanism, where each file is assigned a unique cryptographic hash. This ensures data integrity and allows efficient retrieval of files without relying on centralized servers. By storing only the hash on the blockchain, the system reduces storage costs while maintaining security.

Hyperledger Fabric is employed as an additional decentralized storage and security layer. It is a permissioned blockchain framework that supports encrypted data storage and controlled access. In the proposed system, Hyperledger Fabric is used to store encrypted hash values and manage access keys, ensuring that only authorized users can access sensitive information. This enhances privacy and provides an extra layer of protection for critical healthcare data.

Web3.js / Web3 Libraries are used to facilitate interaction between the frontend application and the Ethereum blockchain. These libraries enable functions such as sending transactions, reading smart contract data, and managing user accounts through wallets. They act as a bridge between the user interface and blockchain network, allowing seamless communication.

Metamask is used as a cryptocurrency wallet and gateway to interact with the Ethereum blockchain. It manages user identities, stores private keys securely, and allows users to sign transactions. Metamask enables stakeholders to authenticate themselves and perform blockchain operations such as executing smart contracts and verifying transactions.

Development Environment and Requirements include a system capable of running modern web

browsers, blockchain tools, and decentralized storage nodes. The implementation requires a machine with sufficient computational resources to deploy smart contracts, run IPFS nodes, and interact with blockchain networks. Internet connectivity is essential for accessing the Ethereum network and decentralized storage systems.

Overall, the combination of these software tools and libraries provides a robust, secure, and scalable environment for implementing the blockchain-based healthcare supply chain system. The integration of smart contract platforms, decentralized storage, and web-based interfaces ensures efficient operation and seamless interaction among stakeholders.

nd internet connectivity for Telegram alerts.

6. RESULTS AND DISCUSSION

The experimental evaluation of the proposed blockchain-based healthcare supply chain system was conducted by simulating real-world supply chain operations involving multiple stakeholders, including manufacturers, distributors, wholesalers, retailers, and healthcare providers. The system was tested across key functional scenarios such as stakeholder registration, product lot creation, purchase order processing, shipment tracking, and final delivery confirmation. These operations were executed using Ethereum smart contracts, with decentralized storage support provided by IPFS and Hyperledger Fabric, ensuring a comprehensive validation of the system architecture.

The deployment and execution of smart contracts demonstrated successful automation of supply chain processes. The Registration Smart Contract effectively added authorized stakeholders to the blockchain network, recording their Ethereum addresses along with timestamped details. The Purchase Order Smart Contract enabled seamless order placement and confirmation between stakeholders, with all transactions being immutably stored on the blockchain. The Product Lot Smart Contract successfully tracked the lifecycle of medical products, including batch information, ownership transfer, and delivery status. The results confirm that the system provides complete traceability of products from manufacturing to end-user delivery.

The cost analysis of smart contract operations was evaluated using gas consumption metrics. The Stakeholder Addition function incurred a transaction cost of approximately 46,298 gas, while the Purchase Order and Product Delivery functions required 29,068 gas and 26,891 gas respectively. These results indicate that the system maintains a balance between functionality and computational efficiency, ensuring that operational costs remain manageable while supporting complex supply chain workflows.

From a security perspective, the system demonstrated strong resilience against common vulnerabilities. The use of cryptographic hashing and immutable ledger structures ensured that all recorded transactions remained tamper-proof. Access control mechanisms restricted system interactions to authorized stakeholders only, thereby preventing unauthorized data manipulation. Additionally, vulnerability analysis using tools such as SmartCheck and OYENTE confirmed that the smart contracts were free from critical issues such as reentrancy attacks, denial-of-service conditions, and transaction ordering dependencies. This validates the robustness and reliability of the implemented smart contract logic.

The integration of decentralized storage significantly improved data management efficiency. Large files, including product documentation and verification records, were successfully stored in IPFS, while their corresponding hashes were securely maintained on the blockchain. Hyperledger Fabric provided an additional security layer by encrypting hash values and managing access permissions. This hybrid storage approach reduced on-chain data load while preserving data integrity and ensuring secure access.

The system also demonstrated improved transparency and coordination among stakeholders. Real-time tracking of product movement enabled stakeholders to monitor supply chain activities and verify product authenticity at every stage. The traceability mechanism allowed users to retrieve the complete history of any product lot, including manufacturing details, shipment records, and delivery confirmations. This significantly reduced the risk of counterfeit products entering the supply chain and enhanced trust among participants.

Furthermore, the proposed system showed better performance compared to existing solutions. Unlike traditional supply chain systems that rely on centralized databases, the blockchain-based approach eliminated single points of failure and ensured continuous availability of data. The comparison with other blockchain-based solutions revealed that the proposed system uniquely integrates smart contracts,

decentralized storage, and DApp compatibility, providing a more comprehensive and scalable solution.

Overall, the results demonstrate that the proposed system effectively improves security, transparency, traceability, and efficiency in healthcare supply chain management. The combination of blockchain technology, smart contracts, and decentralized storage provides a robust framework capable of addressing the limitations of traditional systems while ensuring reliable and secure delivery of medical products.

7. CONCLUSIONS

The integration of complex behavioral biometrics and static signature analysis in an endpoint environment has significant impact for both individual and organizational cybersecurity in the broad context of Cyber Supply Chain security. Point-in-time authentication is insufficient; any weakness in an unlocked system may put the entire organizational network at risk. Through ML-based continuous behavioral authentication and CTI-based threat intelligence for rapid payload detection, this research enhances workstation-level CSC security.

The experimental framework demonstrated that the combined results of Isolation Forest, One-Class SVM, and heuristic regex matching successfully identify anomalies including user impersonation, HID injection attacks, and typed malicious commands. The 23-feature biometric profile effectively extracts threat cadence, which integrates into the ML classifiers for threat prediction. The weighted detection engine provides a unified, nuanced risk score that supports tiered automated responses without alert fatigue.

Future work will evaluate extending localized models into a federated learning approach for privacy-preserving multi-endpoint deployment. Additional enhancements planned include multi-user profile management, integration with cloud-based CTI feeds for real-time signature updates, and SIEM platform integration for centralized enterprise monitoring. Deep learning techniques for sequential pattern analysis and cross-platform support (Linux/macOS) are also identified as promising directions.

ACKNOWLEDGEMENT

The authors express sincere gratitude to Raghu Engineering College (Autonomous), Visakhapatnam, affiliated to JNTU Vizianagaram, for providing the necessary facilities to carry out this research. Special thanks to Sri Raghu Kalidindi (Chairman), Dr. A. Vijay Kumar (Principal), and the Department of Computer Science and Engineering for their continued support and guidance throughout this project.

REFERENCES

[1]. M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "On the Malleability of Bitcoin Transactions," in *Proc. International Conference on Financial Cryptography and Data Security*, 2015.

[2]. A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain Technology Applications in Healthcare: An Overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.

[3]. J. LaPointe, "Exploring the Role of Supply Chain Management in Healthcare," *RevCycle Intelligence*, 2022.

[4]. World Health Organization (WHO), "1 in 10 Medical Products in Developing Countries is Substandard or Falsified," Nov. 2017.

[5]. P. Gerwil, "Blockchain in the Healthcare Supply Chain," *Digital Health Buzz*, 2022.

[6]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proc. IEEE International Congress on Big Data*, 2017, pp. 557–564.

[7]. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[8]. S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains," in *Proc. IEEE NCA*, 2018, pp. 1–10.

[9]. S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario," *IEEE Access*, vol. 7, pp. 115122–115133, 2019.

[10]. H. M. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[11]. T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains Everywhere – A Use Case of

Blockchains in the Pharma Supply Chain," in *Proc. IFIP/IEEE IM*, 2017, pp. 772–777.

[12]. IBM, "Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains," Jan. 2018.

[13]. F. Casino, T. K. Dasaklis, and C. Patsakis, "Enhanced Vendor-Managed Inventory Through Blockchain," in *Proc. SEEDA-CECNSM*, 2019, pp. 1–8.

[14]. Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, "Blockchain-Based Framework for Improving Supply Chain Traceability and Information Sharing in Precast Construction," *Automation in Construction*, vol. 111, p. 103063, 2020.

[15]. S. Bryatov and A. Borodinov, "Blockchain Technology in the Pharmaceutical Supply Chain: Researching a Business Model Based on Hyperledger Fabric," in *Proc. ITNT*, 2019.

[16]. I. Haq and O. M. Esuka, "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs," *International Journal of Computer Applications*, vol. 180, no. 25, pp. 8–12, 2018.

[17]. E. Fernando et al., "Success Factors of Implementation of Blockchain Technology in Pharmaceutical Industry: A Literature Review," in *Proc. ICITACEE*, 2019.

[18]. M. M. Rashid, S.-H. Lee, and K.-R. Kwon, "Blockchain Technology for Combating Deepfake and Protecting Video/Image Integrity," *Journal of Korea Multimedia Society*, vol. 24, no. 8, pp. 1044–1058, 2021.

[19]. IPFS, "InterPlanetary File System (IPFS) Documentation," 2022.

[20]. Hyperledger, "Hyperledger Fabric Documentation," 2022.

[21]. S. Tikhomirov et al., "SmartCheck: Static Analysis of Ethereum Smart Contracts," in *Proc. International Workshop on Emerging Trends in Software Engineering for Blockchain*, 2018, pp. 9–16.