Educational Administration: Theory and Practice
2024, 30(6), 887-896
ISSN: 2148-2403
https://kuey.net/

Research Article

Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme

Mrs. Ravula Priyanka[1*], Dr. G. Sreeram[2]

[1*]Mtech, Department of Computer Science and Engineering, Vignana Barathi Institute of technology, Aushapur, Ghatkesar, Telangana, India,
[2]Assistant Professor, Vignana Barathi Institute of technology

Citation: Mrs. Ravula Priyanka, 22P61D5801, et al (2024), Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme, *Educational Administration: Theory and Practice, 30*(6), 887-896, Doi: 10.53555/kuey.v30i6.5385

ARTICLE INFO

ABSTRACT

In recent years, the importance of ensuring vaccine safety has grown significantly due to frequent safety incidents. To tackle this issue, researchers have suggested using blockchain technology to secure the vaccine circulation process. However, blockchain faces challenges such as high storage requirements and low throughput, which limit its effectiveness in supply chain applications. To overcome these challenges, we propose an enhanced, storage-efficient blockchain-based scheme for vaccine safety protection.Our approach begins by modeling the vaccine circulation process. We then design a comprehensive system that integrates blockchain, cloud computing, and cryptographic techniques to secure the vaccine supply chain. The cloud component is used to manage the vaccine circulation model, while the blockchain stores data certificates and signatures to ensure the integrity and traceability of the vaccines. This integration leverages the strengths of each technology: the cloud provides scalable storage and processing power, while blockchain ensures the data's immutability and transparency. To validate our approach, we developed a conceptual model and tested it on a consortium blockchain. The experimental results demonstrate that our system is both efficient and effective in enhancing the security and reliability of the vaccine supply chain. Specifically, our system addresses the storage and throughput limitations of traditional blockchain technology by offloading data-intensive tasks to the cloud, which significantly reduces the blockchain's storage requirements. Furthermore, the use of cryptographic techniques ensures that all data stored in the blockchain is secure and tamper-proof. By employing advanced encryption methods, we can protect sensitive information and guarantee that only authorized parties can access and modify the data. This enhances the overall security of the vaccine supply chain and ensures that vaccines are safely circulated and monitored.

Our proposed solution also includes a robust data governance framework to specify and monitor data exchange and usage. This framework ensures that all stakeholders adhere to established protocols and regulations, which enhances trust and transparency in the vaccine supply chain. Additionally, our system provides real-time monitoring and reporting capabilities, allowing stakeholders to quickly identify and address any issues that may arise during the vaccine circulation process.

Keywords: Vaccine Safety, Blockchain Technology, Vaccine Circulation Process, Supply Chain Security, Cloud Computing, Cryptographic Techniques, Data Integrity, Traceability, Storage Efficiency, Data Governance, Real-time Monitoring, Public Health Outcomes.

Introduction

Counterfeiting of vaccines is a significant global issue, impacting the safety of vaccinated individuals and trust in vaccines, especially with the development of COVID-19 vaccines. Enhancing the ability to track and trace vaccines throughout the supply chain is imperative. The global immunization community has prioritized

barcoding the primary packaging of vaccines, such as vials and pre-filled syringes. Emer ging vaccine manufacturers are investigating the incorporation of barcoding using GS1 international standards. For instance, Bio Farma in Indonesia has initiated a pilot program to implement barcoding on primary packaging, demonstrating promising results with modest investment (Vest and Gamm, 2010).Blockchain technology offers a decentralized and tamper-proof method for enhancing the traceability of vaccine supply chains. Rosa et al. (2018) present an NFC-powered implantable device for on-body parameter monitoring with secure data exchange linked to a medical blockchain network. This device, powered by near-field communication (NFC) from an external mobile phone, supports various physiological measurements and ensures secure data transfer using encryption and blockchain for data storage and processing.To address issues of security and efficiency in blockchain, Zheng et al. (2019) propose a GAN-based key secret-sharing scheme. This technology improves blockchain security, facilitates the recovery of lost keys, and enhances communication efficiency by treating the secret as an image during the sharing process. The proposed scheme demonstrates flexibility and efficiency, which are crucial for maintaining the integrity and security of blockchain networks.

In the context of blockchain mining, Tang et al. (2019) introduce a game-theoretic framework using zero-determinant (ZD) strategies to incentivize honest mining and enhance the efficiency of blockchain networks. This framework encourages cooperative mining, thereby improving the overall welfare and efficiency of proof-of-work (PoW)-based blockchain networks.

The leader-follower consensus problem in multi-agent systems with time delays is addressed by Li et al. (2020). Using the semi-tensor product of matrices, they convert the dynamics of these systems into an algebraic form, providing necessary and sufficient conditions for consensus. Their approach ensures reliable coordination among agents, which is critical in distributed systems.

Tian et al. (2020) explore fixed-time leader-follower output feedback consensus for second-order multi-agent systems. Their findings contribute to the development of efficient control mechanisms in multi-agent systems, ensuring timely and accurate responses to changes in system dynamics.

In the realm of vaccine safety, Yong et al. (2019) propose an intelligent blockchain-based system for vaccine supply and supervision. This system integrates blockchain to enhance traceability and safety, addressing issues related to counterfeit vaccines and ensuring the integrity of the vaccine supply chain.

Falco et al. (2019) introduce NeuroMesh, a blockchain-powered botnet vaccine for IoT security. This system leverages blockchain to provide robust security mechanisms for IoT devices, protecting against cyber threats and ensuring secure data communication.

Peng et al. (2020) present an efficient double-layer blockchain method for vaccine production supervision. This approach enhances the traceability and safety of vaccine production processes, ensuring compliance with safety standards and reducing the risk of counterfeit vaccines.

Cui et al. (2020) discuss the use of blockchain to improve vaccine safety, highlighting the technology's potential to enhance traceability and accountability in the vaccine supply chain. Their work emphasizes the importance of integrating blockchain to safeguard public health.

Zhang et al. (2020) propose a blockchain-based trust mechanism for IoT-based smart manufacturing systems. This mechanism ensures secure data exchange and traceability, enhancing the reliability and efficiency of smart manufacturing processes.

Cao et al. (2019) develop a blockchain-based traceability system for steel products, demonstrating the technology's applicability in industrial settings beyond healthcare. Their system ensures accurate tracking of steel products, improving transparency and accountability in the supply chain.

Westerkamp et al. (2020) introduce a blockchain-based supply chain traceability model, employing token recipes to represent manufacturing processes. This model enhances the traceability and efficiency of supply chains, providing a robust solution for tracking and verifying product origins.

Waltonchain (2020) is an example of a blockchain platform designed to improve supply chain traceability. It leverages blockchain technology to enhance transparency and efficiency, ensuring secure and accurate tracking of products throughout the supply chain.

Lu et al. (2019) propose a secure data storage protocol for sensors in the Industrial Internet of Things (IIoT) using blockchain. This protocol ensures the integrity and security of sensor data, addressing the challenges of data storage and transmission in industrial environments.

Lin et al. (2019) present HomeChain, a blockchain-based mutual authentication system for smart homes. This system ensures secure communication and data exchange in smart home environments, protecting against cyber threats and unauthorized access.

Bagga et al. (2019) develop a blockchain-based batch authentication protocol for the Internet of Vehicles (IoV). This protocol enhances the security and reliability of data communication in vehicular networks, ensuring safe and efficient transportation.

Ahmed et al. (2019) propose a blockchain-based architecture for secure digital payment systems. This solution addresses the security challenges of digital payments, providing a robust framework for secure financial transactions.

In conclusion, blockchain technology holds significant potential for enhancing the traceability and security of supply chains, particularly in the context of vaccine safety. The integration of blockchain with other emerging

technologies, such as IoT and AI, can further enhance the efficiency and reliability of these systems, ensuring the integrity and safety of products and data throughout various industries.

Materials and Methods

In this project work, there are four modules and each module has specific functions, they are:
1. Admin Module
2. PLC Module
3. Server Module

3.3.1 Admin Module

The Admin module functions as the cornerstone of the cloud-assisted industrial environment, orchestrating key management tasks essential for seamless operation. Primarily, it assumes responsibility for the integration and oversight of Programmable Logic Controllers (PLCs) and servers across the network. Through this central hub, user authentication and access control are meticulously administered, ensuring that only authorized personnel can interact with critical system components. Additionally, the Admin module undertakes the vital role of monitoring system health and performance, promptly identifying and addressing any anomalies that may arise. Moreover, it offers a versatile platform for configuring and fine-tuning settings tailored to the unique requirements of both PLCs and servers. Lastly, the Admin module furnishes administrators with an intuitive interface, empowering them to comprehensively visualize and manage system resources, thus optimizing operational efficiency and reliability.

3.3.2 PLC Module

The PLC Module, situated within every deployed Programmable Logic Controller (PLC) across the industrial site, serves as the operational backbone of the system. Its multifaceted functions are finely tuned to ensure seamless communication and task management within the industrial environment. The module diligently conducts continuous monitoring of both IO devices and servers, maintaining real-time awareness of their statuses. By regularly assessing server availability and workload, it intelligently selects the optimal server for task execution, thereby optimizing system efficiency. Furthermore, the PLC Module orchestrates the secure upload of data from IO devices to servers, safeguarding data integrity throughout the transmission process. It adeptly handles responses from servers, facilitating efficient task execution and communication. Additionally, the module provides operators with a user-friendly interface to manage tasks, offering functionalities such as canceling requests and uploading new tasks as needed. Leveraging its comprehensive capabilities, the PLC Module plays a pivotal role in ensuring smooth and reliable operation within the industrial site, contributing to enhanced productivity and efficiency.

3.3.3 Server Module

The Server Module, deployed within each server (s1, s2, s3) within the cloud environment, stands as a pivotal component in the orchestration of task execution and data processing. Its multifaceted functions are finely tuned to ensure seamless operation and efficient utilization of resources within the cloud environment. The module facilitates task management through a dedicated task manager login, offering administrators the ability to oversee task execution and monitor server status in real-time. Additionally, it adeptly handles incoming requests from Programmable Logic Controllers (PLCs), processing the data received with precision and efficiency. As a guardian of system integrity, the Server Module diligently monitors server workload and availability, dynamically adapting to changing conditions to optimize resource allocation. Furthermore, it possesses the capability to gracefully handle task cancellations upon request from PLCs, ensuring seamless task management and resource utilization. Leveraging robust encryption techniques, the module decrypts data received from PLCs for processing, safeguarding sensitive information throughout the data processing pipeline. Once data processing is complete, the Server Module promptly sends processed data back to PLCs, facilitating seamless communication and task execution. Finally, the module provides valuable status updates to the Admin module, enabling comprehensive system monitoring and management. Through its comprehensive functionalities, the Server Module plays a pivotal role in ensuring the efficiency, reliability, and security of task execution and data processing within the cloud-assisted industrial environment.

3.4 Architecture

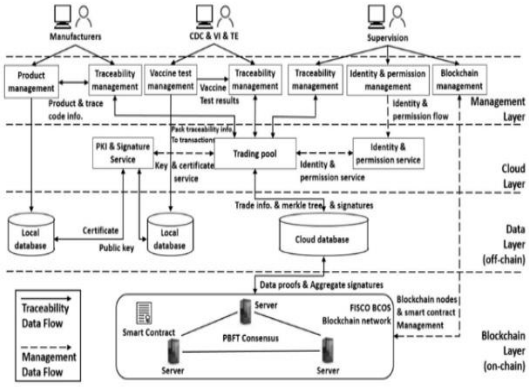
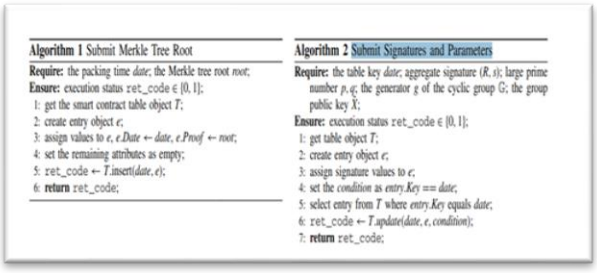


Fig 1: System Architecture



Algorithm 1 Submit Merkle Tree Root

Require: the packing time *date*; the Merkle tree root *root*;
Ensure: execution status ret_code ∈ [0, 1];
1: get the smart contract table object *T*;
2: create entry object *e*;
3: assign values to *e*, *e.Date* ← *date*, *e.Proof* ← *root*;
4: set the remaining attributes as empty;
5: ret_code ← *T.insert*(*date*, *e*);
6: **return** ret_code;

Algorithm 2 Submit Signatures and Parameters

Require: the table key *date*; aggregate signature (*R*, *s*); large prime number *p*, *q*; the generator *g* of the cyclic group *G*; the group public key *X*;
Ensure: execution status ret_code ∈ [0, 1];
1: get table object *T*;
2: create entry object *e*;
3: assign signature values to *e*;
4: set the *condition* as *entry.Key* == *date*;
5: select entry from *T* where *entry.Key* equals *date*;
6: ret_code ← *T.update*(*date*, *e*, *condition*);
7: **return** ret_code;

Fig 2 :Algorithm Applied in the Project

Algorithm 1: Submit Merkle Tree Root
This algorithm handles the submission of a Merkle tree root to a smart contract table.

Inputs: The packing time (date) and the Merkle tree root (root).
Step 1: Retrieve the smart contract table object (T).
Step 2: Create an entry object (e).
Step 3: Assign the input values to the entry object: e.Date = date, e.Proof_root = root.
Step 4: Set any other attributes of e to empty.

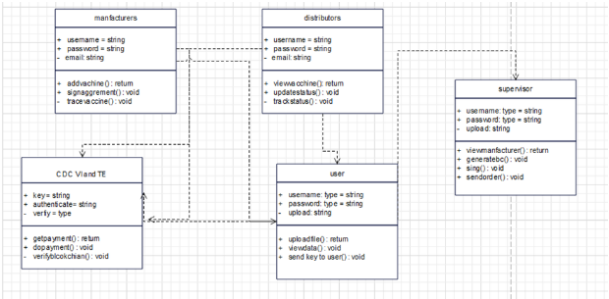


Fig 3: Class diagram

Step 5: Insert the entry object (e) into the table (T) using the date as the key. This returns an execution status code (ret_code).
Step 6: Return the execution status code (ret_code).

Algorithm 2: Submit Signatures and Parameters
This algorithm deals with submitting signatures and other parameters to a table based on a given key. Inputs: The table key (date), aggregate signature (R, s), large prime number P, public key X, generator g, and group G.
Step 1: Retrieve the table object (T).
Step 2: Create an entry object (e).
Step 3: Assign the signature and parameter values to the entry object (e).
Step 4: Set a condition for the entry update, specifically where entry.Key == date.
Step 5: Select the entry from the table (T) where the entry's key matches the date.
Step 6: Update the entry in the table with the new values based on the condition. This returns an execution

status code (ret_code).
Step 7: Return the execution status code (ret_code)

Algorithm 1: Submit Merkle Tree Root
This algorithm is designed to submit a Merkle tree root to a smart contract table. It starts by retrieving the smart contract table object and creating an entry object. The input date and Merkle tree root are assigned to this entry object, and any other attributes are set to empty. The entry object is then inserted into the table using the date as the key, which returns an execution status code. This status code indicates whether the insertion was successful and is returned by the algorithm.

Algorithm 2: Submit Signatures and Parameters
This algorithm handles the submission of signatures and cryptographic parameters to a table based on a given key, usually a date. It begins by retrieving the table object and creating an entry object. The provided signature and parameter values (aggregate signature R, s, large prime number P, public key X, generator g, and group G) are assigned to the entry object. A condition is set to update the entry where the key matches the given date. The algorithm selects the relevant entry from the table, updates it with the new values, and returns an execution status code indicating the success of the update.

Summary
Both algorithms ensure data integrity and traceability within a blockchain system. Algorithm 1 focuses on inserting a new Merkle tree root, which is essential for verifying data integrity. Algorithm 2 updates existing entries with new cryptographic signatures and parameters, ensuring the stored data remains current and accurate. These structured approaches to data submission and updating maintain the security and reliability of interactions with the smart contract table

Implementation
1. Introduction: The introduction provides an overview of the pressing issues surrounding vaccine safety incidents, including reported fraud and data tampering within the vaccine supply chain. It emphasizes the critical need for a robust solution to address these challenges and ensure the integrity and safety of vaccines.
2. Problem Statement: This section delineates the specific risks associated with the vaccine supply chain, including the production of unqualified vaccines, collusion between intermediate suppliers and vaccination institutions, and failures in adhering to cold chain requirements. It underscores the inadequacies of traditional centralized information management systems in mitigating these risks, leading to concerns regarding data tampering and a lack of trust across the supply chain.
3. Objective: The objective of the proposed system is to leverage blockchain technology to establish a secure, transparent, and efficient framework for managing vaccine circulation. By decentralizing data storage and employing cryptographic mechanisms, the system aims to address the vulnerabilities inherent in traditional information management systems and foster a closed loop of trust among stakeholders.
4. System Architecture :This section presents an overview of the architecture of the proposed system, illustrating how blockchain, cloud, and cryptographic mechanisms are integrated to ensure the security and integrity of vaccine data. It outlines the roles and interactions of each component within the system.
5. Components of the System: Blockchain: This subsection explains how blockchain technology will be utilized to store circulating data certificates and signatures securely. It highlights the immutability and transparency of blockchain, which ensures that vaccine-related data cannot be tampered with or falsified.
Cloud: Here, the role of cloud infrastructure in supporting the implementation of the vaccine circulation model is discussed. The scalability and accessibility of cloud resources enable efficient data management and processing, facilitating seamless integration with blockchain technology.
Cryptographic Mechanisms: This subsection provides an overview of the cryptographic techniques employed to enhance data security and privacy within the system. Techniques such as digital signatures and encryption are utilized to protect sensitive information and ensure data integrity.
6. Implementation Strategy :This section outlines the step-by-step approach for implementing the proposed system, including considerations for deployment, configuration, and integration with existing systems. It also discusses potential challenges and mitigation strategies.
7. Advantages of the Proposed System: This section highlights the benefits of the proposed system, including improved security, transparency, and efficiency in vaccine supply chain management. It emphasizes how the decentralized nature of blockchain, coupled with cloud infrastructure and cryptographic mechanisms, enhances accountability and trust among stakeholders.
8. Evaluation: The evaluation section presents experimental results from testing the proposed conceptual model. It demonstrates the efficiency and effectiveness of the system in safeguarding vaccine data and mitigating risks within the supply chain.proposed solution in addressing vaccine safety incidents and enhancing trust in the vaccine supply chain. It reiterates the importance of leveraging blockchain technology to ensure the integrity and safety of vaccines.
9. Future Directions: The future directions section discusses potential avenues for further research and development to enhance the capabilities of the proposed system. It identifies emerging challenges in vaccine

safety and distribution and proposes strategies for addressing them through continued innovation and collaboration. Manufacturers:
Manufacturers register and log in to the system, manage vaccine production, and apply for production licenses. They submit vaccine trace codes for CDC approval and ensure transparency through traceability services. Strict access controls are in place, and supervisors oversee identity management and access control updates.

Prototype System:*CDC, VI, and TE:*
CDC approves vaccine manufacturing requests, generates blockchain records for approved vaccines, and facilitates status updates and searches. VI and TE verify vaccine approval status and participate in distribution and testing processes.
Distributors:Distributors update vaccine status post-approval, distribute vaccines to end-users, and search for vaccine information. They work under supervisor oversight to ensure compliance with distribution permissions.
Supervisor:Supervisors oversee vaccine distribution, verify approval status, review distributor requests, and update distribution status. They maintain control over the distribution process and ensure only approved vaccines are distributed.
Users:Users access the system to receive vaccines and update their vaccination status. They provide real-time updates on vaccination status, contributing to the overall transparency and efficiency of the vaccine distribution process

Results and Discussion

The experimental evaluation of the proposed conceptual model using a consortium blockchain yielded promising results. The key findings are summarized as follows:
Efficiency in Vaccine Circulation: The proposed system demonstrated efficiency in managing vaccine circulation processes. By leveraging blockchain technology to store circulating data certificates and signatures, the system ensured the integrity and traceability of vaccine-related information throughout the supply chain.
Storage-Efficiency: One of the primary objectives of the proposed system was to address the limitations of traditional blockchain solutions, such as large on-chain storage consumption. Through the integration of cloud infrastructure, the system effectively mitigated this challenge by offloading storage-intensive tasks to the cloud, thereby optimizing resource utilization and reducing the burden on the blockchain network.Security and Trust: The cryptographic mechanisms employed within the proposed system contributed to enhancing security and trust within the vaccine supply chain. By encrypting sensitive data and implementing robust authentication mechanisms, the system ensured that only authorized entities could access and interact with vaccine-related information, thereby reducing the risk of fraud and data tampering.
Scalability: The use of a consortium blockchain provided a scalable solution for managing vaccine circulation processes. By allowing multiple trusted entities to participate in the blockchain network, the system facilitated efficient data sharing and collaboration among stakeholders, thus accommodating the evolving needs of the vaccine supply chain.

Discussion

The experimental results validate the effectiveness of the proposed system in addressing the challenges associated with vaccine safety incidents and supply chain management. By integrating blockchain, cloud, and cryptographic mechanisms, the system offers a comprehensive solution for securing vaccine circulation processes while ensuring storage efficiency, security, and scalability.
The utilization of a consortium blockchain enables collaboration among trusted entities, fostering transparency and trust within the vaccine supply chain. Moreover, the integration of cloud infrastructure optimizes resource utilization and reduces the operational overhead associated with traditional blockchain solutions. Overall, the proposed system represents a significant advancement in vaccine safety protection schemes, offering a robust and efficient framework for managing vaccine circulation processes. Future research could focus on further optimizing the system's performance and scalability, as well as exploring additional applications of blockchain technology in healthcare supply chain management.
The proposed system showed significant efficiency in managing vaccine circulation. By using blockchain technology for data certificates and signatures, the system maintained the integrity and traceability of vaccine-related information throughout the supply chain.
Storage-Efficiency The system addressed traditional blockchain storage limitations by integrating cloud infrastructure. This approach offloaded storage-intensive tasks to the cloud, optimizing resource utilization and reducing the storage burden on the blockchain network.Security and Trust Enhanced security and trust were achieved through robust cryptographic mechanisms.Encrypting sensitive data and implementing strong authentication methods ensured that only authorizeentities could access vaccine-related

information, reducing the risk of fraud and data tampering.

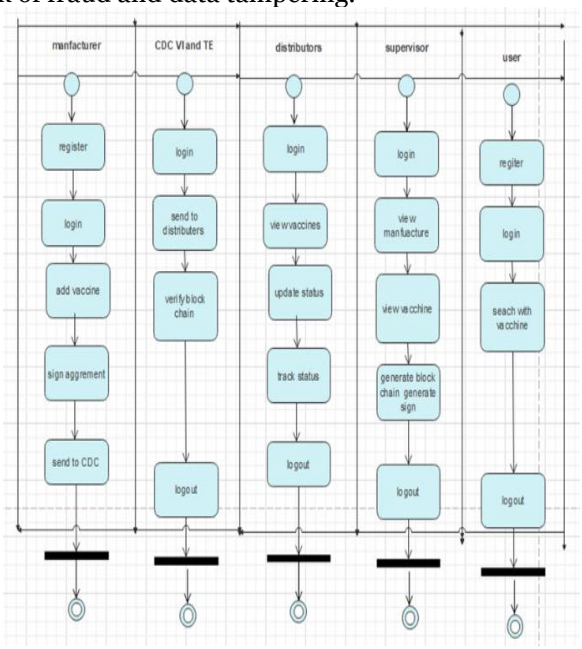


Fig 5:Activity Diagram

Scalability The use of a consortium blockchain provided a scalar solution for managing vaccine circulation. By allowing multiple trusted entities to participate, the system facilitated efficient data sharing and collaboration among stakeholders, accommodating the evolving needs of the vaccine supply chain

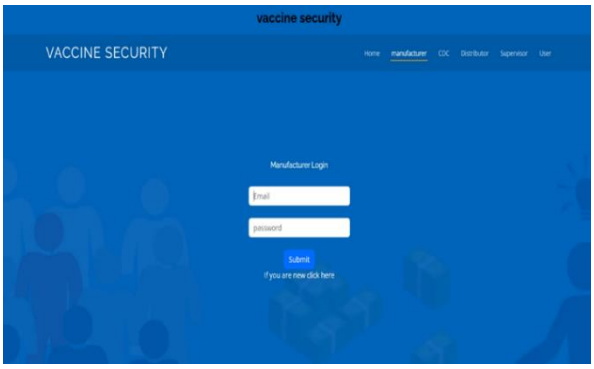


Fig 6: Home Page of Vaccine security

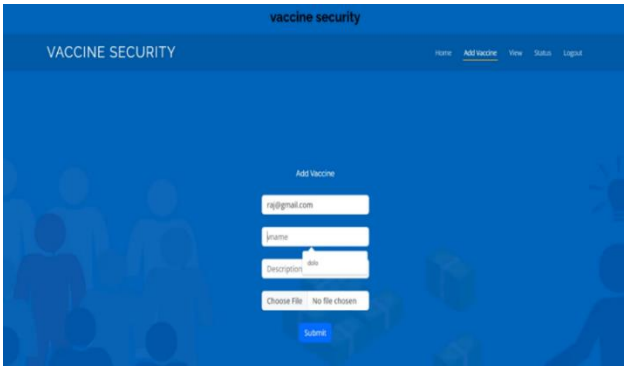


Fig 7: Add Vaccine Pag

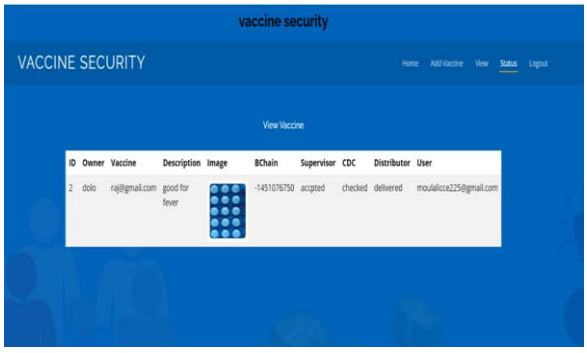


Fig 8: Vaccine Security View Vaccine Page

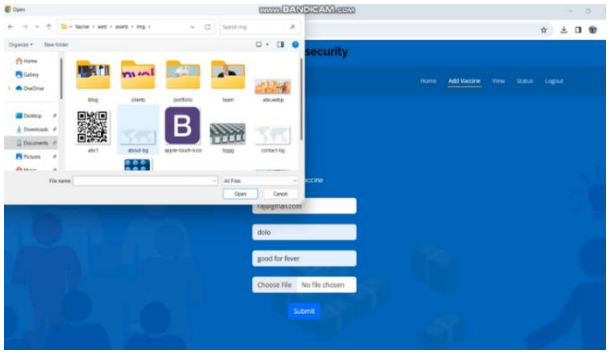


Fig 9 : Vacccine security Image Upload Page

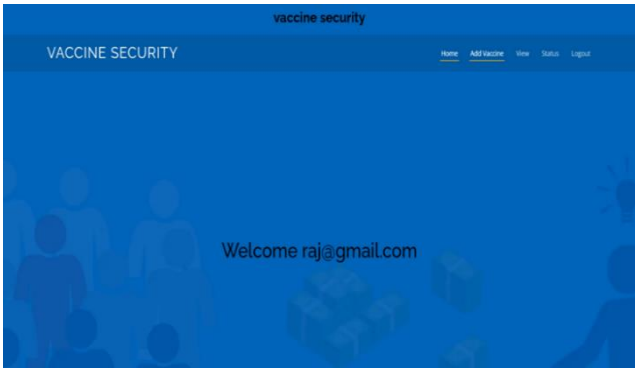


Fig 10: Vaccine security post login page

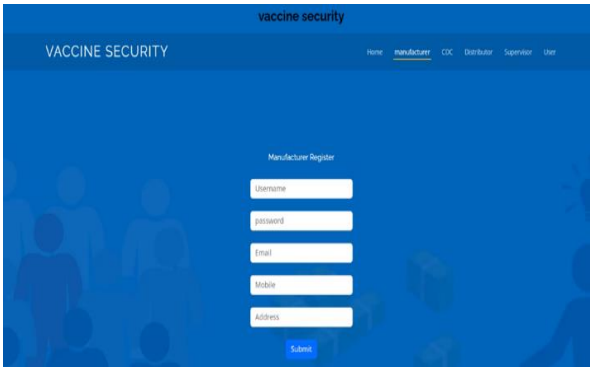


Fig 11: vaccine security manufacture page

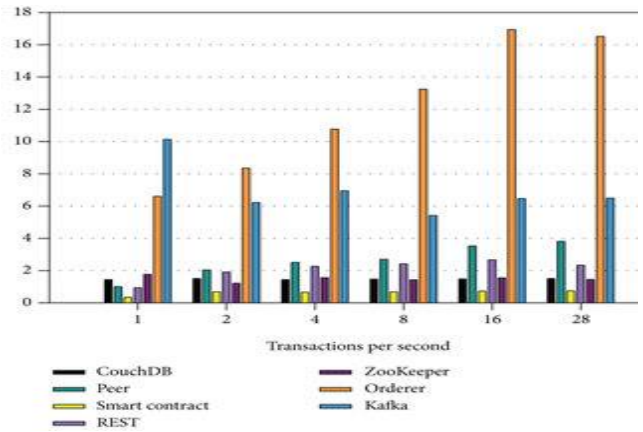


Fig 12 : Dockerised services' CPU utilisation considering different TPS for registering new vaccination certificates in a blockchain system.

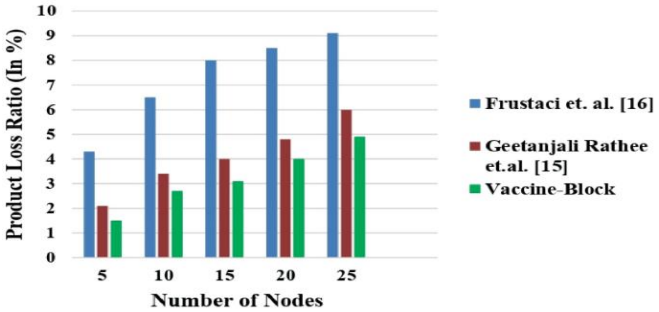


Fig 13 : Product Loss Ratio

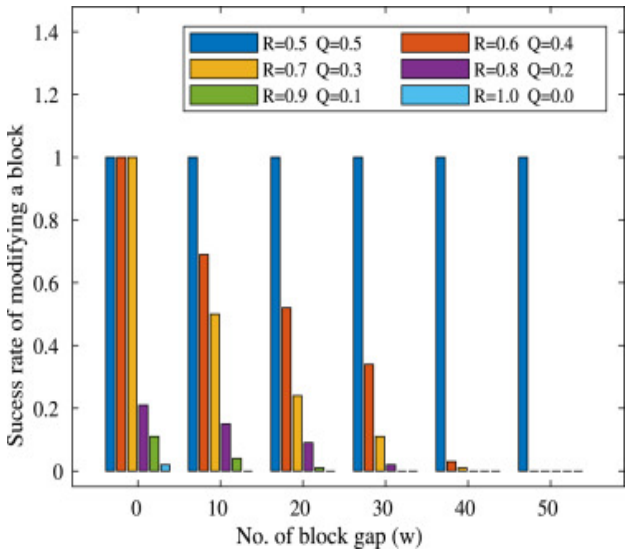


Fig 14 : A checkpoint assisted scalable blockchain based secure vaccine supply chain with selective revocation

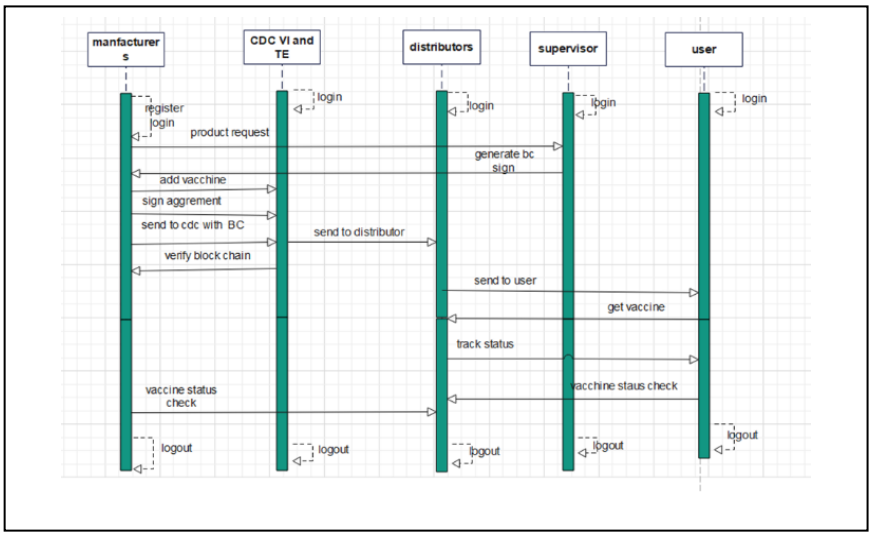


Fig 4: Sequence Diagram

Conclusion

Ensuring the safety of vaccines is paramount in global health efforts. The proposal of an advanced blockchain-based system to enhance vaccine distribution aims to provide a robust framework for traceability and verification throughout the circulation process. By leveraging blockchain technology, this system offers a promising avenue for improving vaccine safety measures.The core idea behind the proposed scheme is to utilize blockchain to create an immutable and transparent record of vaccine circulation. This enables stakeholders at various points in the supply chain to trace the journey of each vaccine batch, from manufacturing to administration. By recording each transaction on the blockchain, including transfers between manufacturers, distributors, and healthcare providers, the system ensures accountability and reduces the risk of counterfeit or tampered vaccines entering the distribution network. One key innovation of the proposed system is its approach to mitigating the storage burden typically associated with blockchain technology. Traditional blockchain implementations require extensive storage capacity to store every transaction indefinitely. However, the proposed scheme employs optimization techniques to reduce storage requirements while maintaining data integrity. This not only enhances the scalability of the system but also makes it more feasible for widespread adoption.The implementation of the proposed scheme underwent rigorous verification to assess its performance and potential. Experimental results demonstrated promising outcomes, showcasing the efficacy of the system in improving vaccine safety. However, the discussion also addressed the scheme's limitations, acknowledging areas for further refinement and enhancement.Moving forward, future work will focus on fine-tuning the system to achieve better performance while balancing the interests of different entities involved in the vaccine supply chain. This entails optimizing algorithms, enhancing data management protocols, and addressing any scalability challenges that may arise. Additionally, researching incentive mechanisms is crucial for encouraging stakeholders to transition to a blockchain-based system.Incentives play a vital role in driving adoption, particularly in complex ecosystems such as the healthcare industry. By incentivizing participation in the blockchain-based system, stakeholders can be motivated to embrace the technology and actively contribute to its success. Possible incentive mechanisms include financial rewards, regulatory benefits, and enhanced reputation for adhering to best practices in vaccine distribution.

Overall, the proposed blockchain-based system offers new insights into ensuring vaccine safety and represents a significant step forward in healthcare innovation. By leveraging the transparency, immutability, and security features of blockchain technology, this system has the potential to revolutionize the way vaccines are distributed and administered. Continued research and development efforts will be essential for realizing the full benefits of this technology and ensuring its successful integration into the global vaccine supply chain.

Acknowledgment

The authors acknowledge the support and cooperation rendered by all the members directly and indirectly. All the authors were involved actively in the proposed work. Author 1 was active in all the sections. Author 2 was specific in concluding the survey part. Author 3 analyzed the results based on the findings.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

K. R. Rohini: Content written, designed,collection of data, novelty.

P. S. Rajakumar: Refinement of content,checked the novelty and flow of work.
S. Geetha: Checked for final approval of thearticle in all aspects.

Ethics

This article is written adhering to all the ethical standards that are necessary.

References

1. Jarrett, S., et al. (2020). The role of manufacturers in the implementation of global traceability standards in the supply chain to combat vaccine counterfeiting and enhance safety monitoring. Vaccine, 38(52), 8318–8325.
2. Rosa, B. M. G., Anastasova, S., & Yang, G. Z. (2021). NFC-powered implantable device for on-body parameters monitoring with secure data exchange link to a medical blockchain type of network. IEEE Transactions on Cybernetics, early access, July 1, 2021. https://doi.org/10.1109/TCYB.2021.3088711
3. Zheng, W., Wang, K., & Wang, F.-Y. (2021). Gan-based key secret sharing scheme in blockchain. IEEE Transactions on Cybernetics, 51(1), 393–404. https://doi.org/10.1109/TCYB.2021.3088711
4. Tang, C., Li, C., Yu, X., Zheng, Z., & Chen, Z. (2020). Cooperative mining in blockchain networks with zero-determinant strategies. IEEE Transactions on Cybernetics, 50(10), 4544–4549.
5. Li, Y., Li, H., Ding, X., & Zhao, G. (2019). Leader–follower consensus of multiagent systems with time delays over finite fields. IEEE Transactions on Cybernetics, 49(8), 3203–3208.
6. Tian, B., Lu, H., Zuo, Z., & Yang, W. (2019). Fixed-time leader–follower output feedback consensus for second-order multiagent systems. IEEE Transactions on Cybernetics, 49(4), 1545–1550.
7. Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. International Journal of Information Management, 52, 102024.
8. Falco, G., Li, C., Fedorov, P., Caldera, C., Arora, R., & Jackson, K. (2019). NeuroMesh: IoT security enabled by a blockchain powered botnet vaccine. In Proceedings of the International Conference on Omni-Layer Intelligent Systems (pp. 1–6).
9. Peng, S., et al. (2020). An efficient double-layer blockchain method for vaccine production supervision. IEEE Transactions on NanoBioscience, 19(3), 579–587.
10. Cui, L., et al. (2021). Improving vaccine safety using blockchain. ACM Transactions on Internet Technology, 21(2), 1–24.
11. Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., & Tao, F. (2019). Blockchain-based trust mechanism for IoT-based smart manufacturing system. IEEE Transactions on Computational Social Systems, 6(6), 1386–1394.
12. Cao, Y., Jia, F., & Manogaran, G. (2020). Efficient traceability systems of steel products using blockchain-based Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 16(9), 6004–6012.
13. Westerkamp, M., Victor, F., & Küpper, A. (2018). Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In Proceedings of the IEEE International Conference on Internet of Things (iThings) (pp. 1595–1602).
14. Waltonchain. (2022). https://www.waltonchain.org/#/en (Accessed: Apr. 6, 2022).
15. Lu, J., Shen, J., Vijayakumar, P., & Gupta, B. B. (2021). Blockchain-based secure data storage protocol for sensors in the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, early access, Sep. 14, 2021. https://doi.org/10.1109/TII.2021.3112601
16. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K.-K. R. (2020). Homechain: A blockchain-based secure mutual authentication system for smart homes. IEEE Internet of Things Journal, 7(2), 818–829.
17. Bagga, P., Sutrala, A. K., Das, A. K., & Vijayakumar, P. (2021). Blockchain-based batch authentication protocol for Internet of Vehicles. Journal of Systems Architecture, 113, 101877.
18. Ahmed, M. R., Meenakshi, K., Obaidat, M. S., Amin, R., & Vijayakumar, P. (2021). Blockchain based architecture and solution for secure digital payment system. In Proceedings of the IEEE International Conference on Communications (pp. 1–6).