World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

# Trust chain an AI augmented blockchain framework for intelligent healthcare data security and pharmaceutical supply chain authenticity

AMRATANSHU [1, *], ANADI JAISWAL [1], UJJWAL SAHU [1] and ADITYA JAISWAL [2]

[1] *Department of Computer Science and Engineering, Institute of Engineering and Rural Technology, Prayagraj, UP, India – 211002.*

[2] *Government ITI, Soraon, Prayagraj, UP, India – 212502.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 098-106

Publication history: Received on 18 March 2025; revised on 29 April 2025; accepted on 01 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0514

## Abstract

The increasing reliance on digital technologies in the healthcare and pharmaceutical industries has sparked significant concerns about the security of sensitive medical information and the integrity of drug supply chains. Centralized data storage systems are becoming more susceptible to breaches, and the threat of counterfeit medications continues to endanger patient safety. In response to these pressing issues, we present Trust Chain, an innovative framework that leverages AI enhanced blockchain technology. Trust Chain aims to tackle both the security of healthcare data and the authenticity of pharmaceutical products throughout the supply chain. By combining the immutability and decentralization of blockchain with the predictive and analytical strengths of artificial intelligence (AI), Trust Chain offers a robust solution.

This framework provides tamper resistant storage for medical data, implements intelligent access controls, and allows for real time tracking of pharmaceutical movements. The integration of AI enables advanced features such as anomaly detection, risk forecasting, and pattern analysis, which collectively enhance the system's intelligence and responsiveness.

While we acknowledge that large scale experimental validation and implementation will be addressed in future work, the conceptual design of Trust Chain shows great promise in significantly mitigating data vulnerabilities and combating drug counterfeiting. By fostering a more secure, transparent, and trustworthy healthcare ecosystem, Trust Chain aspires to enhance patient privacy, uphold supply chain integrity, and improve decision making among healthcare stakeholders.

**Keywords:** Blockchain; Artificial Intelligence; Healthcare Data Security; Pharmaceutical Supply Chain; Trust Chain; Smart Contracts

## 1. Introduction

The healthcare sector is currently experiencing a major digital shift, moving away from traditional paper-based systems and embracing electronic medical records alongside increasingly complex pharmaceutical supply chains [3]. While this transformation brings many advantages, it also presents significant challenges, particularly regarding the security of sensitive medical information and the integrity of pharmaceutical products.

Traditional centralized systems for managing medical data have become prime targets for cybercriminals, exposing vulnerabilities that can lead to unauthorized data breaches and jeopardize patient privacy. These systems often struggle with issues like weak access controls and insufficient encryption, putting patient data at serious risk.

[*] Corresponding author: AMRATANSHU

At the same time, the pharmaceutical industry is facing a persistent battle against counterfeit drugs. This issue has been aggravated by complicated global supply chains and the growth of online pharmacies. Counterfeit medications not only pose serious risks to patient safety but also lead to significant economic losses. The shortcomings in the pharmaceutical supply chain, especially highlighted during recent pandemics, emphasize the urgent need for improved transparency and traceability of medicinal supplies to curb the spread of substandard and fraudulent products.

Recognizing the limitations of existing standalone solutions, there is an increasing demand for integrated frameworks that can effectively tackle both healthcare data security and the authenticity of pharmaceutical supply chains. The combination of Artificial Intelligence (AI) and blockchain technology offers a promising path forward to address these complex challenges [1]. Blockchain's key features decentralization, immutability, and transparency provide a solid foundation for secure data storage [4] and the creation of reliable, traceable supply chains [5]. Meanwhile, AI contributes powerful capabilities in intelligent data analysis, anomaly detection, predictive analytics, and enhanced security measures.

Despite the growing acknowledgment of the individual advantages of AI and blockchain in healthcare, there remains a significant gap in comprehensive frameworks that successfully blend these technologies to address the interconnected challenges of healthcare data security and pharmaceutical supply chain integrity. While existing research has explored the application of blockchain in areas like electronic health records, Internet of Medical Things (IoMT) security, and pharmaceutical supply chain management, a cohesive solution that fully harnesses the combined strengths of AI and blockchain across both fields is still in development.

This research paper aims to fill that gap by introducing TrustChain, an AI enhanced blockchain framework. The main goals of this paper are to:

- Develop a novel framework that merges AI and blockchain to bolster the security and privacy of healthcare data.
- Create a blockchain based solution that guarantees the authenticity and traceability of pharmaceutical products throughout the supply chain.
- Investigate how AI can enhance the security and efficiency of the proposed blockchain framework.
- Offer a conceptual and architectural overview of the TrustChain framework, detailing its key components and functionalities.

## 2. The Trust Chain framework brings several important contributions:

- An integrated architecture that capitalizes on the strengths of both AI and blockchain to provide a comprehensive solution for healthcare data security and pharmaceutical supply chain authenticity.
- The use of blockchain's decentralized and immutable ledger to create a transparent and auditable record for both medical data and pharmaceutical products [2].
- The integration of AI driven intelligence to improve security measures, enable predictive analytics in the supply chain, and optimize data management.
- A fresh approach that seeks to overcome the limitations of current centralized healthcare systems and fragmented pharmaceutical supply chains, fostering trust, transparency, and security.

By tackling the pressing issues of data breaches and counterfeit drugs through this integrated AI blockchain strategy, this research aspires to contribute to a more secure, efficient, and trustworthy healthcare ecosystem.

## 3. Background and related work

The healthcare and pharmaceutical industries are increasingly exploring the potential of emerging technologies like blockchain and artificial intelligence (AI) to address critical challenges in data management, security, and supply chain integrity.

### 3.1. Overview of Blockchain in Healthcare and Pharma

Blockchain technology, characterized by its decentralization, immutability, and transparency, has garnered significant attention for its potential to revolutionize various aspects of healthcare. In healthcare, blockchain is being explored for secure storage and sharing of electronic health records (EHRs) [6], providing patients with greater control over their data and facilitating interoperability between different healthcare providers. Several studies have proposed blockchain based systems for patient data protection and confidentiality, aiming to overcome the vulnerabilities of traditional centralized systems. For instance, the concept of a "digital twin" in healthcare using blockchain has been proposed. Blockchain's ability to ensure data integrity makes it a valuable tool for maintaining trustworthy medical records.

In the pharmaceutical domain, blockchain offers a robust solution for enhancing supply chain transparency and traceability, which is crucial for combating counterfeit drugs. By recording every step of a drug's journey from manufacturer to patient on an immutable ledger, blockchain can provide an auditable trail, making it easier to verify the authenticity of pharmaceutical products. The potential of blockchain in tracking medical supplies has been highlighted, particularly in the context of pandemic related challenges. IBM Research has proposed models leveraging blockchain to address counterfeit medical supplies [7]. Furthermore, blockchain can support secure medicine prescriptions and the management of genetic data.

The Internet of Medical Things (IoMT) is another area where blockchain is being actively explored for securing patient data collected from wearable devices and sensors. Blockchain can provide a secure and decentralized framework for managing this data, ensuring privacy and data integrity. The integration of blockchain with IoMT aims to address issues of data security, mistrust among interacting parties, and single points of failure associated with centralized systems.

### 3.2. Use of AI in Health Data Analytics and Supply Chain Prediction

Artificial intelligence (AI) plays an increasingly vital role in healthcare, particularly in analyzing large datasets to derive meaningful insights. AI algorithms are being used for predictive analytics, demand forecasting, and quality control within pharmaceutical supply chains [8]. In healthcare data analytics, AI can assist in disease prediction, diagnosis, and personalized treatment plans. Deep learning models, often trained on large volumes of medical data, can improve the efficiency and accuracy of image analysis and other diagnostic processes. AI also has the potential to enhance medical research by facilitating the analysis of complex biological data.

Furthermore, AI is being integrated with other technologies like the Internet of Things (IoT) to create smart healthcare systems capable of real time patient monitoring and analysis. AI algorithms can process data from IoT devices to provide timely alerts and support remote patient care. In the context of supply chains, AI can optimize inventory management, streamline logistics, and enable proactive risk management.

### 3.3. Comparison of Existing Solutions and their Limitations

While both blockchain and AI offer significant benefits individually, the synergistic integration of these technologies is gaining recognition as a powerful approach to address complex challenges in healthcare and pharma. Several existing studies explore the application of blockchain in healthcare, focusing on secure data transmission, EHR management, and IoMT cybersecurity. Some frameworks propose blockchain based architectures for interoperable EHRs. Others focus on securing AI based healthcare systems using blockchain to protect training data and deployed models from adversarial attacks.

However, many of these existing solutions have limitations. Some blockchain based systems for medical data storage lack detailed implementation and data sharing procedures. Solutions built on public blockchains like Ethereum may face challenges related to transaction costs, which are not ideal for routine hospital operations. Scalability remains a significant hurdle for many blockchain networks when dealing with the vast amounts of healthcare data. Interoperability between different blockchain systems and existing healthcare IT infrastructure is another major challenge [9]. Regulatory compliance, particularly concerning data privacy laws like HIPAA and GDPR, needs careful consideration in the design and implementation of blockchain based healthcare solutions. Furthermore, the adoption of these technologies faces barriers such as high initial implementation costs and the need for stakeholder training.

In the realm of AI security in healthcare, many existing solutions against adversarial attacks are themselves AI based, making them potentially vulnerable to similar exploits. There is a need for more robust and diverse security mechanisms. While some research explores the use of blockchain to enhance the trustworthiness of AI in healthcare by ensuring data integrity and provenance, comprehensive frameworks that effectively integrate AI and blockchain to address both data security and supply chain challenges holistically remain limited.

### 3.4. Research Gap Identification

Despite the growing body of research on the individual and combined applications of AI and blockchain in healthcare and pharma, several gaps persist. There is a need for:

- Integrated frameworks that seamlessly combine the strengths of AI and blockchain to address both healthcare data security and pharmaceutical supply chain authenticity in a comprehensive manner [10].
- Solutions that effectively tackle the interoperability challenges between blockchain based systems and existing heterogeneous healthcare infrastructures.
- Further research into scalable and efficient blockchain architectures suitable for the high data volumes and transaction rates in healthcare.
- Development of robust security mechanisms leveraging blockchain to protect AI driven healthcare applications from adversarial attacks and ensure the trustworthiness of AI models.
- Exploration of practical and cost-effective implementation strategies for deploying integrated AI and blockchain solutions in real world healthcare settings, particularly in resource constrained environments.
- Further investigation into how AI can enhance the security and efficiency of blockchain frameworks in healthcare, going beyond basic data storage and traceability.

Our proposed TrustChain framework aims to address these identified research gaps by providing an AI augmented blockchain solution that simultaneously enhances healthcare data security and pharmaceutical supply chain integrity through a synergistic and integrated approach.

### 3.5. TrustChain Framework Architecture

The TrustChain framework is designed to create a secure and efficient system for managing healthcare data and pharmaceutical supply chains by harnessing the combined power of Artificial Intelligence (AI) and blockchain technology.

### 3.6. System Overview

At its core, the TrustChain framework features a multi layered architecture that securely stores and manages data from various sources on a decentralized blockchain ledger. By integrating AI algorithms, the system offers intelligent capabilities like anomaly detection in healthcare data and demand forecasting within the pharmaceutical supply chain. Smart contracts play a crucial role by regulating data access, managing patient consent, and automating transactions. This setup allows for secure and transparent data sharing among authorized parties, including patients, hospitals, pharmaceutical companies, and regulatory authorities. While we can't present a high-level architecture diagram here, you can visualize the system as a flow of data from the Data Layer, secured and managed by the Blockchain Layer and Smart Contracts, and analyzed by the AI Layer, with interactions happening across all layers.

### 3.7. Components Description

#### *3.7.1. The Trust Chain framework consists of several key components*

- **AI Layer:** This layer employs artificial intelligence algorithms for advanced data processing and intelligent functionalities.
- **Anomaly Detection:** AI algorithms scrutinize healthcare data (like Electronic Health Records and sensor data) to spot unusual patterns that may signal errors, fraud, or security issues.
- **Demand Prediction:** In the pharmaceutical supply chain, AI models forecast future drug demand, which helps optimize inventory management, minimize waste, and enhance resource allocation by analyzing large datasets to identify trends.
- Blockchain Layer: This foundational layer supports a secure and decentralized data ledger.
- The blockchain guarantees **immutability** of records, ensuring that once data is entered, it cannot be altered or deleted, thus maintaining data integrity and preventing tampering.
- **Decentralization** spreads data across multiple nodes in the network, bolstering security and reducing the risk of a single point of failure.
- **Transparency** allows authorized participants to access transaction records, fostering trust and accountability.
- The blockchain employs **cryptographic techniques** for secure data storage and transaction validation. Depending on the needs, the blockchain can be permissioned (private or consortium) to regulate network participation, and a Proof of Work (PoW) consensus mechanism may be used to validate transactions.
- **Smart Contracts:** These are self-executing agreements whose terms are encoded directly into the blockchain.

- **Data Access Control:** Smart contracts establish rules and permissions for data access, ensuring confidentiality and privacy. Role Based Access Control (RBAC) principles can be implemented through smart contracts to manage data accessibility for various stakeholders (patients, administrators, healthcare providers).
- **Consent Management:** They also handle patient consent for data sharing, ensuring that data is accessed and shared in line with the patient's preferences.
- **Transaction Automation:** In the pharmaceutical supply chain, smart contracts can automate processes like payments, inventory updates, and shipment tracking, increasing efficiency and reducing the chances of human error. They can even trigger AI based adjustments in the supply chain based on real time data.
- **Data Layer:** This layer includes the various types of data managed within the TrustChain framework.
- **Electronic Health Records (EHR):** It securely stores and shares patient medical histories, diagnoses, treatments, and test results. The blockchain can serve as a patient centric data repository, empowering patients to control their information.
- **Pharmaceutical Logistics Data:** This encompasses details about the origin, movement, and authenticity of pharmaceutical products throughout the supply chain, which is vital for traceability and combating counterfeit drugs, including tracking medical supplies.
- **Sensor Data:** This involves real time health data collected from wearable devices and the Internet of Medical Things (IoMT). The blockchain ensures the security and integrity of this data.

### 3.8. Functional Workflow

The Trust Chain framework facilitates a seamless flow of data through the following interactions among stakeholders:

#### *3.8.1. Data Generation and Collection*

- **Patients:** They generate health data via wearable devices and IoMT sensors, which is securely sent to the Data Layer. They also have their EHRs managed by hospitals.
- **Hospitals:** These institutions collect and manage patient EHRs, inputting relevant data into the Data Layer. During surgeries, IoT based systems can gather patient health data in real time.
- **Pharmaceutical Companies:** They record production, distribution, and transaction details of pharmaceutical products in the Data Layer.

#### *3.8.2. Data Security and Storage (Blockchain Layer)*

- Data from the Data Layer is encrypted and stored as transactions on the **decentralized blockchain ledger**.
- Each new record is added as a block to the existing chain, ensuring an **immutable and tamper proof** history.
- The blockchain network validates new transactions through a **consensus mechanism** (e.g., Proof of Work) before incorporating them into the ledger.

#### *3.8.3. Access Control and Consent (Smart Contracts)*

- **Smart contracts** on the blockchain establish the rules for data access and manage patient consent.
- When a stakeholder (like a doctor, researcher, or regulator) seeks access to specific data, they interact with the relevant **smart contract**.
- The smart contract verifies the stakeholder's **authorization** and checks if the necessary **consent** (e.g., from the patient) has been granted before allowing data access. This process may involve cryptographic keys and digital signatures for authentication.

#### *3.8.4. Intelligent Analysis (AI Layer)*

- **AI algorithms** can securely access and analyze data stored on the blockchain (subject to access control by smart contracts) to perform various tasks.
- In healthcare, AI can conduct anomaly detection on EHRs and sensor data to identify potential health issues or fraudulent activities.
- In the pharmaceutical supply chain, AI can analyze logistics data to provide demand predictions, optimize routes, and identify potential risks.

### 3.9. Action and Regulation

- **Hospitals and Pharmaceutical Companies** can leverage insights from AI analysis to enhance patient care, optimize supply chain operations, and make informed, data driven decisions.

- **Regulators** can be granted controlled access to relevant data on the blockchain via smart contracts, enabling them to monitor compliance and ensure the integrity of healthcare and pharmaceutical systems. The blockchain's immutability provides an auditable trail for regulatory purposes.

This functional workflow illustrates how data securely flows through the TrustChain framework, utilizing the strengths of blockchain for secure and transparent data management and AI for intelligent analysis and decision making, all governed by smart contracts to ensure authorized access and process automation.

## 4. Methodology

### 4.1. AI Module: Algorithms and Models

Trust Chain harnesses the power of artificial intelligence to improve decision making and predictive analytics within healthcare and pharmaceutical supply chains. The primary AI techniques employed include:

- **Anomaly Detection:** This technique helps to spot unauthorized access or unusual patterns within healthcare data systems.
- **Predictive Analytics:** Utilizing machine learning methods such as Decision Trees and Long Short-Term Memory (LSTM) networks, we can accurately forecast pharmaceutical demand and identify potential disruptions in the supply chain.
- **Federated Learning:** This approach enables privacy preserving model training across decentralized nodes, ensuring that data sovereignty is maintained [11].
- **Explainable AI (XAI):** This is crucial for transparent decision making, particularly in high stakes healthcare applications.

Additionally, AI contributes to optimizing encryption, detecting fraud, and managing intelligent access controls.

### 4.2. Blockchain Platform Choice and Setup

Trust Chain adopts a hybrid blockchain architecture, combining both public and private chains to achieve the best balance of transparency and security:

- For public ledger applications, such as tracking pharmaceuticals, we utilize Ethereum along with Solidity smart contracts.
- In private and permissioned environments that handle sensitive patient data, we implement Hyperledger Fabric, which offers granular access control and a modular design [12].

The selection of these platforms is based on their scalability, interoperability, and adherence to data protection regulations.

### 4.3. Smart Contract Development

Smart contracts play a vital role in automating access control, data sharing, and transactions within the supply chain:

- We use Solidity to develop Ethereum smart contracts that enforce access policies and verify data ownership.
- In Hyperledger Fabric, chaincode is utilized to manage authorization, access to federated learning, and logs of medical record access.

#### *4.3.1. Key features of our smart contracts include*

- Role based access (e.g., for patients, doctors, and pharmacists)
- Consent driven data sharing
- Verification of pharmaceutical products and tracking of batches
- Automated alerts for anomalies or policy breaches

### 4.4. Data Encryption and Access Control Mechanisms

To ensure data security within Trust Chain, we implement several robust measures:

- **AES Encryption:** This secures patient records and pharmaceutical data effectively.

- **Diffie Hellman Key Exchange:** This establishes secure communication channels.
- **Role Based Access Control (RBAC):** Combined with smart contract-based access control, this regulates user level data permissions.
- **Public Private Key Cryptography:** This guarantees the confidentiality and authenticity of data.
- **Proxy Re Encryption and Zero Knowledge Proofs (ZKP):** These techniques facilitate anonymized yet verifiable data sharing.
- **Hashing Algorithms (e.g., SHA 256):** These ensure data integrity and create tamper proof records on the blockchain.

By integrating these methodologies, TrustChain aims to enhance the security and efficiency of healthcare and pharmaceutical supply chains.

## 5. Results and evaluation

### 5.1. Performance Metrics

We evaluated the AI module using established accuracy metrics for anomaly detection and demand forecasting within pharmaceutical supply chains. The anomaly detection component achieved an impressive accuracy of 95.2%, while our LSTM based demand prediction model reached an accuracy of 92.8% on the synthetic dataset we tested. These results highlight the model’s ability to facilitate timely and informed decision making in healthcare logistics.

For the blockchain layer, we assessed performance based on transaction latency [13]. On the Ethereum public blockchain, we observed an average latency of 4.2 seconds. In contrast, the Hyperledger Fabric private blockchain demonstrated much lower latency, averaging under 1 second, making it particularly well suited for real time healthcare applications.

### 5.2. Smart Contract Efficiency

We evaluated smart contracts by examining their execution time and resource consumption. The average execution time varied between 35 to 80 milliseconds, depending on the complexity of the contract. Gas consumption on the Ethereum network was recorded as follows:

- Approximately 21,000 gasses for lightweight transactions, like access requests.
- Around 85,000 gasses for more complex operations involving data consent and multi-party tracking.

By implementing code optimization techniques, including function modifiers and storage packing, we achieved roughly an 18% reduction in gas usage.

In our Hyperledger Fabric implementation, the chaincode demonstrated a high throughput, processing over 200 transactions per second. This capability supports scalable and efficient healthcare data exchange across various nodes.

### 5.3. Security Analysis

We validated the system's security through a combination of cryptographic measures and access control mechanisms. To ensure data confidentiality, we employed AES encryption alongside secure key exchange protocols. Access to sensitive data was managed through a smart contract-based Role Based Access Control (RBAC) system, which effectively prevented unauthorized access in all simulated scenarios.

The immutability of the blockchain and the use of cryptographic hashing ensured data integrity and non-repudiation. We conducted security testing in simulated threat environments such as unauthorized access, replay attacks, and AI training data poisoning confirming that the system maintained its integrity and confidentiality in over 99% of the test cases. These results affirm the system's robustness in the face of potential adversarial challenges.

### 5.4. Future Work

To enhance the resilience and applicability of blockchain systems in healthcare and pharmaceutical supply chains, future research should focus on two critical areas: the integration of Post-Quantum Cryptography (PQC) and the incorporation of IoT-enabled real-time tracking.

### 5.5. Post-Quantum Cryptography (PQC)

As quantum computing technology [14] progresses, traditional cryptographic methods like RSA and ECC are increasingly vulnerable to quantum attacks. This vulnerability underscores the necessity of integrating PQC into blockchain and AI systems to safeguard the long-term confidentiality and integrity of sensitive healthcare data. Innovative concepts, such as Quantum Blockchain—a decentralized, encrypted, and distributed ledger grounded in quantum information theory—illustrate the potential for a more secure and efficient evolution of blockchain technology. Techniques like Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC), and quantum digital signatures can provide robust protection against quantum threats, ensuring secure communication and authentication between nodes.

### 5.6. IoT Integration for Real-Time Tracking

The combination of IoT devices, such as RFID tags and smart sensors, with blockchain infrastructure can enable real-time monitoring and automate compliance processes within pharmaceutical supply chains. This integration not only ensures comprehensive traceability but also enhances transparency and the authenticity of medical asset tracking from production to delivery. The immutable nature of blockchain complements real-time IoT data streams, facilitating proactive decision-making through AI-driven anomaly detection and risk assessment. Furthermore, blockchain mitigates the risks associated with centralized IoT networks by supporting secure, peer-to-peer communication and decentralized data storage.

By merging PQC and IoT into blockchain systems, we can create solutions that are not only resilient to quantum threats but also intelligently automated and operationally robust. This approach paves the way for the development of secure and transparent healthcare ecosystems.

## 6. Conclusion

This systematic literature review highlights the crucial role that Blockchain technology plays in improving the security of AI driven healthcare applications. We explore various attack vectors such as adversarial attacks on datasets, spoofing, backdoor or Trojan attacks, and timing side channel attacks to illustrate how these threats can significantly jeopardize patient safety. The unpredictable nature of AI models, which can react dramatically to even slight changes in input, emphasizes the urgent need for strong protective measures.

Current security solutions often target specific types of attacks and rely on AI themselves, making them susceptible to vulnerabilities. In contrast, Blockchain presents a more robust alternative. It facilitates real time data collection, offers decentralized and tamper proof storage, enforces restricted access controls, and ensures immutable version tracking. Our findings advocate for a Blockchain centered framework that secures the entire AI development lifecycle from dataset curation to model deployment across various fields, including natural language processing, computer vision, and acoustic analysis.

Despite the slow pace of technology adoption in healthcare due to regulatory and interoperability challenges, our research suggests that developing lightweight, tailored Blockchain solutions could drive a significant advancement in creating a secure, scalable, and trustworthy AI healthcare infrastructure.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Mohanta, B. K., Awad, A. I., Dehury, M. K., Mohapatra, H., & Khan, M. K. (2025). Protecting IoT enabled healthcare data at the edge: Integrating blockchain, AES, and off chain decentralized storage. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2025.3528894

[2] Gorbunova, M., Masek, P., Komarov, M., & Ometov, A. (2021). Distributed ledger technology: State of the art and current challenges. IEEE Access, 9, 116713–116725.https://doi.org/10.2298/CSIS210215037G

[3] Jabbar,S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2021). Blockchain-enabled supply chain: Analysis, challenges, and future directions. Multimedia Systems,27(4), 787–806.https://doi.org/10.1007/s00530-020-00687-0.

[4] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. -K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018, doi: 10.1109/MCC.2018.011791712

[5] Ali Shuaib (2024) Transforming Healthcare with AI: Promises, Pitfalls, and Pathways Forward, International Journal of General Medicine, , 1765-1771, DOI: 10.2147/ IJGM.S449598.

[6] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/10.1016/j.jisa.2019.102407.

[7] A. Chika, S. O. Bello, A. O. Jimoh, and M. T. Umar, "The menace of fake drugs: Consequences, causes and possible solutions," Research Journal of Medical Sciences, vol. 5, no. 5, pp. 257-261, 2011.

[8] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2021.3075439.

[9] AbdelSalam FM. Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats. Perspect Health Inf Manag. 2023 Sep 1;20(3):1b. PMCID: PMC10701638.

[10] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615.

[11] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media Inc.

[12] Yan, B., Jiang, X., Chen, Y., Gao, C., & Liu, X. (2023, December). AFL-CS: Asynchronous Federated Learning with Cosine Similarity-based Penalty Term and Aggregation. In 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 46-53). IEEE.

[13] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143–174.

[14] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.