SEVAS Publishing

Computing Technology Research Journal
(Compute. Technol. Res. J. (Jan, 2023) 2(1):40-42)

ISSN: 2583-6501
DOI: 10.58973/CTRJ.xxxxx

BLOCKCHAIN TECHNOLOGY FOR DETECTING FRAUD IN PHARMACEUTICAL SUPPLY CHAIN MANAGEMENT

A. Lalitha Venkatesan, B. Sathis Kumar
School of Computer Science Engineering, Vellore Institute of Technology, Chennai.
Email: sathiskumar.b@vit.ac.in

Received: 10th December 2022, Accepted: 3rd January 2023 and Published: 3rd January 2023

ABSTRACT

Aim: This paper mainly focused on proposing a new pharmaceutical supply chain management system based on block chain technology.
Results: A seven steps pharmaceutical supply chain management is designed based on blockchain technology. The patients are encouraged to access the technology for finding genuinity of the medicine and to reduce fraud detection.
Conclusion: Blockchain is used to make the system more efficient and effective and designing such genuine system with all necessary parameters can boost patient confidence during medication.

Keywords: Pharmaceutical supply chain management, blockchain technology, patients, medicine

HIGHLIGHTS:

1. A seven step pharmaceutical supply chain management is designed based on blockchain technology to avoid fraud detection, counterfeit medicines and to boost patient confidence.

INTRODUCTION

In today's world, not all medicines produced by pharmaceutical companies are genuine, and the demand for medicine has increased exponentially during the pandemic. Ensuring the confidentiality, integrity, and availability of medicines has become crucial in identifying their authenticity. Privacy, security, and reliability remain major concerns in the healthcare industry. A seven step pharmaceutical supply chain management is designed based on blockchain technology to overcome the difficulties faced by patients in detecting fraud medicines.

RESULTS

Pharmaceutical and insurance companies rely on blockchain technology to save and maintain data as smart contracts, including insurance claims, medical record management, biomedical research, and health ledgers. A data-driven architecture (Figure 1) of blockchain includes data-driven applications, supply chain management, and the Internet of Medical Things to support data management and storage. A centralized ledger health information repository (HIR) is also necessary to store all node information. If the HIR fails, there is a risk of data loss or leakage.

The decentralized ledger is continuously connected, and each node is aware of its neighboring node. If one node fails, the other nodes take over the required data from the sibling node, which contains all the information in the form of transaction records. Each transaction is dependent on design but independent in implementation. The Internet of Medical Things (Figure 2) plays an essential role in providing telemedicine services based on data storage and tracking various body parameters through Wi-Fi, LAN, or bluetooth.

Due to the increased number of health records, it is necessary to store data in the cloud. MediRec [1] is a decentralized electronic medical record that supports data authentication, permission, and operations or functions recorded in the blockchain and initiated by smart contracts. MediRec provides complete medical information about the supplier, ensuring confidentiality, auditing, data integrity, and data authentication. Data storage is achieved using third-party apps that can store information in the cloud, particularly on block cloud. Block cloud is provided using blockchain as a service (BAAS), which provides the necessary information which may include Ethereum , R3 Corda, Quorum, chain core, bitcoin and Hyperledger Fabric.

ISSN: 2583-6501
DOI: 10.58973/CTRJ.xxxxx

The steps involved in pharmaceutical supply chain management based on blockchain technology are as follows:

1. Clinical trials are recorded on a blockchain.
2. Upon successful completion of a trial, a block is added to the blockchain.
3. Production of medicine includes recording the time, barcode, lot number, and expiry date on the blockchain.
4. Drugs and medical supplies are distributed to healthcare providers.
5. Healthcare providers, such as hospitals or clinics, access the medical information.
6. They submit the details to the retailer.
7. Patients are encouraged to verify the authenticity of the medicine through the blockchain supply chain management.

Implantable and wearable medical devices (IWMDs) are commonly used to monitor, diagnose, and treat various medical conditions. However, these devices are not immune to failures, making them less reliable and more susceptible to attacks such as hardware failures, wireless attacks, malware or software exploits, and software errors. Wireless Body Area Network (WBAN) connects independent nodes such as sensors and actuators that are located on the body or under the skin. The actuator is equipped with a program to wirelessly change configuration commands and instructions. For devices such as pacemakers, programmers are available in hospitals, and patients should seek a healthcare professional to fine-tune the device according to their needs. Personal medical information is collected, maintained, and stored for further investigation. Each Personal Healthcare System (PHS) consists of four parts: medical sensors, the patient's smartphone or PC, a remote health server, and the doctor's smartphone or PC. The devices are well-monitored and controlled, ensuring proper information exchange without causing any damage to the system. It follows IEEE 802.11 network which relies on proper bandwidth to ease access to the device. Reliability, confidentiality, integrity, availability, and privacy are all important requirements for healthcare systems. However, confidentiality, availability, and integrity are given more importance. Certain Personal Healthcare Systems are capable of being threatened by hardware or software errors, malware attacks, radio attacks, side channel attacks, malicious code, and vulnerability exploits. Failures can be caused by undetected manufacturing defects or wear and tear. For example, certain neurostimulators can cause a patient to experience a jolt, whereas other neurostimulator devices are used.

Fault Tolerant Design

Reliability plays a crucial role in most life-critical healthcare systems that contain complex electronic circuits. To address design inadequacies caused by concurrent detection and correction of fault effects, fault-tolerant designs are necessary. One such scheme is triple modular redundancy (TMR). Implantable wearable medical devices (IWMDs) are becoming increasingly complex, with added functionality and wireless network connectivity, posing challenges in software programmability and reliability. These devices are also susceptible to attacks and threats, affecting their performance. To overcome these issues, fault-tolerant designs can be implemented in critical IWMD functions, either aggressively or non-aggressively, to proactively address potential issues before they reach the market.

CONCLUSION

Identifying the genuineness of medicine is crucial for ensuring that users can consume it without any confusion and are aware of potential reactions. Regular monitoring is essential for achieving the desired level of satisfaction. Although identifying faults in the system is not an easy task, the design and implementation of a system that facilitates fault identification can simplify maintenance. While certain drawbacks persist in even the most efficient systems, the use of blockchain can enhance their effectiveness. The inclusion of all necessary parameters in the design of a genuine system can ensure greater satisfaction. Therefore, continued efforts to develop and refine personal healthcare systems are necessary to optimize their benefits.

REFERENCES

1. https://doi.org/10.1007/978-3-540-39878-3_19
2. http://dx.doi.org/10.7717/peerj-cs.840

SEVAS Publishing

Computing Technology Research Journal
(Compute. Technol. Res. J. (Jan, 2023) 2(1):40-42)

ISSN: 2583-6501
DOI: 10.58973/CTRJ.xxxxx

TABLES & FIGURES:

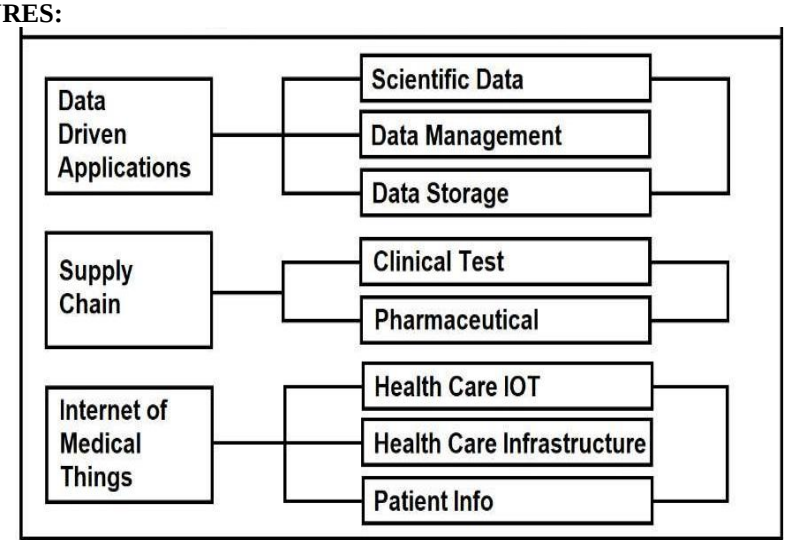

Figure 1: Data Driven Architecture used in blockchain technology

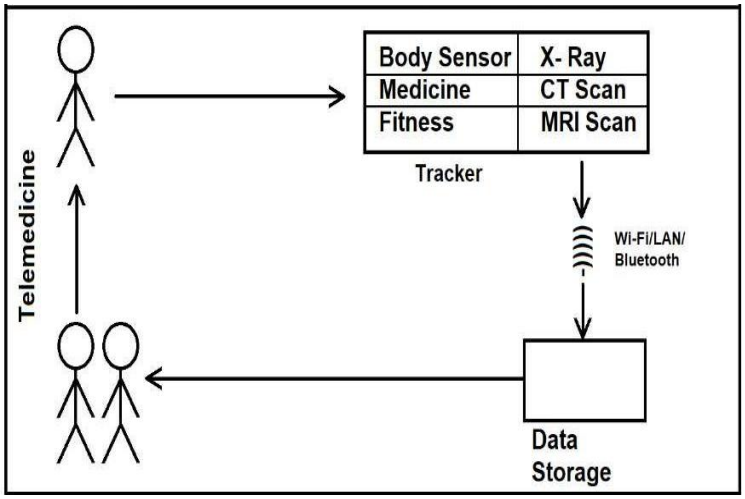

Figure 2: Internet of Medical things (IoMT)