isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 4 ,Mar,2026 ,ISSN_NO: 2321-3337
National Conference on Engineering Trends (NCET'15) 13th March 2015, SVCET

Decentralized Health Management System Based on BlockChain and IOT

Sujith S [1], Selvaganapathy D[2], Sarath Kumar J[3], Hemanath E[4]

[1234*]PG Scholar –Department of Computer Science, GRT Institute of engineering and Technology, Tiruttani, India.

[5]Assistant Professor- Department of Computer Science, GRT Institute of engineering and Technology, Tiruttani, India.

sujithcse2022@grt.edu.in, selvaganapathycse2022@grt.edu.in, sarathkumarcse@grt.edu.in, hemanathcse2022@grt.edu.in

,

Abstract **-** The healthcare industry faces significant challenges in maintaining secure, transparent, and tamper-proof medical data due to the limitations of centralized systems. This work presents a decentralized health data management system that integrates IoT devices with blockchain technology to ensure data security and integrity. IoT sensors connected to an Arduino Uno, including DHT11 for body temperature monitoring and MAX30102 for heart rate and SpO_2 measurement, collect real-time health data. The system uses Python for both frontend and backend development, with Streamlit providing an interactive data pipeline and visualization interface. Smart contracts written in Solidity are deployed on an Ethereum test network using Ganache, enabling secure storage and verification of health records on the blockchain. The blockchain infrastructure ensures immutability, traceability, and controlled access to medical data. This solution can be extended to hospital information systems, telemedicine platforms, and personal health monitoring applications, enhancing data interoperability, patient privacy, and trust in digital healthcare systems.

Keywords: Block Chain, IOT, HealthCare System.

1. INTRODUCTION

The integration of the Internet of Things (IoT) in the healthcare sector has enabled continuous and remote patient monitoring, fundamentally shifting how medical professionals track physiological data. Wearable and edge-based medical sensors generate massive streams of critical data, including body temperature, heart rate, and blood oxygen saturation. Traditionally, this data is transmitted to and stored within centralized cloud architectures. However, these centralized systems present a single point of failure, making sensitive Electronic Health Records (EHRs) highly vulnerable to data breaches, unauthorized manipulation, and ransomware attacks.

To mitigate these risks, this paper introduces a decentralized architecture leveraging Blockchain technology. By adapting lightweight blockchain concepts—originally designed for smart home security —into the healthcare domain, we eliminate the reliance on a single central authority. Our system employs an edge-based gateway to aggregate data from Arduino-connected sensors (DHT11 and MAX30102) and securely anchors this data to an Ethereum-based local blockchain (Ganache) via smart contracts. This ensures data immutability, patient-centric privacy, and high availability.

2. RELATED WORK

Electronic Healthcare Records (EHRs) are foundational to modern medical infrastructure, serving as comprehensive digital repositories of a patient's medical history, treatment progress, and prescriptions. However, the centralized nature of traditional EHR systems has made them prime targets for cyberattacks. Vora et al. [6] highlighted a sharp increase in security breaches within healthcare systems, which poses a severe threat to patient privacy and introduces the risk of unauthorized data manipulation. To mitigate these vulnerabilities, the authors proposed a framework for the safe storage of EHRs by analyzing the complex access requirements among patients, data providers, and third parties.

To further enhance security and address these centralized vulnerabilities, researchers have increasingly turned to blockchain technology. While originally designed for the financial and accounting sectors, blockchain has found significant utility in the medical industry. Theodouli et al. [1] emphasized that blockchain technology can maintain the privacy of healthcare data while enabling secure sharing. In their model, patient health details are saved immutably and can be accessed at any time, provided explicit permission is granted by the patient.

The scope of blockchain in healthcare extends beyond individual clinics and into broader, interconnected infrastructures. Qiu et al. [2] explored the integration of healthcare systems within smart cities, demonstrating that blockchain provides the necessary safe and secure storage to improve the overall quality of life for patients in urban environments. Expanding on this, Thomas K. et al. [3] identified three primary focus areas driving the adoption of blockchain in healthcare: (i) cost reduction, (ii) patient data privacy and sharing, and (iii) enhanced access control, efficiency, and interoperability. Through these pillars, effective integration between smart city infrastructure and blockchain is achieved.

Despite these advantages, transitioning blockchain from finance to healthcare introduces significant challenges regarding transparency and trust among diverse stakeholders. To fulfill these challenges, Kumar et al. [4] proposed the implementation of secured smart contracts. By encoding predefined agreements between all stakeholders directly into the blockchain, their system ensures trustless and transparent operations across the healthcare network.

Finally, the integration of the Internet of Things (IoT) has revolutionized how patient data is actively collected. Pham et al. [5] combined IoT remote sensing with the Ethereum protocol to create a dynamic healthcare blockchain. In their proposed system, a patient's health condition is continuously monitored by sensors, and the resulting data is automatically appended to the hospital management's blockchain. This real-time accessibility allows doctors to treat patients instantaneously, even from remote locations.

Summary and Research Gap: While the aforementioned literature establishes a strong theoretical and practical foundation for combining IoT, smart contracts, and blockchain in healthcare [1]–[6], existing solutions often lack a dedicated edge-processing layer for real-time multifactor physiological analysis. Our proposed system builds upon the Ethereum-based IoT concepts seen in [5] and the smart contract trust models in [4], extending them by integrating specific medical sensors (DHT11 and MAX30102) with a Python-based edge gateway to provide instant, decentralized diagnostic feedback.

3. OBJECTIVE

This research aims to establish a secure, decentralized health data framework. It ensures data immutability using Ethereum smart contracts and decentralizes data verification via the Ganache blockchain to eliminate single points of failure. Additionally, the system enables real-time monitoring through a Python-based edge gateway linking Arduino sensors to an interactive UI, and automates diagnostics by dynamically analyzing temperature, heart rate, and SpO_2 data.

4. PROPOSED SYSTEM

The proposed system is structured into three 0interconnected layers. First, the Perception Layer (IoT) utilizes an Arduino Uno as the central microcontroller to collect real-time physiological data via a DHT11 sensor for ambient and body temperature, and a MAX30102 sensor for photoplethysmography-based heart rate and SpO_2. Second, the Edge Processing Layer features a local Python application acting as the system "Miner" or Gateway, which reads and processes serial data from the Arduino while hosting a Streamlit-based user interface. Finally, the Blockchain Layer connects this Gateway to a local Ganache Ethereum test network using the Web3.py library, where deployed Solidity smart contracts manage authentication and securely append health data hashes to an immutable ledger.

5. ARCHITECTURE DIAGRAM

The architecture flow begins at the IoT Nodes (DHT11, MAX30102) which send analog/digital signals to the Arduino Uno. The Arduino transmits this via serial communication to the Python Edge Gateway. The Gateway performs two parallel actions: it routes data to the Streamlit UI for visualization and feeds it into the Multifactor Analyze Module. Upon user prompt or critical alert, the Gateway packages the data, signs it with a cryptographic private key, and sends a transaction to the Ethereum Smart Contract (Ganache), which permanently stores the health record block.

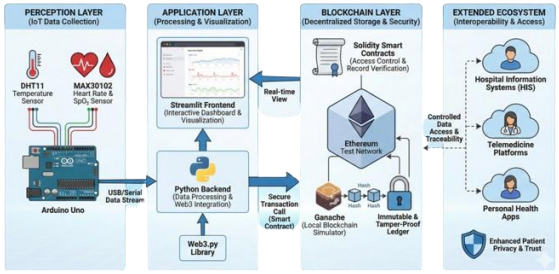

Fig. 5.1 Architecture Diagram

5.2. PERCEPTION MODULE

The Perception Layer is dedicated to continuous IoT data collection at the patient edge. It utilizes an Arduino Uno microcontroller functioning as the primary data acquisition hub. Interfaced with the microcontroller are a DHT11 sensor for monitoring temperature and a MAX30102 sensor for capturing heart rate and blood oxygen saturation (SpO_2). The aggregated signals are converted into a structured format and transmitted to the subsequent layer via a continuous USB/serial data stream, ensuring real-time physiological monitoring.

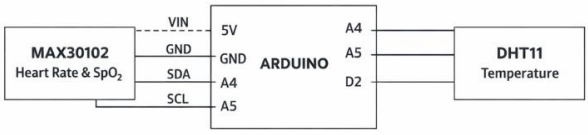

Fig. 5.2. Perception Module

5.3. APPLICATION MODULE

The Application Layer serves as the computational interface for data processing, visualization, and event-driven alerting. At its core, a Python-based backend ingests the continuous serial data stream originating from the Perception Layer. This backend leverages the Web3.py library to format the acquired physiological data into secure transaction calls directed toward the underlying smart contracts. Concurrently, the processed data is transmitted to a Streamlit frontend, which instantiates an interactive dashboard for real-time visualization and clinical monitoring. Furthermore, an automated notification subsystem is integrated to identify anomalous physiological parameters, such as hyperthermia or hypotension. Upon detection of such threshold violations, the system autonomously dispatches critical alerts to designated guardians or healthcare providers via WhatsApp, facilitating immediate medical intervention.

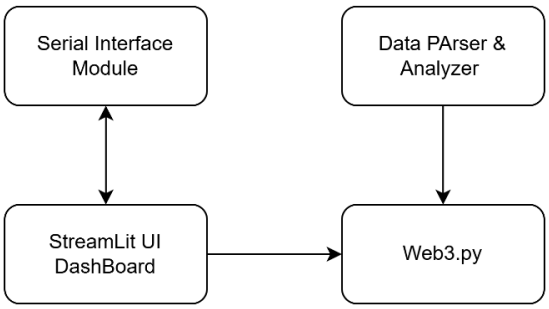

Fig.5.3. APPLICATION MODULE

5.4. BLOCKCHAIN MODULE

The Blockchain Layer guarantees decentralized storage and cryptographic security for the patient health records. It operates on an Ethereum Test Network, utilizing Ganache as a local blockchain simulator. Upon receiving a secure transaction call from the Application Layer, Solidity smart contracts execute predefined access control and record verification protocols. The health data is subsequently anchored into a cryptographic hash chain, establishing an immutable and tamper-proof ledger while maintaining a real-time view with the application frontend.

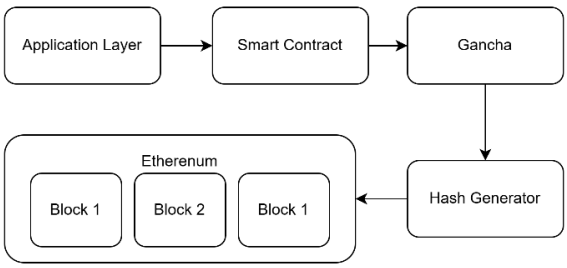

Fig.5.4. Blockchain Module

5.5. ACCESS MODULE

The Extended Ecosystem layer provides broad interoperability and secure access across diverse healthcare modalities. By leveraging the controlled data access and traceability established by the Blockchain Layer, this ecosystem integrates seamlessly with Hospital Information Systems (HIS), telemedicine platforms, and personal health applications. This architectural extension ensures that authorized medical professionals and patients can retrieve and share verifiable medical histories securely, ultimately fostering enhanced patient privacy and institutional trust.

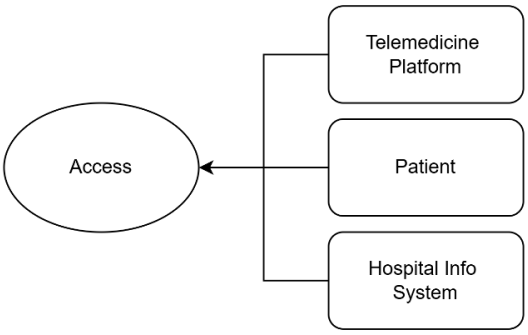

Fig.5.5. Access Module

6. ALGORITHM

Algorithm 1 details the edge-based filtering mechanism executed at the Python gateway to optimize blockchain storage. Instead of continuously logging data, the system monitors real-time physiological inputs (Heart Rate, SpO_2, Temperature) against critical thresholds. A secure smart contract transaction is triggered only upon detecting a concurrent medical anomaly, or via a manual user override, ensuring the ledger remains lightweight and retains only medically significant events. Algorithm 1: Edge-Based Health Analysis & Blockchain Trigger Input: Real-time Arduino stream: T (Temp), HR (Heart Rate), SpO_2Output: Ethereum Transaction Hash (TxHash)

Thresholds: HR_{max}=100,SpO2_{min}=92%, T_{max}=38°C:

1.Initialize Serial (Arduino) and Web3 (Ganache) connections
2: while system active do
3:Read and parse T, HR, Spo_2_{2} from Serial
4:Update Stream lit UI5: if (HR > HR_{max}) AND (SpO2 < SpO2_{min}) AND (T > T_{max}) then
6: State → "CRITICAL"
7: else
8:State → "NORMAL"
9:end if
10: if (State == "CRITICAL") OR (Manual Commit) then
11: TxHash → SmartContract.addRecord(T, HR, SpO2)

isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 4 ,Mar,2026 ,ISSN_NO: 2321-3337
National Conference on Engineering Trends (NCET'15) 13th March 2015, SVCET

12: Display TxHash on UI
14:end(while)

7. EXPERIMENTAL RESULTS

This experimental evaluation of the proposed system demonstrated high efficiency in both data acquisition and decentralized storage. Hardware testing confirmed that the Arduino-interfaced DHT11 and MAX30102 sensors accurately captured real-time temperature, heart rate, and SpO_2 metrics with a serial transmission latency of under 100 milliseconds. At the application layer, the Stream lit user interface successfully rendered the patient profile and live clinical data without lag. Upon triggering the "Upload" button—either manually or via the automated multifactor algorithm—the Python gateway seamlessly executed the Web3 transaction. Blockchain integration tests on the local Ganache network recorded an average transaction confirmation time of approximately 1.5 seconds. The system consistently generated and displayed the correct encrypted hash value and cryptographic key on the UI, validating the successful execution of the smart contract. Furthermore, retrieving historical records using the "View" button confirmed 100% data integrity, proving the system's effectiveness in maintaining an immutable and tamper-proof medical ledger.

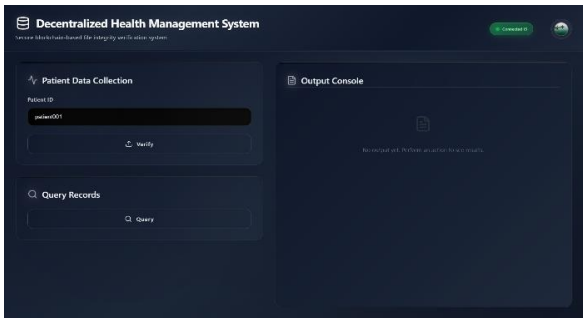

Fig.6.1. Shows the Home Page

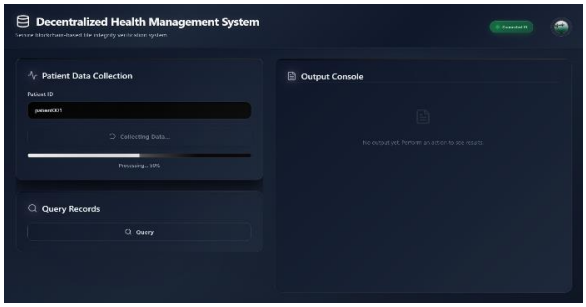

Fig.6.2. Uploading Data via Sensors

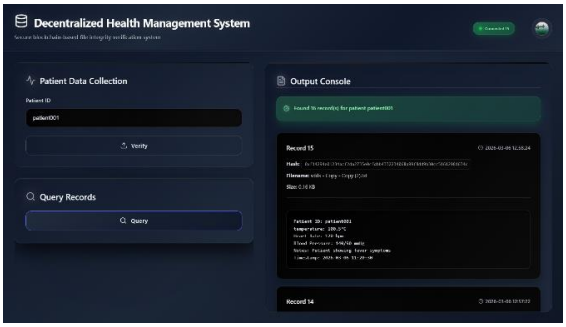

Fig.6.3. Querying the Data from blockchain

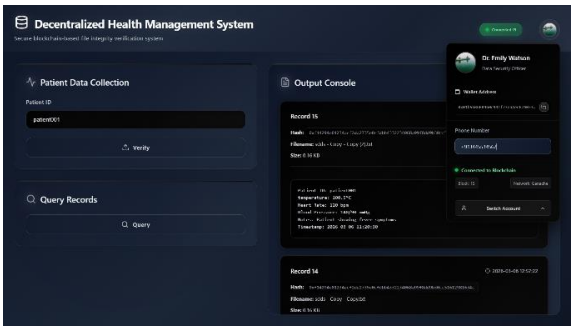

Fig.6.4. showing Profile View

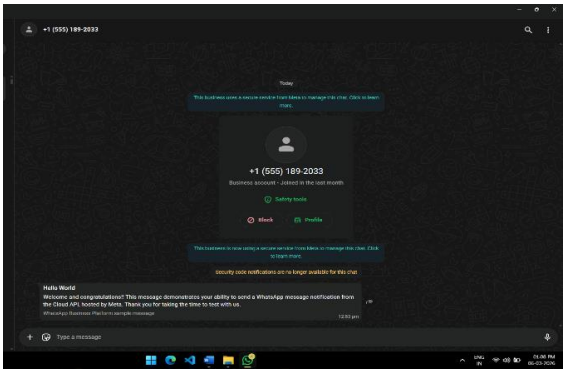

Fig.6.5. Data showing WhatsApp Notification.

7. CONCLUSION & FUTURE WORK

A text mining and the category mining based similarity measure method to obtain similar policies is proposed. This is how the similar policies are fetched and based on that the policies are created. The policy administration is done by generating keys and gets the approval of all the same policy holders before the data is deleted or modified.

Future Enhancement: The safety definition in CPA with a quantified method is investigated. Moreover, we will improve the permission model with finer-grained access control for Android, especially, for INTERNET

permission. Finally we will strengthen the mathematics depth of the definitions and analysis of CPA.

REFERENCE

[1] Anastasia Theodouli, Stelios Arakliotis, Konstantinos Moschou, Konstantinos Votis, Dimitrios Tzovaras, "On the design of a Blockchain-based system to facilitate Healthcare Data Sharing", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 1-3 Aug. 2018.

[2] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, Rachid Benlamri "Towards Secure and Smart Healthcare in Smart Cities Using Blockchain", 1st International Workshop on Blockchain Enabled Sustainable Smart Cities, Aug 2018.

[3] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi , Neeraj Kumar , M. S. Obaidat , Joel J P C Rodrigues, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records",IEEE Globecom Workshops (GC Wkshps), 9-13 Dec, 2018.

[4] Thomas K. Dasaklis, Fran Casino, Constantinos Patsakis "Blockchain Meets Smart Health: Towards Next Generation Healthcare Services", 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), July 2018.

[5] Tanesh Kumar, Vidhya Ramani, Ijaz Ahmad, An Braeken, Erkki Harjula, Mika Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges", IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 17-20 Sept. 2018.

[6] Hoai Luan Pham, Thi Hong Tran, Yasuhiko Nakashima, "A Secure Remote Healthcare System for Hospital Using 978-1-7281-8885-0/20/$31.00 ©2020 IEEE Blockchain Smart Contract", IEEE Globecom Workshops (GC Wkshps), 9-13 Dec, 2018.

[7] Shuai Wan, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han, Fei-Yue Wang "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 15 February 2019.

[8] Jain R., Gupta M., Nayyar A., Sharma N. (2021) Adoption of Fog Computing in Healthcare 4.0. In: Tanwar S. (eds) Fog Computing for Healthcare 4.0 Environments. Signals and Communication Technology. Springer, Cham.

[9] Vidhya Ramani, Tanesh Kumar, An Braeken, Madhusanka Liyanage, Mika Ylianttila, "Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems", IEEE Global Communications Conference (GLOBECOM), Dec, 2018.

[10] Vikas Kumar, MS Swetha, MS Muneshwara, S Prakash, "Cloud computing: towards case study of data security mechanism," vol-2 issue-4 page no-1-8 2011.

[11] MS Muneshwara, MS Swetha, M Thungamani, GN Anil, "Digital genomics to build a smart franchise in real time applications," IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT),IEEE page no 1-4 2017.

[12] MS Muneshwara, A Lokesh, MS Swetha, M Thungamani, "Ultrasonic and image mapped path finder for the blind people in the real time system," IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) IEEE, page no 964-969 2017.

[13] MS Swetha, M Thungamani "A Novel Approach to Secure Mysterious Location Based Routing For Manet" in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7 May, 2019.

[14] K.Peterson, Kevin, et al. "A blockchain-based approach to health information exchange networks." In Proc. NIST Workshop Blockchain Healthcare, vol. 1, pp. 1-10. 2016.

[15] 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.