Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, No. 1, August : 2023

BLOCKCHAIN-BASED HEALTHCARE SYSTEM USING SHA 256 ALGORITHM AND MACHINE LEARNING

Ms. Gayatri Sanjay Rahane, Ms. Manjeet Kaur Mandeep Singh Gahir, Ms. Iqrafatema Rizwan Inamdar, Mr. Atharva Anil Astekar. Student of Final Year Computer Engineering, Guru Gobind Singh Engineering and Research Center Nashik

Abstract
Prescription and Maintenance of Health Records impact the efficiency of healthcare. In medical services, Data Confidentiality and Privacy are critical concerns. For the vast majority of people, Data Security and Secure Storage of Medical Data are always top priorities. A technology platform is necessary for a secure, smooth communication system in a Healthcare System. Blockchain has been evolving technology for a few years now. The main characteristics of Blockchain that draw in the majority of developers are its Distributed Ledger, Decentralization and Immutability. Therefore, Blockchain Technology can be used to safely store personal medical data. Its usage in healthcare systems will have a significant influence. In recent years, there has been a paradigm shift in Health Record storage in Mobile Cloud Environments, with mobile devices integrated with Cloud Computing to facilitate sharing of medical data between Patients and Providers. This Healthcare system enables healthcare services with low operating costs, high flexibility, and high medical data history availability. The proposed system includes Medical History sharing framework that combines Blockchain on a Desktop Application. In particular, we have designed a trusted access control mechanism to securely share health records among various patients and healthcare providers. We present a prototype implementation that predicts the disease and treatment to be prescribed to the patient based on the symptoms using Machine Learning Techniques. In this system, the model helps doctors to examine the symptoms of patients in real-time and make decisions quickly. Thus, a machine learning model uses patient data to make informed predictions which helps in the prescription part. This system includes a hardware USB RFID Card Reader which reads information from RFID cards and communicates with a computer or other devices via a USB interface. The advantage of using this is to get complete information by scanning the card with the unique ID of patients and doctors. The proposed system includes a healthcare system that interacts with Doctors, Patients, and Pharmacies or Medical Stores while securely managing Patient Medical Data.

Keywords:- Blockchain, Patient, Doctor, Medical History, Prescriptions, Claims, Symptoms, Reports, Machine Learning Model, Prediction, RFID Card Reader, RFID Tags.

I. INTRODUCTION

We don't have time to wait in infamously long medical lines in today's busy society. The issue is that the administrative staff at the hospital frequently manages the queue manually. The patient then takes a token, waits for their turn, and asks for the doctor. The most frustrating part is that after traveling a long distance to get there, they learn that the doctor is either on vacation or cannot get an appointment. Second, the confidentiality of medical records is essential to the delivery of quality healthcare since it involves safeguarding the private and sensitive health information of patients. In order to prevent unauthorized access during transmission and storage, medical records should be encrypted.

This system will help us to overcome all these problems because now patients can make appointments at home, and they can check whether the doctor they want to see is available or not. Doctors can also confirm or decline the appointments, which helps both the patient and the doctor because if the doctor declines' the appointment, then the patient will know this in advance and the patient will visit the hospital only when the doctor confirms' the appointment this will save time and money of the patient. Patients can also pay the doctor's consultant fee online to save their time.

This system is essential for all healthcare establishments, be it Hospitals, Nursing Homes, Health Clinics, Rehabilitation Centres, Dispensaries, or Clinics. It is a health care system that securely manages personal medical data and creates interaction between Doctors, Patients, and Pharmacy shops or Medical shops. It mainly focuses on the security of the medical records of every individual, and using blockchain the system will become more efficient for data storage. blockchain technology offers numerous advantages, including decentralization, security, transparency, efficiency and immutable record-keeping.

Aspect mining is a term used in Machine Learning and natural language processing (NLP) referring to the process of extracting specific aspects of a target entity from textual data. It is used to develop clinical decision support systems that provide informed decisions to healthcare providers for diagnosis, treatment planning, and patient management. Thus, helps in healthcare organizations to improve patient care and safety.

The system is divided into 3 parts:

- Patient needs to register and mention the history of medical records in start for further process.
- Doctors will be able to diagnose the illness and to generate an effective prescription.
- According to the prescriptions the Medical Stores can provide the prescribed medicines.

II. BACKGROUND AND LITERATURE REVIEW

"Healthcare System Using Blockchain", Gauri Lodha, Manu Pillai, Ankit Solanki, Sarvesh Sahasrabudhe, Ashwini Jarali, International Conference on Intelligent Computing and Control Systems (ICICCS 2021)[1]

This paper addresses the crucial issues of medical data privacy and data protection. In this paper, a healthcare system was designed that securely manages personal medical data and establishes interactions between doctors, patients, insurance companies, and pharmacies. They have used theconcept of private blockchain which is an efficient way to revolutionize data storage in a healthcare system. This private blockchain will have all the details of doctors, insurance companies with whom the patients have interacted. The transaction and insurance details will be stored with the help of smart contracts.

This paper discusses four modules in which the first module describes the system for patients for storing medical history and booking appointments online. The second module elaborates on the solution for doctors in which doctors can access patients' medical data and treat them accordingly. After treatment, the doctors can then upload prescriptions or suggest lab tests accordingly. The third module is for insurance companies which allows insurance companies to document verification and further processes. This reduces unwanted fraud by patients. The last module is for medical store facilities. As per the prescription by doctors, patients can buy medicines from the store and this information will be stored in the system.

The implementation is done using ganache – a personal blockchain for Ethereum and Corda distributed application development. They have also used TruffleSuite and Meta Mask and an IPFS system for storing all large files. A few of the limitations identified are patients must have mobile phones and an internet connection to interact with the system.

"Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems",Dinh C. Nguyen , Pubudu N. Pathirana ,Ming Ding, Aruna Seneviratne, Institute of Electrical and Electronics Engineers (IEEE 2019)[2]

This paper mainly focuses on sharing of electronic health records (EHRs) with the help of mobile cloud computing and blockchain. This paper proposes a novel EHRs sharing architecture based on blockchain and IPFS for an e-health system on a mobile cloud platform. The authors discuss few of the preliminaries like Ethereum account, smart contracts and Transaction.

It includes a real-time data-sharing scenario on a mobile app with Amazon cloud computing through which patients can collect their personal health information using wearable devices and share it on

cloud environments. The healthcare providers can then access this information and provide timely medical support to the patient.
The platforms used in this paper are – Android, AWS, and Ethereum for Blockchain. Primarily focusing on preventing unauthorized access, the authors presented two use cases of authorized and unauthorized access to evaluate the performance of our Access Control by Designing EHRs sharing model.
This framework enables medical users to share medical data in mobile cloud environments reliably and quickly compared to traditional schemes to achieve the desired level of patient privacy and network security.
"Advanced Healthcare System Using Artificial Intelligence", Santosh Sanjeev, Gowtham Sai Ponniekanti,
G. Pradeep Reddy, International Conference on Cloud Computing, Data Science Engineering (Confluence 2021)[3]
Health is one of the major factors which determines and improves the comfort of humans. Advanced technologies can be used to change the current scenario.
This paper proposed a web interface that enables access of medical records to the patients and a neural network model which predicts medication for ailments.
The author proposes use of speech to text model and applies Natural Language Processing (NLP) on the text to provide patient with a prescription. The author also describes development of a neural network which helps in predicting the medication for a patient based on the symptoms.
The proposed system is explained in three parts in which the first part focuses on the front end of the proposed system which describes the user interface for patients as well as doctors. The second part describes the back-end process of the web application. The third part explains the creation of an AI bot that predicts medication using neural networks. The authors have used HTML, CSS for the front end, and Django for the back end. It has a Word Error Rate of 21.5 percent for the custom-trained speech-to-text model. The AI bot achieved an accuracy of 88 percent.
"Design of a Secure Medical Data Sharing Scheme Based on Blockchain", Xu Cheng, Fulong Chen, Dong Xie, Hui Sun, Cheng Huang, Journal of Medical Systems, Springer [4]
The blockchain's decentralization feature is helpful in solving the problem that the secure authentication process relies heavily on a trusted third party and the implementation of secure data transmission. This paper discusses the use of blockchain technology to describe the security requirements in the authentication process and a blockchain-based MCP network model is proposed.
In the system model, each hospital's medical data hash and location index of abstract and cloud medical data are stored in the medical consortium chain as encrypted text. The author describes BAN logic which helps to prove authentication and key establishment thus proving the validity of the protocol. The paper combines cloud storage with cryptography to analyze the feasibility of blockchain security authentication in MCPs.
"Towards Using Blockchain Technology for eHealth Data Access Management", Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher, International Conference on Advances in Biomedical Engineering (ICABME 2017)[5]
This paper mainly focuses on specific issues and highlights the benefits of blockchain technology in implementing a secure and scalable medical data exchange solution for best performance.
The author mentions it is infeasible and provokes very poor performance to store all the data on the blockchain, so they have used blockchain only to transfer only part of the data and an Off-Chain database is used for storage.
The implementation mentions the use of sensors for generating data which triggers a smart contract that sends a notification to the doctors.
This approach provides a transparent and efficient way to access and share patient data confidentially and securely, with the patient completely in control of his own data. This approach is completely user-centric.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, No. 1, August : 2023

III. PROPOSED SYSTEM

A. ARCHITECTURE

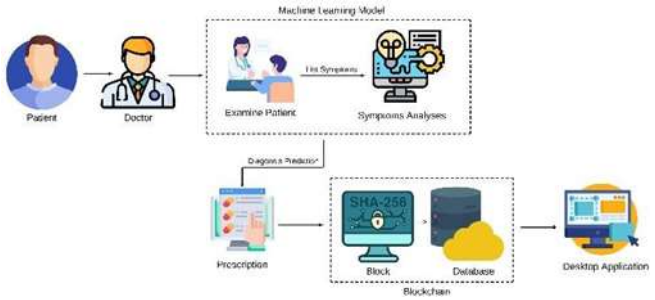

Fig 1: Proposed System

We have designed a trusted access control mechanism to securely share health records among various patients and healthcare providers. We present a desktop application running on firebase cloud that predicts the disease and treatment to be prescribed to the patient based on the symptoms using machine learning technique as well as using blockchain we secure the prescription from being modified. SHA 256 Algorithm is used for the encryption of the prescription and the concept of Aspect Mining is used for Disease Prediction.

This system illustrates the specific problems and highlights the benefits of blockchain technology to deploy a secure and scalable solution for medical data exchange in order to have the best performance possible.

The proposed system includes a healthcare system that interacts with doctors, patients, and pharmacies or medical stores while securely managing patient medical data.

B. METHODLOGY Aspect Mining

Aspect mining is a natural language processing technique that involves identifying and extracting symptoms and risk factors associated with a particular disease from clinical data such as electronic health records (EHRs) or medical literature. This technique aims to automatically identify the most relevant features of a patient's health status or medical history that are associated with a particular disease, which can be used to predict the likelihood of the patient developing the disease or to support clinical decision-making.

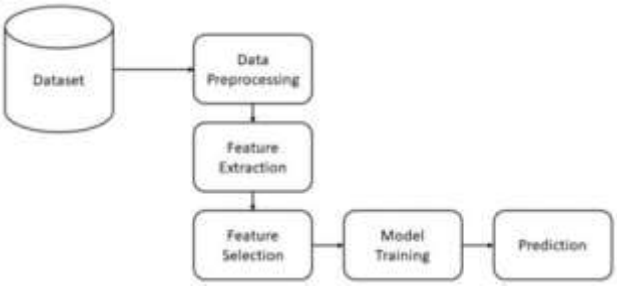

Fig 2: Concept of Aspect Mining

Aspect mining for disease prediction typically involves several steps, including data preprocessing, feature extraction, feature selection, and model training.

Data Preprocessing: In this step the clinical data is cleaned and normalized to remove any noise or irrelevant information.

Feature Extraction: In this step natural language processing techniques are used to identify and extract relevant features such as symptoms, risk factors, and other clinical variables from the preprocessed data.

Feature Selection: In this step the statistical and machine learning techniques are used to identify the most informative features that are most strongly associated with the disease.

Model Training: In this step a predictive model is trained using the selected features to predict the likelihood of the patient developing the disease.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, No. 1, August : 2023

SHA 256 Algorithm

The SHA-256 algorithm is a widely used cryptographic hashing algorithm in the blockchain technology. It is used to secure the integrity of the data stored in the blockchain by producing a unique and irreversible 256-bit hash value for every block.

Fig 3: Structure of Blockchain

Following are the steps to create a block using the SHA 256 algorithm in the blockchain:

- Data Collection: Collect all the necessary data that you want to store in the block. This could be transaction data, digital signatures, timestamps, etc.
- Hashing: Once you have all the data, you need to hash it using the SHA-256 algorithm. This will produce a fixed-length hash value that uniquely identifies the data.
- Creating the Block Header: The block header contains metadata about the block, including the hash of the previous block, the current block's hash, the timestamp, and a nonce.
- Mining: To create a block, you need to solve a complex mathematical puzzle, known as the proof-of-work (PoW). This involves finding a value for the nonce in the block header that, when hashed along with the other data, produces a hash value that meets a specific difficulty target.
- Verification: Once the puzzle is solved, the block is added to the blockchain, and all other nodes on the network verify its validity.

So, in summary, to create a block using the SHA 256 algorithm, you need to collect the necessary data, hash it using SHA-256, create the block header, mine the block, and finally, verify its validity.

IV. RESULTS AND DISCUSSION

We have built a desktop application that predicts the disease and treatment to be prescribed to the patient based on the symptoms using Machine Learning Techniques. In this system the model helps doctors to examine the symptoms of patients in real-time and make decisions quickly. Thus, a machine learning model uses patient data to make informed predictions which helps in the prescription part. Once the prescription is generated it is secured by encrypting it with SHA 256 Algorithm using Blockchain.

If someone tries to modify the prescription the patient will immediately be notified regarding the modifications made in the prescription. This system also includes a hardware USB RFID Card Reader which reads information from RFID cards and communicate with a computer or other devices via a USB interface. In particular, we have designed a trusted access control mechanism to securely share health records among various patients and healthcare providers.

Fig 4: Splash Screen

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, No. 1, August : 2023

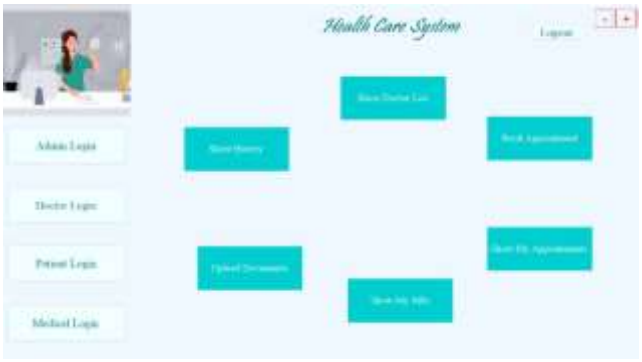

Fig 5: Patient Dashboard

Fig 6: Doctor Login Page

Fig 7: Treatment Details Page

V. CONCLUSION

With the current challenges of eHealth and the benefits of blockchain technology, there could be a revolution in the definition of many areas. The future is towards a distributed Internet, and blockchain technology is the silver bullet for such a future, despite its multiple difficulties. Patients will be connected to doctors, medical stores in a trustless-no third- party environment. Continuous access to all data and sharing of patient medical data, privately and securely, with complete patient control over their data, who can see and use their data.

This approach will revolutionize future applications, becoming extremely secure, private, and user-centric. The patient's end allows the patient to make appointments and also access the prescriptions. The system predicts the diseases based on the symptoms entered by the patient. The doctor's end provides the doctors with the patient's medical history to make the diagnosis more efficient.

The data of all the diseases can be collected to train the system and make it more efficient. Location based real time solutions through continuous tracking.

VI. REFERENCES

1. Gauri Lodha, Manu Pillai, Ankit Solanki, Sarvesh Sahasrabudhe, Ashwini Jarali, "Healthcare System Using Blockchain", International Conference on Intelligent Computing and Control Systems (ICICCS 2021).
2. Dinh C. Nguyen , Pubudu N. Pathirana ,Ming Ding, Aruna Seneviratne, "Blockchain for Secure EHRs Sharing of MobileCloud Based E-Health Systems", Institute of Electrical and Electronics Engineers (IEEE 2019).
3. Santosh Sanjeev, Gowtham Sai Ponniekanti, G. Pradeep Reddy, "Advanced Healthcare System Using Artificial Intelligence", International Conference on Cloud Computing, Data Science Engineering (Confluence 2021).
4. Xu Cheng, Fulong Chen, Dong Xie, Hui Sun, Cheng Huang "Design of a Secure Medical Data Sharing Scheme Based on Blockchain", Journal of Medical Systems, Springer.
5. Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher, "Towards Using Blockchain Technology for eHealth Data Access Management", International Conference on Advances in Biomedical Engineering (ICABME 2017).