Smart Contract-Driven Access Control Mechanism for Diabetic Health Records in Decentralized EHR Systems

Mr. Chayan Bhattacharjee[1], Ms. Sayali Parab[2]

[1]Department of Information Technology, Chikitsak Samuha's Patkar Varde College, Mumbai, India
[2]Department of Information Technology, SES's L. S. Raheja College of Arts & Commerce, Mumbai, India

Abstract - Blockchain has evolved in numerous domains such as Government, Banks, Industries, online voting, Logistics and Healthcare, etc. The advent of Blockchain technology has become a bench of remarkable and growing development in recent decades. One of the most trending and evolving domains is healthcare which consists of EHRs (Electronic Health Records). Diabetes is a chronic disease and growing rapidly and problems arise when it is not treated at an early stage and diagnosed properly at an appropriate time. Hence leads to major health issues and leads to death and the ratio of death globally varies from person to person. Diabetes diseases can be controlled if it is predicted earlier. This Research paper proposes in Securing Healthcare Data for detection of Diabetes provides an earlier detection of this disease by using various Machine learning classification and algorithms and maintains the EHRs of the patient in a secure and timely manner. The diabetic patient has different parameters such as pregnancies, skin thickness, insulin level, blood, age, glucose, Diabetes prediction function, pressure to calculate the chance of likely getting diabetes or not. The Patient dataset is fed to the ML model to find the higher accuracy giving the prediction result. Our EHRs sharing the framework technology combines symptoms-based disease predictions with the help of Blockchain and Interplanetary File System (IPFS) in which the data of the patients' health information are collected suffering from these diseases. We have designed an Extensible Application and predict the diabetes diseases as per the symptoms learned by Machine Learning Algorithm. The ML Model collects the Input data and then executes for further processing to analyze. The prediction results are recorded along biomedical parameters in Blockchain to ensure the integrity and backtracking and anti-repudiation. The information summary of a patient's concerns with his/her guardians is then recorded in Blockchain. Our proposed system will help the society in order to store, process, and share the patient's health information securely and keep transparency in a specific manner. The overview of biomedical treatments can change the technological terms and treatment to achieve better future building for new Innovation.

***Keywords*:** Blockchain Technology, Smart Contracts, Electronic Health Records (EHRs), Diabetes Prediction

I. INTRODUCTION

The advancement of big technology Blockchain has a huge demand as it ensures a highly secure Application using in various sectors and large investors companies. Also making it the preferred highly transparency and fairness platform for keeping the information secure, maintains integrity, confidentiality and privacy. The broadcast technology provides all the necessities in just one single click. Advancement features and control systems play a crucial role in every aspect of human life such as agriculture, smart cities, industrial automation, Banks, and healthcare. Healthcare is one of the most advanced and vital in human life. A significant amount of work is focused on smart healthcare to address traditional healthcare limits and meet mesmerizing premium healthcare expectations.

This development offers considerable opportunities for biomedical innovation and cost reductions is Blockchain Technology. With the help of this we can design an insight Application which facilitates the organization and in society perspective as well. Diabetes is a chronic disease when the pancreas does not produce enough insulin hormone (Insulin is a hormone regulates blood glucose) increases the level of blood sugar abnormally high, causes impact on the body and causes complications if untreated and undiagnosed at early phase. Intelligent systems have gained popularity from a recent study for the detection and prevention of diabetes in recent years. Intelligent system acts like a human being and it is the same as a carbon copy of human beings to make tasks which are complex and made easier and more efficient by applying various methods.

The Healthcare Application performs a significant role in retrieving the health records data which is easy to use, low cost and stronger timeliness for medical services. In a smart healthcare system patients data parameter can be checked and diagnosed by applying various Machine Learning models and Deep Learning. The patient's sensitive data sensitivity and privacy we have overcome the problem of data leak and cause of failures. We need a secure system to tackle the data privacy issues and Blockchain has the ability to fully challenge the issues faced by the patients in a smart healthcare system. Blockchain is a decentralized distributed system ledger where the transactions or records are stored, secured immutably with smart contracts.

Hence motivated by the recent revolution of Blockchain in various fields, specifically in healthcare, this study aims to develop a Blockchain - Securing Healthcare Data for detection of Diabetes diseases which consists of the following phases includes:

1. Registration Phase
2. Authentication Phase
3. Communication with Blockchain Phase.

The application suggested in this paper uses Random Forest, CNN, Support Vector Machine (SVM) and deep learning concepts to predict and diagnose the health status of diabetic patient that whether patient has diabetes or not. Finally, the performance efficiency of the prediction model is analyzed with the help of performance metrics such as accuracy, sensitivity, precision, specificity and f1-measure etc. It will assist the physician and patient in accurate diagnosis of diabetic patients and future conditions with safeguarding of patient's sensitive data.

II. BACKGROUND

Blockchain has revolutionized the technology of digital transformation, contracts, transactions and records which forms the defining structure of the economic, political, social and legal systems that governs this world. The first generation of Blockchain technology was introduced with the introduction of bitcoin generation by the pseudonym Satoshi Nakamoto in the year 2008 which introduced the concept of Blockchain and marked the deployment of cryptocurrencies in financial applications involving cash and digital payment systems. The second generation was called Blockchain 2017, which was essentially the realization that the underlying technology that operated bitcoin could be separated from the currency and used for all kinds of other interorganizational cooperation. The third innovation was called the "smart contract," embodied in a second-generation Blockchain system called Ethereum, which built little computer programs directly into Blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin. The Ethereum smart contract platform now has a market cap of around a billion dollars, with hundreds of projects headed toward the market. The fourth innovation, includes the current cutting edge of Blockchain thinking, is called "proof of stake**.**" Current generation Blockchain are secured by "proof of work," in which the group with the largest total computing power makes the decisions. These groups are called "miners" and operate vast data centres to provide this security, in exchange for cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree of security. Proof-of-stake systems are expected to go live later this year.

The fifth major innovation on the horizon is called Blockchain scaling. Right now, in the Blockchain world, every computer in the network processes every transaction. This is slow. A scaled Blockchain accelerates the process, without sacrificing security, by figuring out how many computers are necessary to validate each transaction and dividing up the work efficiently. This innovation landscape represents just 10 years of work by an elite group of computer scientists, cryptographers, and mathematicians. As the full potential of these breakthroughs' hits society, things are sure to get a little weird. Self-driving cars and drones will use blockchains to pay for services like charging stations and landing pads. International currency transfers will go from taking days to an hour, and then to a few minutes, with a higher degree of reliability than the current system has been able to manage. Blockchain has potential to digitally transform the way the world transacts by allowing the contracts to be digitally embedded in databases that are transparent and provide security against tampering. This key attribute of blockchain technology eliminates the need of third parties and intermediaries like banks, lawyers etc. Although the potential of blockchain is immense, there are some issues and challenges that need to be resolved for its widespread adoption. Blockchain application areas includes Banking and Finance, Governance, Healthcare, Logistics and Supply chain management, IoT (Internet of Things), Insurance, Voting etc.

A. Blockchain Technology

A blockchain is a distributed transaction/data ledger composed of blocks, with each block representing data linked to the previous block (layers of increasingly complex data secured by cryptographic hashing layers the data chronologically). For use as a distributed ledger, a blockchain is often managed by a peer-to-peer network cooperatively adhering to a protocol for authenticating new blocks into the blockchain. A batch of transactions is called Blockchain. Blockchain is the Chain of Blocks that contain some specific Information. Thus, a Blockchain is a ledger i.e file that constantly grows and keeps the record of all transactions permanently. This process takes place in a secure, chronological (Chronological means every transaction happens after the previous one) and immutable way. Each time when a block is completed in storing information, a new block is generated. Blockchain is a way of storing, sharing and securing information in a permitted network eliminating the need of third parties like banks or government. It is Decentralized Distributed Ledger System. Blockchain technology has reached phenomenally in the last few decades and it is a fully-distributed, peer-to-peer software network, to store data and easily transfer digital assets. Each block is encrypted and decrypted for protection and hence forms a chain of preceding to another block in chronological order. The data stored is immutable and cannot be altered or modified. Hence the information will be highly secure and transparent.

B. Smart contract

The new generation of smart blockchains, such as Ethereum, NEO and NEM are interesting platforms that offer several useful features for developing blockchain-based health care data management. There is both a public chain and a private chain. The private chains could store private data, maintaining control of the network with the benefit of blockchain technology. Smart blockchains have asset functionality, which means that new tokens (assets) can be created and distributed on the network; these assets could be assigned different purposes (eg, in the context of a health care applications, such assets could be used to appoint roles or permissions to health care institutions or label the functionality of an account). Smart contracts use Blockchain technology to execute agreements which eliminates the middleman and adds levels of accountability for all parties involved in a way not possible with traditional agreements. This saves businesses time and money, while also ensuring compliance from everyone involved. Contracts are expressed in a piece of code that are designed to carry out set of transactions without intermediaries.

Advantages of smart contract as follows:-

1. Cost-Efficiency & Accuracy - Smart contracts are more efficient related to finance so that they can save businesses time and money by processing transactions more efficiently, transparently, and anonymously.
2. Trust and Transparency – It helps more in secret transactions in different sectors and industries. Smart contracts eliminate the middleman and keep the secrets and privacy of the network between third parties and hence maintains the transparency and builds trust in the Blockchain Network.
3. Secure – Transfer of Information is secret and secure so no third party can access and threaten the process of decentralized networks in Blockchain. It keeps the data in digital form and executes to spread, verify a promised contract for each contract participant.
4. Fast retrieval – The speed of data retrieves at a high level of security when transactions are made between the two concerned participants and performs at Blockchain. This reduces the complexity and improves the performance of each transaction in block nodes from previous hash blocks. The cryptographic process used to generate digital fingerprints for secure transaction verification and password storage**.**

5. Communication – A Blockchain-based communication system is a decentralized network structure that uses distributed ledger technology. This creates a network of nodes, each of which has a copy of the ledger. Each transaction is verified by network and added to the ledger creates a permanent and unaltered record of transactions and makes them much more stable than a decentralized system. This can support different persistence stores and includes comprehensive error retry logic when communicating with the Ethereum node.

III. PROBLEM STATEMENT

Large volumes of information are stored in such kinds of format as records, economic papers, clinical test receipt, imaging tests, and vital sign evaluation, all produced by healthcare contributors. Predicting diabetes typically revolves around developing accurate models that can anticipate the likelihood of an individual developing diabetes based on various factors such as age, weight, family history, lifestyle choices, and medical history. Small Healthcare data organisation struggling to keep the hardcopy of the data details includes objective, data collection, feature selection, model development, model evaluation and Deployment of the application model.

The information is always at risk. Being proactive is vital to reduce the chances of healthcare data getting compromised—especially considering how valuable that information is to thieves. Many hospital databases hold records for tens of thousands of patients, if not millions. The quantity of valuable information available makes hackers want to target hospitals, outpatient centers, and similar sites. A cybercriminal could illegally obtain records containing patients' private information, including their illnesses, payment details, and more, and hold all that information at ransom for a high sum. With that danger in mind, some of the biggest data protection challenges in the healthcare industry, and how hospitals and other organizations can minimize their adverse effects. Here some of the data security and challenges:

1. Ransomware attacks occur when hackers lock down data or systems and require the affected parties to pay ransom to restore the information. They're increasingly common—and deadly, with damages expected to cross $30 billion by 2023. Only 29% of people experiencing ransomware attacks reported they could eventually access all their files again.
2. Improper Data handling can also lead to healthcare facilities being busy places, and many workers are under high pressure while juggling many tasks. These combined challenges mean they don't always handle data correctly, which can leave the door unlocked, so to speak, for hackers.
3. Poor internet hygiene and data security practices people who handle healthcare data don't follow best practices for keeping it safe. This issue especially spans numerous industries. One study revealed that 63% of people reuse passwords for work devices and accounts. These reused passwords provide hackers access to more sites. One healthcare system executive had their work laptop—containing over 40,000 medical records—stolen from a locked car. The device's information was unencrypted. Parties from the affected health care system spent more than $200,000 dealing with the event's aftermath and improving policies to reduce the chances of something similar occurring.
4. Third-party health company issues Healthcare organizations have different policies and strategies surrounding data, some of which can lead them into trouble. In another instance, mental health telemedicine company Cerebral admitted a data breach that disclosed protected health information to third parties. The issue reportedly affected more than 3 million patients.

IV. RELATED WORKS

A. Blockchain in Healthcare

Healthcare information-sharing network based on Blockchain uses two liberally-coupled Blockchain to manage various forms of healthcare information and also incorporates off-chain storage and on-chain authentication to meet safety and authenticity criteria. A research also suggest a revolutionary user-centric health data exchange approach through the use of a decentralized and approved Blockchain for guarding confidentiality using the channel creation method and improving individuality protection via the blockchain-based relationship program. Evidence of validity and authentication is indefinitely recoverable from the cloud database and embedded in the blockchain network to protect the confidentiality of health records inside each document.

In a novel framework for the storage of medical data based on Blockchain was introduced. Users should retain valuable data in perpetuity, so where interference is alleged, the originality of the data may be checked. The author makes use of wise data management techniques and a number of cryptographic methods to protect user confidentiality. MedBlock, a blockchain-based information management program, was introduced in [29] for managing information from patients. The centralized MedBlock database in this system allows for secure entry and storage of medical information. The improved consensus process creates consensus on medical history without significant energy consumption and network congestion.

B. Diabetes Prediction

A novel Optimistic Unlabeled learning strategy was introduced, based on clustering and a 1-class classification method. This method initially clusters positive data, studies 1-class classifier models using clusters, selects negative data intersection as the Stable Negative set, and finally uses a binary SVM (Support Vector Machine) classification algorithm. In a scheme called ensemble classification, which is employed by combining multiple classifiers to improve the precision of weak algorithms. The author applies the algorithm to a medical dataset, demonstrating its early utility in forecasting disease.

An updated variant of K-Means based on density was introduced in [34], which provides an innovative and logical approach for choosing the initial centroids. The algorithm's main concept is to pick data points that belong to dense regions and that are appropriately segregated as the initial centroids in feature space. This approach makes comparatively improved estimates of subtypes of cancer from evidence regarding gene expression. A classification algorithm for managing imbalanced datasets was introduced in based on the principle of information granulation (IG). This algorithm assembles data from majority classes into granules to balance the class ratio inside the data. This algorithm first produces a collection of IGs using meta- heuristic methods and applies the data classification algorithm. An edge-cloud-based healthcare infrastructure is proposed in [46] for real-time disease detection, monitoring, and recovery. This approach does not consider the blockchain concept. The proposed method uses blockchain for securing patient health record.

V. RESEARCH METHODOLOGY

1. Registration phase

In this Registration phase the user or existing user tries to login with provided parameters added such as Patient Name, Contact Number, Gmail id, DOB, Address and others related factors. We also add a verification method to prevent the unidentify theft threats. In blockchain using the HTOPS that is event -based OPTs. Intended user Provide the information in the Registration Page and validate the entered details is indeed authentic. Devices face the challenges of a single point of failure a malicious user and can identify to gain access by unauthorized user to stole information and sensitive data which leads to privacy breaches and posses a significant risk to both the confidentiality of user information and the protection of device integrity.

2. Authentication phase

Authentication is widely used to secure data and identify devices. Blockchain is decentralized distributed ledger ensures the data privacy through cryptographic algorithms advanced encryption techniques are employed to guarantee the confidentiality and integrity of data during transmission and storage, at same time a strong communication and authorization mechanism is implemented to verify only authorized devices and users can access ahead and operate the sensitive data. Strong authentication and data encryption are provided for blockchain to guarantee the secrecy and integrity of communications. Moreover, blockchain makes it possible to forge or temper with the device identity information and enhance the credibility of identity authentication. Also it highlights the recurring issues in prior authenticated key agreement schemes, desynchronization attacks and untraceability. Blockchain introduced an Authentication and KeyAgreement (AKA) scheme rooted in dynamic identity asserting their solution resolves all aforementioned scheme, such as temporary information attacks and denial of service attacks.

3. Communication with blockchain interface

Communication in blockchain plays a vital role to establish a communication pattern between intended user and receiver to decrypt the information via building blocks of chain carries data and using the hashing techniques can increase the productivity and data reliability and scalability. Communication in blockchain works in end to end encryption ensuring that only intended recipients can decrypt and read the message. Hence blockchain uses verifiable digital identities reducing the risk of hack and malicious attack on a single point. Data cannot be modified or tampered with as it cannot be altered and immutable so make sure to provide the correct details and information to keep secret and private in cloud storage in blockchain for further uses and benefits to enhance the advantages of blockchain technology.

VI. CONCLUSION

The integration of blockchain technology in diabetes healthcare management presents a transformative opportunity to revolutionize how patient data is accessed, managed, and utilized across various healthcare domains. By leveraging the decentralized, transparent, and secure nature of blockchain, a dynamic and continuously updated data pool can be established, enabling patients, healthcare professionals, and researchers to collaborate in a more efficient and secure environment. This comprehensive data ecosystem not only enhances day-to-day clinical decisions but also fuels ground-breaking research. The ability to identify patterns between patient-specific characteristics and health outcomes through secure and large-scale data analysis could significantly improve the understanding of diabetes progression and treatment effectiveness. Blockchain's compatibility with data lakes offers the potential to consolidate vast amounts of data from both primary and secondary sources, including laboratory results, vital signs, diagnostic imaging, and clinical notes. Furthermore, the integration of patient-generated data—such as home-monitored glucose levels and patient-reported outcome measures (PROMs)—into this ecosystem enhances the personalization and precision of care. For patients, especially those managing chronic conditions like diabetes, blockchain offers two key advantages: ownership and control of personal health data, and the facilitation of seamless, secure data sharing across healthcare institutions. For instance, an elderly diabetic patient could grant access to their family caregiver or physician as needed, ensuring continuous support and oversight without compromising privacy.

In addition, blockchain enables secure sharing of data from home-based monitoring devices, promoting a more connected and proactive approach to diabetes management. As healthcare systems increasingly rely on remote monitoring and digital health tools, blockchain's role becomes even more critical in maintaining data integrity and trust. From a security standpoint, blockchain’s decentralized architecture and cryptographic safeguards ensure that patient data remains immutable, tamper-proof, and accessible only by authorized users. This eliminates common vulnerabilities such as data breaches, unauthorized access, and centralized points of failure. Implementing blockchain on a small scale within existing diabetes care systems offers a practical way to evaluate its real-world effectiveness, scalability, and challenges. Ultimately, adopting blockchain in diabetic healthcare systems has the potential to reshape data governance, empower patients, enhance research capabilities, and strengthen data privacy by paving the way for a smarter, more secure, and patient-centric healthcare future.

REFERENCES

[1] P.J Mercy MCA, M.Phil., N.Antony Aswathi, “Block Chain-Based Secure Healthcare Application For Diabetic-Cardio Disease Prediction In Fog Computing”, in IJCRT ISSN: 2320-2882, volume10, Issue 5 May 2022.

[2] Laxmi, N., Mohana, J. Blockchain-Based hybrid method for diabetic management on daily basis through insulin dosage prediction. Soft Comput (07 July 2023), https://doi.org/10.1007/s00500-023-08932-0, DOI https://doi.org/10.1007/s00500-023-08932-0.

[3] Alharby, M. (2023). Blockchain-based System for Secure Storage and Sharing of Diabetics Healthcare Records. In 1st International Conference in Advanced Innovation on Smart City, ICAISC 2023 - Proceedings. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICAISC56366.2023.10085169

[4] The framework of Privacy-Preserving Diabetes Prediction using Blockchain – “Niharika patel, Manoranajan Panda”, Department of Computer Science and Engineering Odisha University of Technology and Research Bhubaneswar, Odisha, India, in IJCRT volume 10, July 2022, ISSN: 2320-2882.

[5] S Pallavi Singh; P Lavanya; Mb Nirmala; R Madhusudan; Bs Nikhil - “Securing Healthcare Data with Blockchain for Diabetic and Cardio Disease Prediction”, DOI: 10.1109/DISCOVER55800.2022.9974663, Published in: 2022

International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Date of Conference: 14-15 October 2022, Date Added to IEEE Xplore: 12 December 2022.

[6] “Data Retrieval based on the smart contract within the Blockchain”, Zainab Ali kamal and Rana F. Ghani, Computer Science Department, University of Technology, Iraq, Baghdad, Iraq, Periodical of Engineering and Natural Sciences, Vol.9, No-4, October 2021, pp.491-507, ISSN- 2303-4521.

[7] Jingshou-chen, Xiofeng chen, Chin-ling chen chaoyang University of Technology - “A Traceable Blockchain-Based vaccination Record storage and sharing system”, March 2022, Journal of Healthcare Engineering 2022, DOI:10.1155/2022/2211065, License: CC BY 4.0.

[8] Gautami Tripathi, Mohd Abdul Ahad , Gabriella Casalino, **“**A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges” , https://doi.org/10.1016/j.dajour.2023.100344, Volume 9, December 2023, 100344.

[9] W. Wang, B. Yan, B. Chai et al., EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device, High-Confidence Computing (2024), doi: https://doi.org/10.1016/j.hcc.2024.100240.

[10] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry and Y. Nam, "Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing," in IEEE Access, vol. 9, pp. 45706- 45720, 2021, doi: 10.1109/ACCESS.2021.3065440.

[11] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.