International Journal of Engineering Research and Science & Technology

SECURE SHARING ARCHITECTURE OF PERSONAL HEALTHCARE DATA USING PRIVATE PERMISSIONED BLOCKCHAIN FOR TELEMEDICINE

S. SABIYA SULTANA[1], DADI SOWMYA[2], BRUNGI SAHITHI[3],

GUTTA VARUN REDDY[4], KAVALI RAVITEJA[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

ABSTRACT— Blockchain technology has fascinated and significantly sparked research activities and industries due to its transparency in transactions and data sharing. The striking proliferation of blockchain technology is used to confront the challenges associated with trust, transparency, security, centralization, supply chain traceability, and regulatory compliance. The promising technology has the potential to enable several boons across diverse fields like healthcare, supply chain management, manufacturing, cross-border payments, finance, and energy trading. Telemedicine primarily aims to facilitate the transmission of healthcare data through electronic channels, enabling users to access medical services. It supports healthcare services around the globe, aids in early diagnosis and treatment, and assists with remote care by provisioning effective healthcare that is safe, secure, and reliable. However, there are challenges associated with Personal Health Records (PHR) due to lack of ownership of the data, accuracy, reliability, and data transaction security. The architecture presented in this work enables us to benefit from telemedicine and securely share PHR. The proposed model offers a permissioned network-based Hyperledger Fabric blockchain framework for secure PHR sharing amongst healthcare providers. The Byzantine Fault Tolerance consensus mechanism protects patient privacy, and the IPFS protocol is used to store the data off-chain. Additionally, the smart contract is utilized for providing patients with granular access control over PHR data. Hyperledger Caliper is used as a benchmarking tool to test this technology and determine the average latency rate for viewing and updating the

PHR by healthcare providers along with analysis of CPU and memory utilization. As a result, our goals in telemedicine to improve secure sharing and give the patient access control are achieved.

Index Terms – Blockchain, Hyperledger Fabric, telemedicine, Personal Health Records (PHR), Inter Planetary File System (IPFS), smart contracts, healthcare data sharing, permissioned blockchain, Byzantine Fault Tolerance (BFT), access control, healthcare security, decentralized healthcare, Hyperledger Caliper.

I. INTRODUCTION

Telemedicine refers to the delivery of health services and information via the use of telecommunications and electronic information technologies. It enables patient-toclinician communication and suggests monitoring along with remote admissions. Soon, there will be an absolute need for a secure platform for telemedicine for storing, securing, and sharing the personal health records (PHR) of the patient. These services include the administration of access restrictions for patient information, preserving patient data from illegal access, and modification and deletion of stored data [3]. The paper [4] outlines the creation and implementation of a Patients' E-healthcare Records Management System (PRMS) with the objective of safeguarding privacy while utilizing third-party cloud platforms. PHR is vital and highly vulnerable health-related patient information for diagnosis and precise treatment. The amount of patient data stored in numerous health records is constantly and profoundly increasing due to the limited scope and accessibility of existing health records presented as fragmented information owned by individual hospitals [5]. The approach mitigates substantial privacy and security risks linked to the storage of sensitive healthcare data on cloud services. A crucial challenge in the healthcare industry is to ensure that health records are securely accessible and shared across many stakeholders [6], viz. hospitals, physicians, patients, and researchers [7], [8]. But it also raises the issues of privacy, security, and data tampering which may compromise patient care. In need of that, relying on current centralized systems leads to a high risk of data leakage and slow data processing. So, the proposed model uses Blockchain Technology to address the challenges associated with centralized systems. Blockchain technology has fascinated researchers due to its secure, decentralized data management and transparency. [9]

propose a holistic framework that integrates IoT communication security protocols with sophisticated protection measures specifically designed for smart healthcare contexts, incorporating encryption techniques to ensure secure data exchange. The paper focuses on significant privacy concerns and presents an innovative approach to improve the security and reliability of electronic health record (EHR) interactions by trust evaluation mechanisms and cryptographic techniques. Blockchain is concerned with the secure sharing of information between network users and solving the interoperability of data. The idea behind blockchain technology is to provide the current status of every transaction and store a huge amount of data in an organized manner. The updates carried out in the distributed ledger will be documented in the transaction history log of the blockchain network. Blockchain also facilitates smart contracts that ensure trust and confidentiality in the form of a predefined set of code having access rights to medical information without the involvement of any third party. Reference provided test environments for smart health devices for security measures from attacks like Denial of Service and man-in-the middle attacks. Several contributions have been proposed to blockchain-based architectural design providing probable solutions to the existing bottlenecks of Electronic Health Records (EHR). The current trend is not focused on issues related to PHR. In a novel permissioned distributed network is provided to the patients to collect, store, and maintain their PHR securely. In the convergence of Agent-Based Modeling with blockchain smart contracts is proposed to improve participatory decision support systems. The research introduces a patient-centric healthcare framework reference architecture that aims to enhance semantic interoperability among different healthcare systems. The architecture utilizes blockchain, cloud computing, and the Internet of Things (IoT) to guarantee the secure, efficient, and compatible management and sharing of healthcare data.

II. RELATED WORK

A. A multiuser-based data replication and partitioning strategy for medical applications

Multiuser-based data replication and partitioning strategy play a vital role in real-time cloud-based medical computing systems. However, most data replication and partitioning schemes are covered in multiple virtual machines due to high computing costs and time. In this work, a hybrid multiuser-

based data replication and partitioning strategy for medical applications are developed to improve the data replication and partitioning on the large machine learning patterns in a real-time cloud computing environment. This work is implemented in two phases, i.e., data replication phase and multiuser data partitioning phase. Initially, machine decision patterns are replicated among the multiple servers for recovering data phase. In the partitioning phase, cloud data is partitioned. Experimental results proved that data replication and partitioning have better computational efficiency than the conventional approaches on large medical decision patterns. For a wide range of applications, various replicant protocols may be appropriate. A survey of replication approaches has been presented for multiple distributed storage and content management systems extending from distributed database management systems. The measures like accuracy 98.23%, sensitivity 94.53%, and recall 92.29% had been obtained.

B. Low-rank tensor regularized graph fuzzy learning for multi-view data processing

Multi-view data processing is an effective tool to differentiate the levels of consumers on electronics. Recently, the graph based multi-view clustering methods have attracted widespread attention because they can obtain the relationships of multi-view data points efficiently. However, there exist several shortcomings on most existing graph based clustering methods. Firstly, the mostly adopted Euclidean distance can not extract the nonlinear manifold structure. Secondly, graph based methods are mainly hard clustering methods, which means that each data point belongs to only the one cluster exactly. Thirdly, the high-dimension information between multiple views are not taken into account. Thus, a low-rank tensor regularized graph fuzzy learning (LRTGFL) method for multi-view data processing is proposed. In LRTGFL, Jensen-Shannon divergence is adopted to replace the Euclidean distance for obtaining more completely nonlinear structures. In addition, fuzzy learning is adopted to make graph clustering be a soft clustering method. Furthermore, a tensor nuclear norm based on the tensor singular value decomposition (t-SVD) is adopted to take advantage of the high-dimension information. Then, alternating direction method of multipliers (ADMM) is adopted to solve the LRTGFL model. Finally, the effectiveness and superiority of LRTGFL are demonstrated by comparing with various state-of-the-art algorithms on eight real-world datasets.

C. *Projected cross-view learning for unbalanced incomplete multi-view clustering*

Incomplete multi-view clustering (IMVC) aims to partition samples into different groups for datasets with missing samples. The primary goal of IMVC is to effectively address the challenge posed by missing information in clustering analysis. Most existing IMVC methods focus on balanced incomplete multi-view data, assuming a uniform missing rate across all views. However, this assumption does not accurately reflect real-life scenarios. In reality, unbalanced incomplete multi-view data, characterized by varying missing rates among different views, is more prevalent. This presents significant challenges to the clustering process, as varying missing rates can lead to information imbalance. To address these challenges, this paper introduces a novel approach called projected cross-view learning for unbalanced incomplete multi-view clustering (PCL_UIMVC). Specifically, a reconstruction term is integrated, which leverages the information from the existing samples to facilitate the completion of the unbalanced incomplete multi-view data. Next, a projection matrix is incorporated into the model to harmonize feature dimensions across views, mitigating the impact of information imbalance. Then, a graph regularization term is integrated to preserve the geometric structure of the original data. Finally, an iterative algorithm is developed to solve the proposed model. Extensive experiments on eight standard datasets, featuring various rates of missing data, validate the superior clustering performance of the proposed method.

D. *EOG based reading detection in the wild using spectrograms and nested classification approach*

Electrooculography, also known as EOG, is a technique that is used to calculate the corneo-retinal standing potential, which is located between the cornea and the retina of the human eye. Applications of EOG include eye disease diagnosis and eye movement tracking. There has been various research on reading activity detection from EOG signals in controlled laboratory settings. However, determining reading behaviours from data collected from real-world environments remains a challenging problem. Detecting reading in practical scenarios can lead us to track our daily reading activity, thereby improving our learning experience and even workplace productivity. Tracking regular reading behaviour can also lead to further research in cognitive psychology, literacy

development, reading motivation, and reading comprehension. In this study, we investigated an electrooculogram dataset that was collected on the field from 10 users who were engaged in their daily activities on two separate days. We propose a pipeline combining the statistical features with deep learning features from pre-trained ImageNet models. To detect the fine-grained reading activities, we adopted a nested classification approach. Initially, we differentiate between reading and not reading and then we employ an additional classification step to discriminate among three distinct types of reading activities. With our pipeline, we could achieve 66.56% accuracy in detecting the reading activities whereas the original dataset publication showed a baseline performance of only 32%.

III. PROPOSED METHODOLOGY

The proposed system leverages a permissioned blockchain framework using Hyperledger Fabric to securely share Personal Health Records among healthcare providers while giving patients granular access control. Protects against data manipulation and ensures that a consensus is reached even if some nodes fail or act maliciously. Enhances the security and reliability of transactions.

Used for off-chain storage of large PHR data, reducing the on-chain load while maintaining integrity through content addressing. Facilitates efficient data retrieval and sharing.

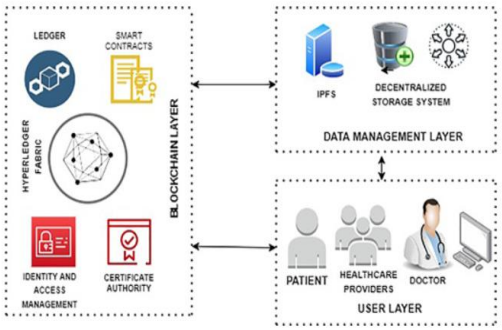


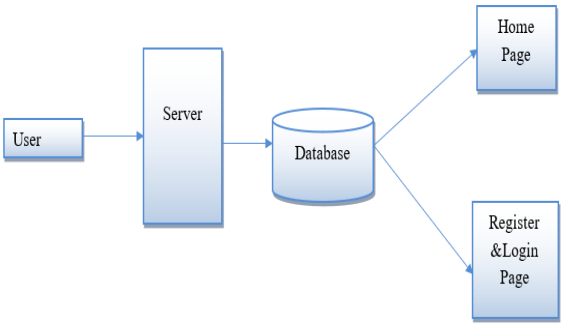
Fig. 1: System Overview

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

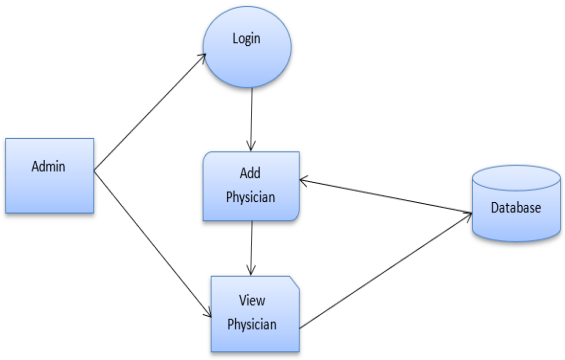
If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

International Journal of Engineering Research and Science & Technology



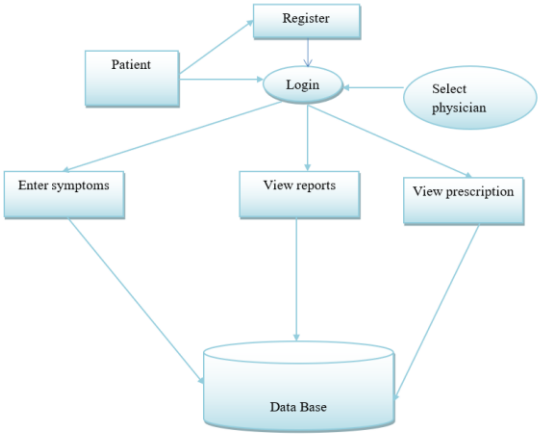
2. Admin

The second module is a Admin. First Admin has to login with a user id and password. After Login admin home page will be displayed, after this admin will add physicians and view physicians.



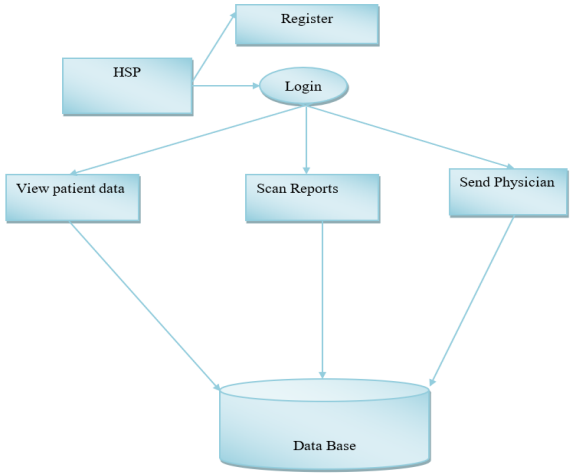
3. Physician

The third module is physician will add by admin and login with a physician id and password. Here physician login to home page and view patients with symptoms and send reports for scanning. After sending reports for scanning physician will view reports and give prescriptions and send to patient.



4. HSP

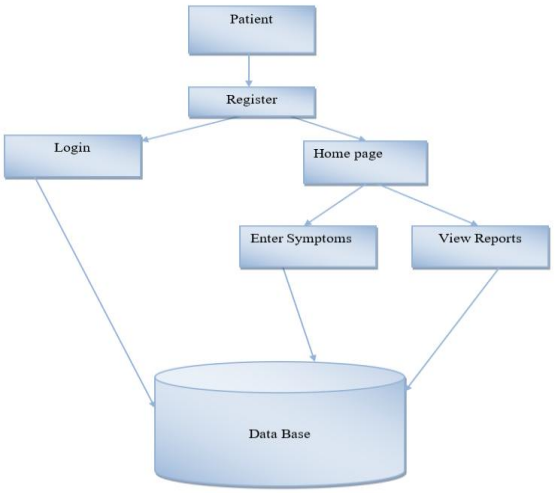
The fourth module is a HSP. HSP will login and scan patient and send reports for physician based on HSP symptoms.



5. Patient

Patient is a fifth module. Patient have to register and login with a patient id and password. Patient has to enter symptoms and send to physician. After sending reports for patient physician will send reports for user and use prescription.

International Journal of Engineering Research and Science & Technology



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed Hyperledger Fabric-based telemedicine framework enables secure and efficient sharing of Personal Health Records (PHRs) using IPFS for off-chain storage and smart contracts for granular access control. Performance evaluation with Hyperledger Caliper demonstrated low latency for PHR viewing and updating, along with efficient CPU and memory utilization. The Byzantine Fault Tolerance (BFT) consensus mechanism ensured secure and reliable data sharing while preserving patient privacy. Overall, the framework provides a scalable, secure, and patient-centric solution for telemedicine applications.

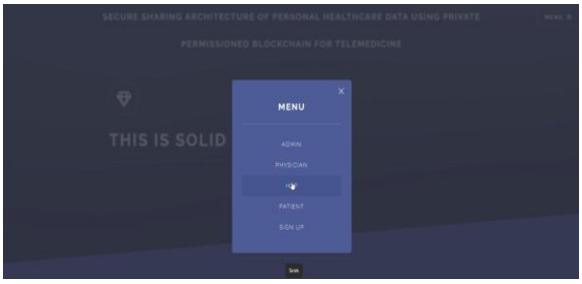


Fig. 2: Menu

Fig. 3: Create Profile

Fig. 4: Registration

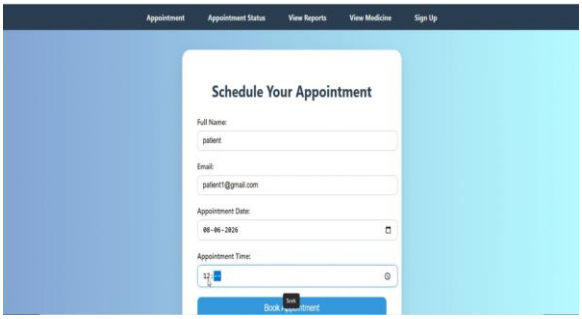


Fig. 5: Book Appointment

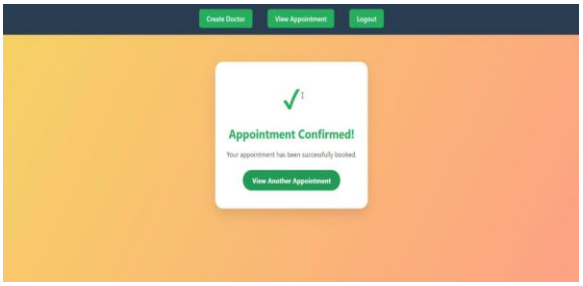


Fig. 6: Appointment Confirmed

Fig. 6: Patient Medical Report

Fig. 6: Upload Report

V. CONCLUSION

PHR contains confidential, and private healthcare information of the Patient. The proposed work presented an architecture for the secure sharing of PHR by involving the Hyperledger Fabric network which is a private permissioned blockchain to store the data. This work also provides the mechanism in which data is accessible to the authorized members of the network according to their access levels defined by the Patient through smart contracts. The healthcare information is stored off-chain using IPFS protocol within the patient database, and its content-address hash is present on-chain in the hyperledger fabric. This work designed the process for teleconsultation for the Patient that is described in the algorithms.

REFERENCES

[1] J. S. Shapiro, D. Crowley, S. Hoxhaj, J. Langabeer, B. Panik, T. B. Taylor, A. Weltge, and J. A. Nielson, ‘‘Health information exchange in emergency medicine,’’ Ann. Emergency Med., vol. 67, no. 2, pp. 216–226, Feb. 2016.

[2] M. Swan, ‘‘Emerging patient-driven health care models: An examination of health social networks, consumer personalized medicine and quantified self-tracking,’’ Int. J. Environ. Res. Public Health, vol. 6, no. 2, pp. 492–525, Feb. 2009.

[3] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.-R. Choo, and N. Zhang, ‘‘Blockchain based searchable encryption for electronic health record sharing,’’ Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019.

[4] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, ‘‘PRMS: Design and development of patients’ e-healthcare records management system for privacy preservation in third party cloud platforms,’’ IEEE Access, vol. 10, pp. 85777–85791, 2022.

[5] J. N. Al-Karaki, A. Gawanmeh, M. Ayache, and A. Mashaleh, ‘‘DASSCARE: A decentralized, accessible, scalable, and secure healthcare framework using blockchain,’’ in Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2019, pp. 330–335.

[6] S. Kumar and M. Singh, ‘‘Big data analytics for healthcare industry: Impact, applications, and tools,’’ Big Data Mining Analytics, vol. 2, no. 1, pp. 48–57, Mar. 2019.

[7] N. Zeinali, A. Asosheh, and S. Setareh, ‘‘The conceptual model to solve the problem of interoperability in health information systems,’’ in Proc. 8th Int. Symp. Telecommun. (IST), Sep. 2016, pp. 684–689.

[8] P. Antón, A. Muñoz, A. Maña, and H. Koshutanski, ‘‘Security-enhanced ambient assisted living supporting school activities during hospitalisation,’’ J. Ambient Intell. Humanized Comput., vol. 3, no. 3, pp. 177–192, Sep. 2012.

[9] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, ‘‘Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare,’’ Sensors, vol. 23, no. 21, p. 8944, Nov. 2023.

AUTHORS Profile

Mrs. S. SABIYA SULTANA has received her B.Tech from JNTUH, Hyderabad in 2014, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017 and Pursuing Ph.D degree in Computer Science from Guru Naanak university, Ibrahimpatnam. She is dedicated to teaching field from the last 2 years. Her research area Machine Learning. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Ms. DADI SOWMYA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. BRUNGI SAHITHI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. GUTTA VARUN REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. KAVALI RAVITEJA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.