Secure Sharing of Electronic Health Records Using Smart Contract and Role Based Access Control

Vijayalakshmi S   
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
svl.cse@psgtech.ac.in

Naveen Kartik R  
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
ramnkartik@gmail.comDeepak V  
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
deepakvellingiri4@gmail.com

Sree Shivesh K  
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
sreeshiveshpsg@gmail.comDharaneesh V  
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
dharaneeshv6@gmail.com

Lokesh Marri Yadav  
*Department of Computer Science and Engineering  
PSG College of Technology*Coimbatore, India  
lokeshmarri2002@gmail.com

***Abstract*—The prevalence of fraud in the insurance industry requires innovative solutions. The main goal of this project is to develop a health insurance fraud detection model that classifies insurance claims with high accuracy, efficiency, and reliability. To accomplish this, a dataset of insurance claims from inpatient or hospitalized patients is used. The dataset is transformed into a machine-understandable format using data pre-processing steps such as standardization and coding techniques, preserving only the features that contribute to learning. While conducting exploratory data analysis (EDA), it was discovered that the dataset was unbalanced. This introduces sampling techniques such as using balanced class weights, random undersampling and oversampling. Further, this approach involves analyzing complex historical feedback data using advanced machine learning algorithms such as logistic regression, decision trees, random forests, and XGBoost. These algorithms are adaptive and continually improve their ability to detect fraudulent patterns by learning from past examples. When comparing four different models combined with different sampling techniques, the eXtreme Gradient Boosting model with SMOTE oversampling is identified as the best in terms of performance metrics like minimum log loss, misclassification rate, false positive rate (FPR), and maximum area under the curve (AUC), F1 score, Balanced Accuracy Score (BACC), Matthew Correlation Coefficient (MCC). This model can also be used to combat widespread insurance fraud through early detection, ultimately benefiting both insurers and policyholders in an ever-evolving environment.**

**Keywords - Insurance frauds, machine learning, logistic regression, decision tree, random forest, xgboost, fraud detection.**

# INTRODUCTION

Electronic health records (EHRs), which contain sensitive medical data, must now be managed and protected at all costs in the digital age. EHRs store a wealth of private medical data, therefore strong access control measures are required to maintain strict privacy and uncompromised security. Over time, a promising method for strengthening EHR access control has arisen through the use of blockchain technology and smart contracts, as mentioned in M Sookhak et al.[2], paving the way for improved data governance and confidentiality. The project aims to present a novel approach to EHR access management, supported by blockchain networks' immutability and smart contracts' revolutionary power. The project seeks to fundamentally alter how electronic health records are maintained and accessed by leveraging blockchain's inherent properties, such as its immutability and decentralized organization.

Blockchain is a decentralized system that operates as an immutable distributed digital ledger. It is a breakthrough technology. It securely and chronologically records an ever-expanding chain of data chunks. Once a block is appended to the chain, it becomes unalterable. Each block comprises a series of transactions. Consensus processes and cryptographic hashing provide this intrinsic security and transparency. Blockchain was first created for digital currencies like Bitcoin, but it has now expanded to be used in a variety of industries, including voting systems, supply chains, banking, and healthcare. Because of its capacity to build confidence, thwart tampering, and facilitate peer-to-peer transactions without the need for middlemen, it has been known as a revolutionary force in contemporary data verification and administration.

RBAC is a time-tested access control mechanism, as justified by Lan Zhou et al.[1] and Sandhu R et al.[5], that provides a structured and efficient way to manage who has access to what within an organization's digital ecosystem. In the realm of EHR management, RBAC assigns roles to users such as doctors, nurses, lab technicians and patients, and determines the possible actions and data that can be accessed based on their roles. This ensures that the right people have the right level of access, and it safeguards against unauthorized access, data breaches, and misuse of sensitive information.

Smart contracts, introduced in Nick Szabo[7], are self-executing digital contracts that, without the need for intermediaries, automatically facilitate, validate, or enforce predetermined activities. Operating on blockchain technology, smart contracts adhere to predefined rules and conditions encoded within their code. As explored in A Saini et al.[3], these contracts ensure transparency, accuracy, and trust across various domains, including financial transactions, supply chain management, healthcare, and real estate. Once conditions are satisfied, smart contracts autonomously execute actions, precisely reflecting the intentions of the involved parties. Their decentralized and tamper-proof nature enhances security while eliminating the reliance on third parties, ultimately streamlining processes and reducing the risk of errors or disputes.

Yan Ding et al.[15] and Thein Than Thwin et al.[16] press the need for access control in the healthcare industry. The access control method is founded on a strategic fusion of smart contracts' dynamic capabilities and Role-Based Access Control (RBAC). The project aims to usher in a new era of precise EHR sharing among authorized institutions by merging RBAC with smart contracts. This approach eliminates the need for time-consuming intermediaries and opens the way for effective and secure data dissemination. Rooted in a robust blockchain architecture, the envisioned system has the potential to exemplify effectiveness, security, and data integrity. EHRs are shielded from unauthorized access while enabling smooth sharing among authorized parties through the lens of role-based access control. Furthermore, the system's security posture is reinforced by the cryptographic validation of smart contracts, ensuring the tamper-proof execution of access control protocols.

In this paper, a comprehensive analysis of the performance and resource utilization aspects of Role-Based Access Control (RBAC) systems is presented. Specifically, a meticulously designed script is employed to measure the time required for access grant and access verification operations, as well as the associated CPU and memory usage during the execution of these critical functions in a hypothetical RBAC system. The script focuses on two distinct RBAC models, Flat and Hierarchy, utilizing a Python library for comparison. The ensuing discussions delve into the intricacies of access grant and verification times, CPU and memory usage changes, offering valuable insights into the efficiency and practical implications of each model. Moreover, graphical representations vividly illustrate the comparative performance of the two RBAC models, emphasizing the superiority of the Hierarchy model in terms of access times and resource utilization. The ensuing chapters aim to provide a nuanced understanding of these findings and their implications for selecting an RBAC model aligned with specific application requirements and performance criteria.

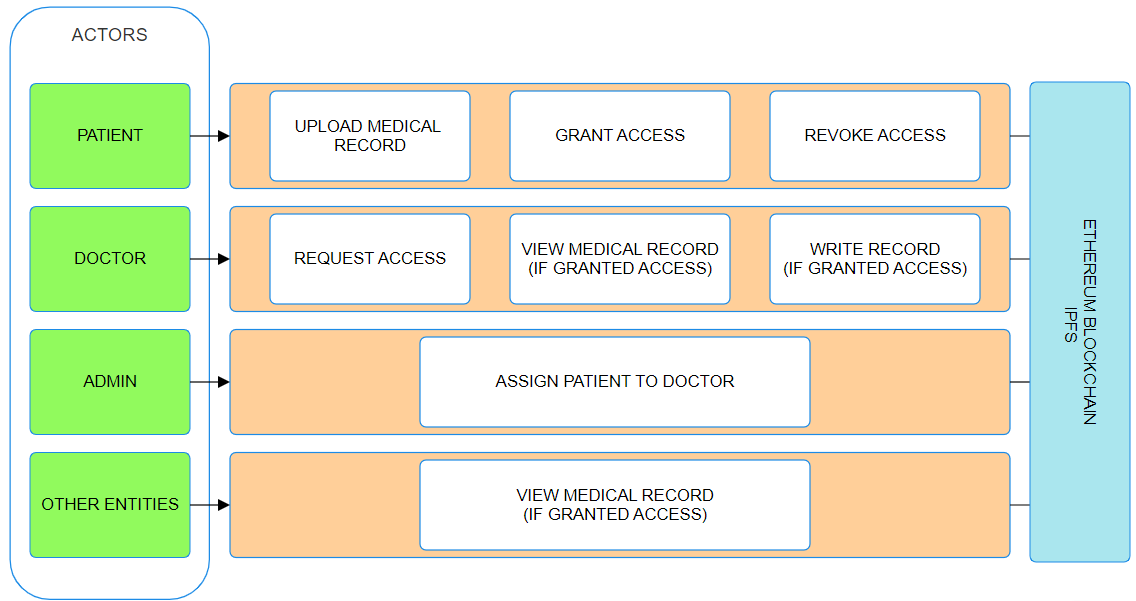
# LITERATURE REVIEW

Lan Zhou et al.[1] explores the fact that the transition of Electronic Health Records (EHRs) to cloud storage presents security challenges in preventing unauthorized access. Researchers have explored cryptographic access control schemes, with a focus on role-based encryption techniques. These approaches enforce role-based access control policies, addressing security weaknesses in practical EHR systems, like the Personally Controlled Electronic Health Record (PCEHR) system of the Australian government. The proposed role-based encryption system offers a secure, flexible solution for safeguarding EHR data in the cloud, enhancing patient privacy and data security in healthcare systems. M Sookhak et al.[2] investigated the impact of emerging technologies, particularly eHealth, on healthcare systems, emphasizing secure electronic health record (EHR) handling. It examines risks to patient privacy from EHR adoption and explores the potential of blockchain and smart contracts for robust access control. The paper presented a detailed survey of blockchain-based access control methods in healthcare, categorizes them, and outlines security concerns. A thematic taxonomy highlights security requirements for accurate access control design. The study also compares traditional and blockchain-based access control methods, addressing key challenges and future directions. A Saini et al.[3] addressed centralization issues in healthcare with scattered electronic medical records (EMRs), proposing a blockchain-based access control framework. Smart contracts are employed to secure EMR sharing among different entities in the smart healthcare system. User verification, access authorization, misbehavior detection, and access revocation are all handled by four different types of smart contracts. Because of the volume of data, hashes are kept in the blockchain and patient digital health records are saved in the cloud in an encrypted form. The effectiveness of the framework in real-time smart healthcare settings is verified by evaluation utilizing a private Ethereum system. H Guo et al.[4] addressed the growing Electronic Health Record (EHR) market by proposing a hybrid architecture for EHR data access control using blockchain and edge nodes. While medical data is stored in off-chain edge nodes and works with blockchain logs to implement access control, a blockchain-based controller oversees identification and access control policies. The evaluation, with a primary emphasis on thwarting unauthorized data extraction, scrutinizes the efficiency of smart contracts and policy execution measured with respect to transaction processing and response time. This analysis is conducted using the Hyperledger Composer Fabric blockchain. Sandhu R et al.[5] explores the field of Role-Based Access Control (RBAC). RBAC has been proven effective, but its lack of a standardized model has led to uncertainty and confusion about its practical application. The paper identifies that RBAC is a dynamic and evolving technology, with various aspects where a consensus has been reached. It categorizes RBAC into four tiers of increasing functional capabilities, including flat RBAC, hierarchical RBAC, constrained RBAC, and symmetric RBAC. Furthermore, the paper presents an alternative approach that combines both flat and hierarchical RBAC while incorporating two unordered elements namely, constraints and symmetry. Advancements in genetics and precision medicine, coupled with IT progress, are transforming healthcare. Blockchain technology offers a solution for health IT interoperability challenges, enabling secure sharing of electronic health data. Laure A. Linn et al.[6] proposed a blockchain-powered access control manager for medical health records to tackle challenges related to industry interoperability and support precision medicine initiatives. Such a national health IT infrastructure could enhance precision medicine, medical research, and patient accountability for their health. Nick Szabo[7] discussed the significance of contracts as a means to formalize relationships, primarily in business contexts. It highlighted the role of contracts in free market economies and their importance in preserving principles like property rights. The article explored how the digital revolution is reshaping relationships and introduced the concept of "smart contracts" which leverage algorithms and digital protocols for more functional and efficient agreements compared to traditional paper-based contracts. It emphasized that smart contracts are not related to artificial intelligence but rather specify promises and protocols within digital frameworks. Ekblaw, A. et al.[8] introduced MedRec, a blockchain-based system for decentralized Electronic Health Record (EHR) management. MedRec offered patients secure access to their medical information, maintaining authentication, confidentiality, and data sharing. It integrates with existing data solutions, incentivises stakeholders as blockchain "miners" for access to anonymised data, and promotes data economics. The paper presented a prototype, discussing blockchain's potential in health IT and research, preparing for practical testing. Pouyan Esmaeilzadeh et al.[9] investigates patient perceptions on blockchain-enabled Health Information Exchange (HIE). It addresses the lack of understanding regarding patient attitudes toward this technology. 2013 respondents engaged in 16 web-based experiments exploring different HIE scenarios. The research unveils significant variations in how patients perceive different exchange mechanisms concerning privacy, trust, opt-in intention, and information sharing. Surprisingly, patients exhibit a positive inclination toward blockchain-based systems for privacy protection and information exchange. The study highlights both potentials and limitations of blockchain in HIE, essential for healthcare organizations aiming to secure and privatize health data exchange. It contributes to blockchain research and offers insights for practitioners aiming to leverage blockchain's benefits in national HIE initiatives. Dagher, G. G. et al.[10] addressed recurring data breaches in patient information despite efforts to enhance electronic health record security. In order to provide safe and easily available medical records for patients, providers, and other parties while protecting patient data privacy, it presents the Ancile blockchain-based platform. Ancile achieves enhanced access control and data obfuscation by utilizing sophisticated cryptography and Ethereum-based smart contracts. The paper aims to analyze Ancile's interactions with various stakeholders' needs and its potential to resolve long standing privacy and security challenges in healthcare. Mettler, M[11] highlighted the growing adaptability of blockchain technology across various sectors, including healthcare. While its application has mainly centered on finance, this is shifting towards other areas like healthcare. The report explores multiple entry points for blockchain in healthcare, such as public healthcare management, user-centric medical research, and tackling pharmaceutical counterfeiting. It aims to showcase the potential impacts and benefits of this disruptive technology in the healthcare industry. Liang, X. et al. [12] proposed a user-centric health data sharing solution using a decentralized and permissioned blockchain. Enabled by mobile and wearable technology, the solution collects health data through a mobile application, syncs it to the cloud for sharing with healthcare providers and insurers. The blockchain ensures privacy protection, identity management, and data integrity with a proof of integrity stored on the blockchain. The approach employed tree-based data processing for scalability and batch processing of large health data sets. S. Neelavathy Pari et al.[13] highlights the impact of blockchain technology in healthcare data sharing, emphasizing its potential in addressing EHR (Electronic Health Records) security and trust issues. It focuses on patient-centric control, privacy, and interoperability. Specifically, the use of Hyperledger Fabric for a permissioned blockchain system is proposed, granting patients control over their medical information and implementing role-based access. The abstract claims a substantial improvement in average latency by 42.71% for access authorization and a 46% reduction in execution time compared to prior solutions. However, a comprehensive literature review could explore existing research on blockchain in healthcare, covering aspects such as data security, patient control, performance metrics, and the efficacy of permissioned blockchains for EHR management. Numerous studies likely examine blockchain's potential, limitations, and practical implementations within the healthcare sector, showcasing the need for secure and efficient data-sharing systems. Yujin Han et al.[14] addressed the limitations of Electronic Health Records (EHRs) in terms of interoperability and privacy, despite their efficiency and security advantages over paper-based records. It explores blockchain's potential to resolve these issues by introducing classic blockchain-based schemes for EHR enhancement. The commentary reviews existing challenges in data management efficiency, access fairness, and system trust. It emphasizes the continued research requirements in the fields of health informatics and data sciences for the implementation of blockchain-based EHRs. These considerations encompass issues like healthcare resource disparities, the environmental consequences of computational requirements, and the potential for skepticism among healthcare providers and patients as blockchain adoption expands. Yan Ding et al.[15] and Thein Than Thwin et al.[16] address the pressing need for access control in healthcare data sharing by introducing a blockchain-based access control mechanism to enhance data security and privacy. They also emphasize the development of robust, patient-centric EHR management systems that ensure data security, privacy, and accessibility in an increasingly digitized healthcare landscape. They collectively address the potential transformation of healthcare data management by utilizing blockchain and smart contracts, resulting in enhanced security and technological advancement. Chrissa McFarlane et al.[17] and M. Jain et al.[18] discuss new standards for data security by employing a hybrid access control system and public key cryptography with Know Your Customer (KYC) verification for user authentication respectively in their papers. They also emphasize the immutability of data records as a fundamental aspect of blockchain-based EHR security and provide ways to ensure the integrity of the patient’s health information. Furthermore, both papers introduce innovative approaches to healthcare data management that prioritize patient empowerment and control over their own health data, thereby ensuring a patient-centric approach to EHR security. J. G. L. A. Jayasinghe et al.[19] and A. A. Mamun et al.[20] provide a comprehensive review of how blockchain can address the limitations of traditional EHRs while providing insights into future research directions, encompassing concepts, prototypes, and implementations. They jointly target scalability, security and interoperability challenges encountered by centralized EHR systems by introducing blockchain-based solutions. The papers position blockchain as a promising solution for decentralization, security, and privacy in EHR management, thereby providing valuable insights for future research. They collectively lay the foundation for a future where EHR management and access control using smart contracts in blockchain technology can revolutionize healthcare. This transformation promises heightened data security, streamlined access, and improved patient care. As the healthcare industry shifts toward embracing these innovations, the outcome is expected to be a more secure, efficient, and patient-centric approach to EHR management.” Kasthuri Bai M et al.[21] and J.UmaMaheswari et al.[22] give an overview on the blockchain technology, renowned for its decentralized and secure infrastructure, stands poised to revolutionize various sectors due to its transparent, efficient, and scalable nature. With the potential to streamline operations, reduce costs, and enhance transparency, it is set to transform governance, as illustrated by the Indian Government's strategy outlined in the NITI Aayog report. The envisioned blockchain applications range across multiple domains, offering a means for direct citizen-government interaction and tailored service provision, exemplified by the proposed framework for vehicle data management by the Indian Road Transport Authority.

# METHODOLOGY

## System Architecture

All the actors interact with the blockchain in 2 ways. The metadata about the medical records, data about access control and actor details are stored in the core blockchain. The actual medical records are stored in the InterPlanetary File System (IPFS) which is a blockchain platform designed especially for file storage. Actors interact with the core blockchain and IPFS. Patients can upload their medical record to the IPFS. The access rights of the files can be modified by either granting or revoking access to external entities. The access rights are stored in the core blockchain. Doctors can request access to a particular patient’s medical record. When granted access, they can view records or update them according to the access permission granted. Administrators can assign patients to doctors. Other entities include lab technician, nurse etc. Other entities can only view the records shared by a patient. They don’t have write access.



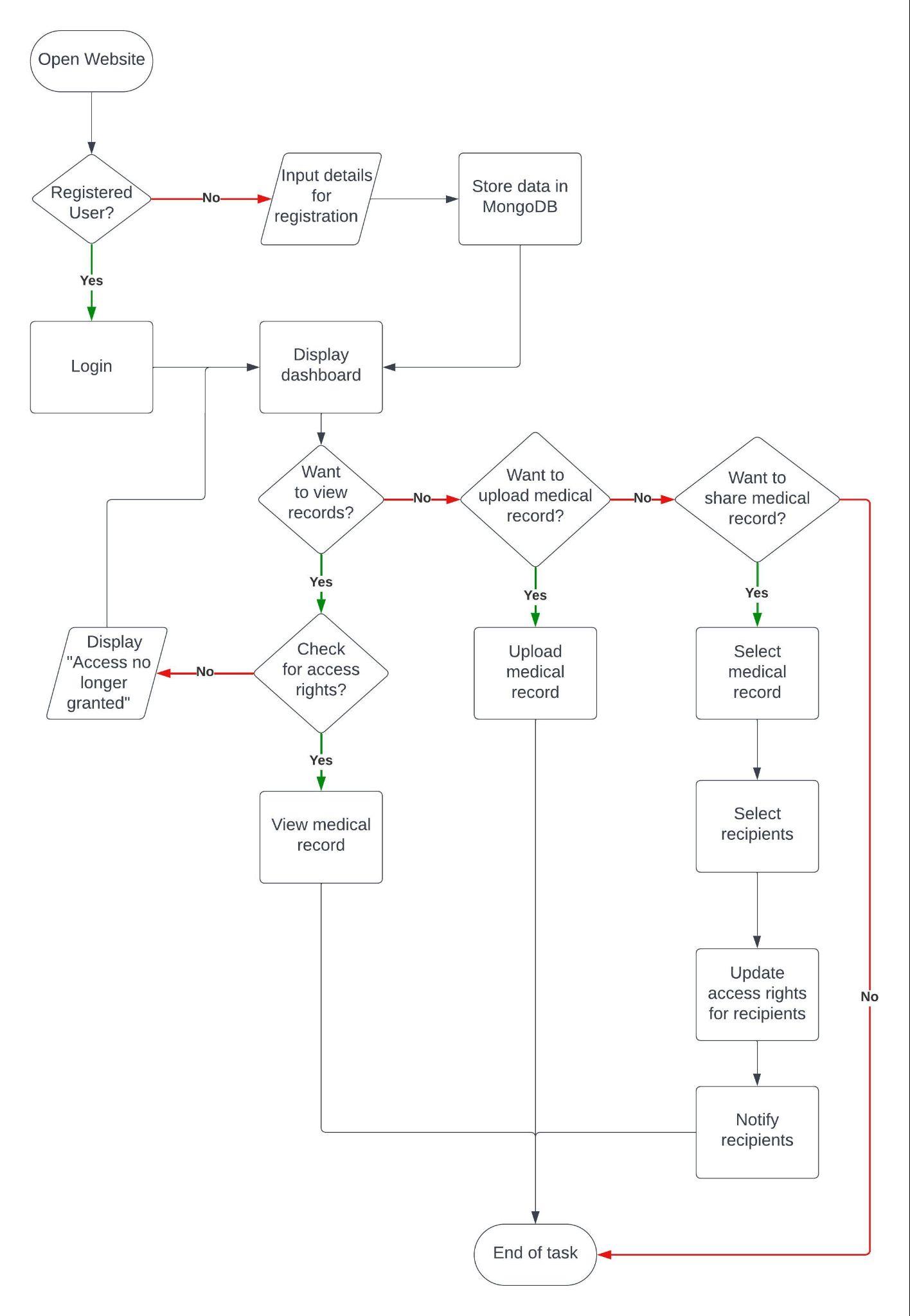
1. System Architecture

## Flowchart

The user interaction and functionality of the system, as illustrated in Fig. 2, encompass a series of actions aimed at ensuring secure and controlled access to medical records within the platform. The login process is the initial step, requiring authentication to guarantee the legitimacy of user access. This login action can be further enhanced to provide feedback in case of invalid usernames or passwords, enhancing user experience and security. Upon successful authentication, users are directed to the dashboard, offering a comprehensive overview of their recent actions within the system. The dashboard serves as a central hub for users to navigate through various functionalities, where three primary actions are made available: View Medical Records, Share Medical Record, and Record Tracking and Revocation.

Users seeking to access medical records undergo a verification process based on Role-Based Access Control (RBAC). This mechanism ensures that users can only view medical records for which they are authorized. The system dynamically checks the user's permissions and displays the respective medical record only if the authorization criteria are met.

The Share Medical Record feature empowers users to share their own medical records or records they are authorized to share. Users can select recipients for sharing, and the system automatically generates access control rules based on the selected recipients. Notifications are then sent to the chosen recipients, informing them of the shared record. Subsequently, when recipients attempt to access the shared record, the system verifies their credentials to ensure compliance with access control rules. The Record Tracking and Revocation functionality provides users with the ability to monitor and track who has access to their medical records. This transparency enhances user awareness and control over their sensitive information. Additionally, users can exercise the crucial capability to revoke access granted to specific individuals whenever deemed necessary. This revocation feature serves as a vital tool in maintaining the privacy and security of medical records, allowing users to adapt access permissions in response to changing circumstances or preferences.



1. Flow diagram

# SYSTEM IMPLEMENTATION

* 1. *Role Based Access Control*

Python's Role-Based Access Control (RBAC) library offers robust functionalities for the seamless implementation of a secure system to manage user roles, permissions, and access requests. This system is exemplified through the creation of a domain represented by the “MedicalRecord” class, specifically designed to oversee medical records within an Electronic Health Record (EHR) system. Roles play a pivotal role in defining user permissions, with specific roles like “can\_create”, “can\_read”, and “can\_update” meticulously crafted to tailor access levels. These roles are intricately associated with permissions such as create, read, and update. The library employs the “add\_permission” method to establish the link between roles and permissions, ensuring a fine-grained control over user actions within the system. For instance, the role “can\_create” is granted the “create” permission, enabling users with this role to initiate the creation of medical records.

The “User” class in this RBAC system represents individuals using the system, particularly doctors. Users are endowed with specific roles and permissions, allowing for a nuanced control over their actions. On the other hand, the “Patient” class symbolizes the end-users, granting them the authority to approve or deny permissions to doctors. The “request\_permission” function facilitates the interaction between doctors and patients, allowing doctors to request specific permissions and patients to grant or deny them after careful consideration. This dynamic exchange is pivotal in establishing a patient-centric approach, where the end-user actively participates in the authorization process. The RBAC system also features a robust method, “has\_permission”, within the User class, which checks whether a user possesses a specific permission. Leveraging the “rbac.go()” method, this function seamlessly manages permissions, providing a mechanism for ensuring security and preventing unauthorized access. In instances where a user lacks the required permission, the system gracefully raises an exception, signaling the absence of the necessary authorization.

This comprehensive RBAC system extends its functionality to address the nuanced interactions between doctors and patients. The ability for doctors to request permissions for actions such as reading or updating medical records underscores the flexibility and adaptability of the system. With a meticulous tracking and management system in place, the RBAC library ensures a secure and efficient user experience while maintaining a patient-centric ethos in the management of medical records. Python’s RBAC library py-rbac offers 4 types of models

* 1. *Metamask*

Primarily associated with the Ethereum blockchain, MetaMask stands out as a widely recognized cryptocurrency wallet and decentralized application (DApp) browser extension. Functioning as a gateway for users to interact with decentralized applications, securely store their cryptocurrency holdings, and manage Ethereum accounts, MetaMask has become an integral tool for participants in the blockchain ecosystem. To utilize MetaMask, users must initiate the process by installing the MetaMask browser plugin, available as an extension for popular browsers such as Brave, Firefox, and Chrome. Once installed, users can conveniently access MetaMask by clicking its icon in the browser toolbar, initiating the account creation process.

The initial step involves establishing a new wallet, where users are prompted to set up a robust password to secure access to their funds. This password is a critical element in safeguarding the wallet's contents and should be kept confidential and secure. Subsequently, users are presented with a unique recovery seed phrase, a pivotal security feature comprising a series of 12 or 24 randomly generated words. This seed phrase serves as a means to recover the wallet in case of a lost password or device and is of paramount importance. Users are strongly advised to diligently record and store the seed phrase in a secure, offline location to prevent potential loss of funds. Sharing the seed phrase or storing it online poses a significant risk to the security of the wallet. Following the setup of the recovery seed phrase, users are required to validate their recorded phrase by selecting the words in the correct order. This step ensures the accurate recording and secure storage of the recovery phrase. Once the recovery phrase is confirmed, users can proceed to establish their first Ethereum account within MetaMask, choosing an account name and adding it to the wallet. Subsequently, MetaMask seamlessly connects to the Ethereum network, providing users with the flexibility to choose the specific Ethereum network they wish to connect to, whether it be the mainnet for real transactions, testnets for testing purposes, or custom networks.

Once connected to the Ethereum network, users gain visibility into crucial information such as their Ethereum account balance, transaction history, and the ability to manage their digital assets, including Ether and ERC-20 tokens, all within the MetaMask wallet. This user-friendly interface and comprehensive functionality make MetaMask an indispensable tool for individuals navigating the decentralized landscape, offering a secure and accessible platform for engaging with blockchain applications and managing cryptocurrency holdings.

* 1. *Ganache*

Ganache stands as an indispensable tool within the Ethereum development landscape, providing Ethereum developers with a versatile and secure environment for testing decentralized applications (DApps) and smart contracts. One of its key strengths lies in its ability to simulate a localized Ethereum blockchain directly on a developer's machine. This simulation allows developers to experiment safely, honing their creations without any impact on the actual Ethereum network. The accessibility of Ganache is another noteworthy feature, available through a command-line tool, a user-friendly desktop application, or a Docker container. This flexibility ensures that developers can choose the interface that aligns best with their workflow. Moreover, Ganache offers a myriad of customizable settings, allowing developers to tailor the environment according to their specific needs. Parameters such as account numbers, gas limits, and network configurations can be easily adjusted, providing a high degree of control and precision in testing scenarios.

An essential aspect of Ganache is its generation of pre-loaded Ethereum accounts, sparing developers the need to use real Ether during testing. This not only streamlines the testing process but also contributes to a more cost-effective and efficient development cycle. Ganache accurately replicates Ethereum transactions, enabling developers to conduct thorough testing without the time-consuming aspect of waiting for confirmations on the live network.For real-world scenario testing, Ganache permits the specification of gas limits, allowing developers to evaluate their smart contracts and DApps under conditions that closely mirror actual usage. Its seamless integration with popular Ethereum development frameworks like Truffle and Remix further enhances its utility, providing developers with a cohesive and streamlined development experience. Debugging is a critical phase in the development lifecycle, and Ganache caters to this need by offering robust debugging tools. Developers can set breakpoints and meticulously inspect changes in contract states, facilitating effective issue identification and resolution. This feature not only accelerates the development process but also contributes to the overall robustness and reliability of the smart contracts.

Ganache also plays a pivotal role in Test Driven Development (TDD) practices, offering a reliable and controlled testing environment for smart contracts and DApps. This approach safeguards against potential security risks by allowing developers to experiment and identify vulnerabilities in a controlled, local setting before deploying to the live Ethereum network. Hence, Ganache empowers Ethereum developers by providing a comprehensive and user-friendly testing environment. Its versatility, customization options, and seamless integration with popular frameworks make it an essential companion in the development toolkit, fostering a more efficient, secure, and reliable Ethereum development process.

* 1. *Deploying Smart Contracts*

In the realm of blockchain technology, smart contracts stand as self-executing programs governed by predetermined parameters and rules. Particularly on the Ethereum blockchain, these smart contracts are commonly scripted using Solidity, a high-level programming language tailored for such decentralized applications. Once the code for a smart contract is written, it undergoes a crucial transformation into bytecode, a low-level representation that can be executed by the Ethereum Virtual Machine (EVM), the computational engine of the Ethereum blockchain. However, before deploying a smart contract onto the live blockchain, it is imperative to subject it to rigorous testing.

Testing of smart contracts is a meticulous process that ensures their functionality and security. This testing can be carried out on a local blockchain environment using tools like Ganache, which simulates blockchain behavior, or on testnets—sandbox environments that mirror the conditions of the mainnet but without real-world consequences. Through comprehensive testing, potential bugs or vulnerabilities within the smart contract can be identified and rectified, safeguarding the integrity of the contract and the data it manages. The Solidity code provided in this application defines a straightforward yet powerful Electronic Health Record (EHR) management smart contract. Its architecture revolves around a “Record” struct, designed to store essential patient data, including the patient's name and pertinent medical information. To establish associations between Ethereum addresses (representing patients) and their respective records, the contract utilizes two mappings: “records” and “authorizedDoctors”. The former links addresses to patient records, while the latter maintains a registry of Ethereum addresses authorized to access and modify these records.

Access control within the smart contract is implemented through two distinct modifiers: “onlyOwner” and “onlyDoctor”. The “onlyOwner” modifier restricts specific functions to be exclusively accessible by the contract's owner—typically, the entity that deployed the contract. On the other hand, the “onlyDoctor” modifier ensures that certain functions can only be executed by Ethereum addresses authorized as doctors, enhancing the security and privacy of patient data. Key functionalities of the contract include the capacity for the contract owner to add and remove authorized doctors, empowering authorized doctors to create and update patient records, retrieve patient records associated with their Ethereum address, and update patient medical data. This comprehensive set of features lays the foundation for an Electronic Health Record management system on the blockchain, where robust access control mechanisms are in place to shield patient data from unauthorized access and modification, thereby advancing the principles of security and transparency in healthcare data management.

1. EVALUATION METRICS

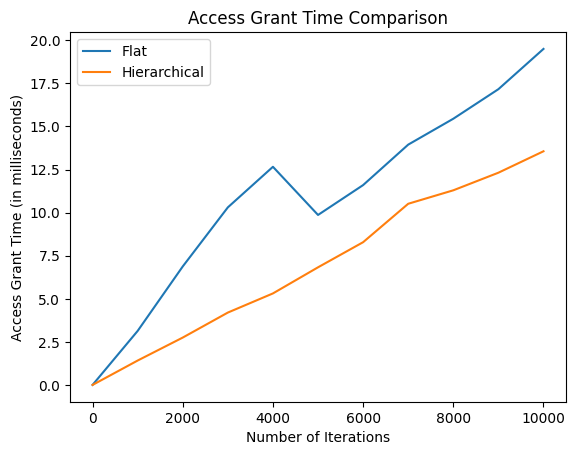
We designed a script to measure the time it takes to perform access grant and access verification operations, as well as the resource utilization (CPU and memory usage) during the execution of these operations in a Role-Based Access Control (RBAC) system. The code uses a hypothetical RBAC system represented by the rbac object, which is assumed to have methods for unlocking, creating subjects (users), and authorizing different actions.

The first part of the script focuses on measuring the time it takes to grant access to a user. The measure\_access\_grant\_time function initializes a timer, unlocks the RBAC system, and then iterates 10,000 times to simulate the creation of users and the authorization of various actions (create, read, and update). The elapsed time is then calculated, and the result is multiplied by 1000 to convert it into milliseconds. The obtained time is printed as "Access Grant Time". Similarly, the second part of the script measures the time it takes to verify access for a user. The measure\_access\_verification\_time function follows a similar structure but involves calling the RBAC system to perform access verifications (using the rbac.go method) and catching any authorization errors. The elapsed time is again converted to milliseconds and printed as "Access Verification Time."

The final part of the script measures resource utilization by capturing the CPU and memory usage before and after performing 1,000,000 access grant operations. The measure\_resource\_utilization function uses the psutil library to obtain CPU usage percentages and virtual memory percentages. The changes in CPU and memory usage are then calculated and printed as "CPU Usage Change" and "Memory Usage Change," respectively. The script provides insights into the performance and resource impact of the RBAC system during access control operations.

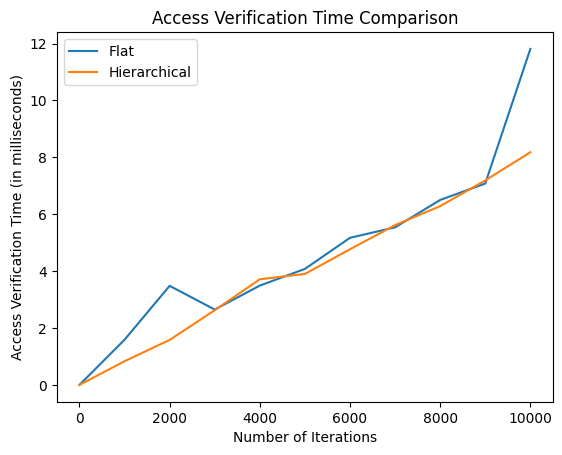
The comparison of two role-based access control (RBAC) models, Flat and Hierarchy, utilizing a Python library, is integral to understanding their performance characteristics. The evaluation metrics, averaged over 10 simulations, provide valuable insights into their efficiency. In evaluating the performance metrics of these two models for role-based access control (RBAC) using a Python library, notable distinctions emerge. On average, the Flat model exhibits an Access Grant Time of 25.56 milliseconds, Access Verification Time of 11.36 milliseconds, a CPU Usage Change of 53.90%, and a Memory Usage Change of 1.74%. In contrast, the Hierarchy model demonstrates improved efficiency, with an Access Grant Time averaging at 16.896 milliseconds, Access Verification Time at 8.43 milliseconds, CPU Usage Change at 46.83%, and Memory Usage Change at 1.73%. These metrics underscore the Hierarchy model's superiority in terms of faster access times and more optimal resource utilization, particularly evident in reduced CPU usage. Such insights provide valuable considerations for selecting an RBAC model tailored to specific application requirements and performance criteria. These metrics illuminate distinctions between the two models. The Hierarchy model consistently exhibits faster access times and more efficient resource utilization, particularly in terms of CPU usage. These findings inform the practical implications and considerations for choosing an RBAC model based on specific application requirements and performance criteria.

Below are the graphical representations of comparisons between Flat and Hierarchical Role Based Access Control models. Flat is represented by the blue line and hierarchical is represented by the orange line. The x-axis represents the number of iterations and the y-axis represents the performance evaluation metric.



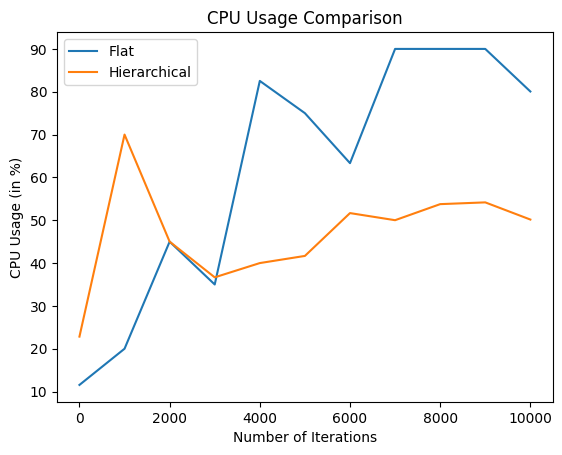
1. Access grant time comparison

From the graph in Fig. 3., we can see how efficient and fast the Hierarchical model is in granting access to the requested roles. Hierarchical model outperforms flat model in both low and high number of iterations by utilizing lesser time to grant access. It is, on an average, faster by 4 milliseconds.



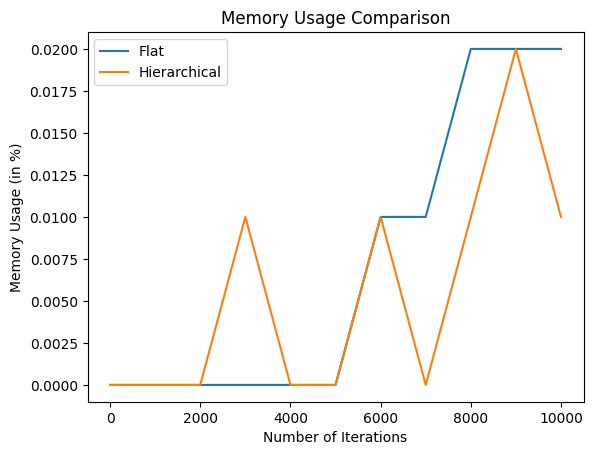
1. Access verification time comparison

From the graph in Fig. 4., we can see that the Hierarchical model is slightly faster than the Flat model with respect to access verification time. For 0 to 3000 iterations and greater than 9000 iterations, hierarchical model is faster than flat model by around 1 millisecond. For 3000 to 9000 iterations, the hierarchical model slightly outweighs the flat model.



1. CPU usage comparison

From the graph in Fig. 5., we can see that the Hierarchical model utilizes less CPU while performing the required access grant and verification tasks. For a lower number of iterations in the range 0 to 2000, the flat model performs better than the hierarchical model. But as the number of iterations increases, the CPU usage in the hierarchical model is 30% less than that of the flat model. This shows that for use cases where the number of users are high, the hierarchical model is preferable.



1. Memory usage comparison

From the graph in Fig. 6., we can see that the hierarchical model has a slight edge over the flat model in terms of memory usage while performing the access verification and grant tasks. Though there are peaks and troughs in the graphs as the number of iterations increases, the average memory usage is lower in the hierarchical model when compared to that of the flat model. In all the above mentioned aspects, the hierarchical model outperforms the flat model which makes it more suitable to integrate with the proposed blockchain based electronic health records management system.

1. CONCLUSION

The implementation of a secure sharing system for electronic health records (EHRs), achieved through the integration of Role-Based Access Control (RBAC), blockchain technology, and storage on the InterPlanetary File System (IPFS), represents a groundbreaking paradigm shift in healthcare industry data management and security. This holistic and innovative solution not only addresses the intricacies of safeguarding sensitive health information but also introduces a comprehensive approach to data integrity, privacy, and availability.

At the core of this advanced system is the utilization of blockchain technology, leveraging its inherent attributes of immutability and transparency. The blockchain serves as an indelible ledger, ensuring the tamper-proof nature of EHRs and providing a reliable audit trail for every interaction with the records. This robust auditability is essential for compliance, accountability, and traceability in the healthcare ecosystem, fostering trust among stakeholders and regulatory bodies. Hierarchical Role-Based Access Control (RBAC) plays a pivotal role in fortifying the security and privacy aspects of this system. RBAC allows for granular control over access permissions, enabling healthcare organizations to tailor access privileges based on the roles and responsibilities of individuals within the system. By delineating who can access specific EHR data and what actions they can perform, RBAC contributes significantly to ensuring that sensitive patient information is accessed and handled only by authorized personnel. This not only mitigates the risk of unauthorized access but also aligns with regulatory frameworks and ethical standards governing the confidentiality of healthcare data. Hierarchical RBAC, as mentioned in the previous section, proves to have better performance than the flat model in terms of time, processing power and memory utilization.

The integration of the InterPlanetary File System (IPFS) as the storage solution adds another layer of sophistication to this innovative approach. By adopting a decentralized and distributed data storage model, the system enhances data availability and resilience. Unlike traditional centralized repositories, IPFS disperses EHR data across a network of nodes, mitigating the risk of single points of failure and ensuring continued accessibility even in challenging network conditions. This decentralized architecture not only bolsters data security but also aligns with the principles of patient-centric care, facilitating seamless access to critical health information when needed. As the healthcare landscape continues to evolve, the adoption of such pioneering solutions becomes imperative to meet the growing demands for data security, privacy, and accessibility. By combining the strengths of RBAC, blockchain, and IPFS, this integrated system establishes a new standard for healthcare data management, providing a robust foundation for advancing patient care, medical research, and the overall efficiency of healthcare delivery. Embracing these innovations is not only a technological leap but a strategic imperative to uphold the confidentiality, integrity, and availability of sensitive medical data in the digital age.

##### REFERENCES

1. Lan Zhou, Vijay Varadharajan and K. Gopinath, "A Secure Role-Based Cloud Storage System For Encrypted Patient-Centric Health Records", The Computer Journal, Vol. 59, no. 1593-1611, 2016.
2. M Sookhak, MR Jabbarpour, NS Safa and FR Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues", Journal of Network and Computer Applications, Elsevier, Vol.178, 2021.
3. A Saini, Q Zhu, N Singh, Y Xiang, L Gao and Y Zhang, "A smart-contract-based access control framework for cloud smart healthcare system", IEEE Internet of Things Journal, IEEE, Vol. 8, no. 5914-5925, 2020.
4. H Guo, W Li, M Nejad and CC Shen, "Access control for electronic health records with hybrid blockchain-edge architecture", 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019.
5. Sandhu R., Ferraiolo D. and Kuhn D., "The NIST Model for Role-Based Access Control: Towards a Unified Standard", Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC '00), Berlin, DE, 2000.
6. Laure A. Linn and Martha B. Koo, “Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research”, ONC/NIST Data Brief, 2016.
7. Nick Szabo, “Smart Contracts: Building Blocks for Digital Markets”, Extropy Journal of Transhuman Thought, No. 16, 1996.
8. Ekblaw, A., Azaria, A., Halamka, J. D. and Lippman, A., “A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data”, Proceedings of IEEE Open & Big Data Conference, Chicago, 2016.
9. Pouyan Esmaeilzadeh and Tala Mirzaei, “The Potential of Blockchain Technology for Health Information Exchange: Experimental Study From Patients’ Perspectives”, Journal of Medical Internet Research, Vol. 21, No. 6, 2019.
10. Dagher, G. G., Mohler, J., Milojkovic, M., Marella, P. B., and Ancillotti, E., “Ancile: Privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records using Blockchain Technology”, Sustainable Cities and Society, Elservier, Vol. 39, no. 283-297, 2018.
11. Mettler, M, “Blockchain technology in healthcare: The revolution starts here”, IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.
12. Liang, X., Zhao, J., Shetty, S., Liu, J. and Li, D., “Integrating blockchain for data sharing and collaboration in mobile healthcare applications”, IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017.
13. S. Neelavathy Pari, S. Rajashree, Adithya Prakash and R. M. Shanthosh, “Role Based Access Control Framework for Healthcare Records Using Hyperledger Fabric”, 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE, 2022.
14. Yujin Han, Yawei Zhang and Sten H. Vermund, “Blockchain Technology for Electronic Health Records”, International Journal of Environmental Research and Public Health, 2022.
15. Yan Ding, Liaoliao Feng, Ying Qin and Chenlin Huang, “Blockchain-based Access Control Mechanism of Federated Data Sharing System”, IEEE, 2022.
16. Thein Than Thwin, Sangsuree Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems", Security and Communication Networks, 2019.
17. Chrissa McFarlane, Michael Beer, Jesse Brown and Nelson Prendergast, “Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.0”, IEEE International Conference on Healthcare Informatics (ICHI), 2017.
18. M. Jain, D. Pandey and N. P. Singh, "EHR: Patient Electronic Health Records using Blockchain Security Framework", International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023.
19. J. G. L. A. Jayasinghe, K. G. S. Shiranthaka, T. Kavith, M. H. D. V. Jayasinghe, K. Y. Abeywardena and K. Yapa, "Blockchain-based Secure Environment for Electronic Health Records", 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2022.
20. A. A. Mamun, S. Azam and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," in IEEE Access, Vol. 10, no. 5768-5789, 2022.
21. Kasthuri Bai M, Vijayalakshmi S, "Blockchain Enabled Services – Survey", Proceedings of the First International Conference on Combinatorial and Optimization, ICCAP 2021, December 7-8 2021, 2021.
22. J.UmaMaheswari, S.Vijayalakshmi G.R.Karpagam, "Blockchain Technology and its Applications - An Overview", International Journal for Research in Applied Science, Engineering Technology (IJRASET) Volume 8, Issue –VIII, August 2020.