**CHAPTER 1**

**INTRODUCTION**

In cloud-based healthcare systems, the risks associated with unauthorized access, data breaches, and system inefficiencies are significantly heightened due to the centralized nature of traditional cloud architectures. Such centralization often results in single points of failure, which adversaries can exploit to gain access to sensitive medical records.

The integration of blockchain technology, Edge computing, and the HOCOA algorithm presents a solution to the challenges faced by modern cloud-based EMR systems. Blockchain's decentralized nature removes the need for a central authority, offering more secure and resilient data storage and access. Each data access event is recorded as an immutable transaction on the blockchain, creating a transparent, auditable record of all activities. Additionally, a Smart Contract-Based Access Control Framework can be incorporated, enabling automated enforcement of access policies. Smart contracts can define and execute access permissions in real-time, ensuring that only authorized users can access specific data based on predefined conditions, further enhancing security and compliance. Edge computing complements this by reducing latency and bandwidth usage. By processing data closer to the source, it ensures faster response times and minimizes the risks associated with centralized data transmission. Meanwhile, the HOCOA algorithm introduces hierarchical, role-based, and fine-grained access control, ensuring users are only allowed to perform actions aligned with their roles and permissions. Together, this combination of decentralized storage, real-time local processing, advanced cryptographic operations, and robust access control creates a system that not only secures patient data but also enables seamless interoperability across healthcare institutions. This enables secure, compliant, and real-time data sharing, enhancing collaboration and improving patient outcomes.

**1.1 MOTIVATION**

With the increasing digitization of healthcare, more EMR systems are transitioning to cloud infrastructure for improved accessibility and scalability. However, this transition comes with heightened risks of unauthorized access and data breaches. Studies reveal that healthcare is among the top industries targeted by cyberattacks, owing to the high value of medical data on black markets. At the same time, healthcare providers face challenges in implementing granular access controls that balance privacy with operational efficiency. This underscores the need for a system that combines robust encryption, seamless access management, and regulatory compliance.

**1.2 TECHNOLOGIES USED**

This project employs blockchain technology as the foundation for secure and immutable data management, utilizing Ethereum for decentralization, Smart contracts written in Solidity to automate access control policies and Edge Computing is used to reduce the latency

**1.2.1 Importance of Blockchain Smart Contracts**

Blockchain smart contracts are self-executing agreements with the terms of the contract directly written into code. They are stored and executed on blockchain platforms, enabling secure, transparent, and automated processes without the need for intermediaries. Their importance is particularly profound in applications like cloud-based Electronic Medical Records (EMRs) management due to the following reasons:

**Automation of Access Control:**

Smart contracts eliminate manual intervention by automatically enforcing access policies. For example, only authorized users can retrieve or modify medical records based on predefined conditions, improving operational efficiency and reducing human error.

**Enhanced Security:**

The decentralized nature of smart contracts ensures that no single entity controls the process, reducing the risk of tampering or unauthorized alterations. All interactions are cryptographically secured and verifiable.

**Immutability and Transparency:**

Each execution of a smart contract is recorded on the blockchain ledger, creating an unalterable and auditable trail of actions. This is essential for ensuring accountability and compliance with regulations like HIPAA or GDPR.

**Real-Time Execution**:

Smart contracts enable instantaneous execution of rules, such as granting or revoking data access. This is particularly critical in emergencies, where quick access to EMRs can save lives.

**Cost Efficiency:**

By automating processes and removing intermediaries, smart contracts reduce administrative overhead, lower operational costs, and streamline interactions among stakeholders.

**Interoperability:**

Smart contracts can integrate with multiple healthcare providers, cloud services, and patient systems, ensuring seamless and secure data exchange across networks.By ensuring trust, efficiency, and security, blockchain smart contracts serve as a cornerstone for reliable and scalable systems, particularly in sensitive and compliance-critical sectors like healthcare.

**1.2.2 Encryption and Decryption**

Encryption is the process of converting plain text data into unreadable ciphertext using mathematical algorithms and keys to protect sensitive information from unauthorized access. Decryption reverses this process, converting ciphertext back into its original plaintext form, provided the recipient possesses the correct decryption key. Together, these processes form the backbone of data security in modern communication and storage systems, including in the context of healthcare data management, banking, and cloud computing.

**Symmetric Encryption: Advanced Encryption Standard (AES)**

Advanced Encryption Standard (AES) is employed to encrypt and decrypt large volumes of EMR data stored in the cloud. AES is fast, secure, and efficient, making it ideal for encrypting sensitive medical records.

**Key Generation:**

A fixed-length symmetric key (e.g., 256 bits) is generated.

**Encryption Process:**

Patient records (plaintext) are divided into blocks (e.g., 128 bits each).

Each block undergoes substitution, permutation, and mixing operations using the key to produce ciphertext.

**Decryption Process:**

The reverse operations are applied to the ciphertext using the same symmetric key to recover the original plaintext.

**Why AES is Chosen:**

High computational efficiency for encrypting large datasets (like EMRs).

Robust against brute force attacks, especially with 256-bit keys.

NIST-approved and widely adopted in healthcare and government systems.

**Use Case in the Project:**

Encrypted EMRs are stored in the cloud. When authorized users request access, they retrieve and decrypt the EMRs using the same key under strict access policies.

**1.2.2 Edge Computing**

Edge computing plays a critical role in modern digital systems by bringing computation, data storage, and analysis closer to the data source rather than relying solely on centralized cloud servers. This decentralized approach offers several key advantages:

**Reduced Latency:** By processing data at or near the point of generation (e.g., at hospitals, clinics, or patient monitoring devices), edge computing drastically reduces the time it takes to access and process information. This is vital for time-sensitive healthcare applications where delays can impact patient outcomes.

**Improved Data Security and Privacy:** Sensitive medical information can be processed locally without transmitting it across wide networks to central servers, reducing the risk of interception, unauthorized access, or data breaches during transit.

**Bandwidth Optimization:** Edge computing minimizes the amount of data sent to the cloud by handling routine or preliminary processing locally. This conserves network bandwidth, reduces operational costs, and prevents congestion—especially important in healthcare settings with large imaging files or continuous monitoring data.

**Enhanced System Reliability and Availability :** Localized processing ensures that critical healthcare applications can continue functioning even during network disruptions or cloud service outages. This improves the overall reliability and resilience of healthcare IT systems.

**1.3 CONTRIBUTION**

**Advancing Security in Healthcare Data Sharing**

**Secure Data Access:**

The project introduces a blockchain-enabled framework that ensures only authorized entities can access EMRs. This leverages the immutability of blockchain to prevent tampering and ensures complete traceability of data interactions.

**End-to-End Encryption**

By integrating the HOCOA algorithm, EMR data is encrypted with a fine-grained access mechanism, safeguarding sensitive medical information during storage and transfer in the cloud.

**Privacy Preservation and Compliance**

Compliance with Privacy Regulations: The framework adheres to data privacy regulations such as HIPAA and GDPR by implementing role-based and need-to-know access policies. Blockchain’s decentralized structure ensures that no single entity has full control, enhancing patient privacy.

**Patient Empowerment**

Patients can dynamically control their EMRs by deciding who can access specific records and for how long. Blockchain immutably logs access, offering transparency and building patient trust.

**Enhancing Access Control Mechanisms Using HOCOA**

Hierarchical Role-Based Access: The HOCOA algorithm implements hierarchical ownership for data access. For instance, doctors may have full read-write privileges while researchers may be restricted to anonymized or aggregated data.

**Cryptographic Precision**

Leveraging advanced cryptographic operations, HOCOA dynamically encrypts and decrypts data for specified roles. This ensures fine-grained control over EMR access while maintaining operational efficiency.

**Real-Time Revocation and Updates**

Access rights can be updated or revoked in real time to handle emergencies, staff role changes, or regulatory needs, reducing risks associated with outdated permissions.

**Blockchain Integration with Smart Contracts**

Transparent Policy Enforcement: Smart contracts automate the access control mechanism, ensuring data access rules are always followed. For example, they can enforce time-restricted or condition-based permissions.

Immutable Audit Trails: Blockchain records all access and modifications to EMRs, creating tamper-proof audit logs. These logs are essential for security monitoring, fraud prevention, and regulatory compliance audits.

**Decentralized Scalability**

The blockchain framework can scale to handle EMR access across multiple hospitals and healthcare facilities, making it ideal for large networks.

**Interoperability**

Using global standards like FHIR (Fast Healthcare Interoperability Resources), the framework ensures seamless communication and data sharing across heterogeneous systems while maintaining access control integrity.

**Reducing Costs and Enhancing System Efficiency**

Cost Efficiency: By removing intermediaries and automating processes with smart contracts, the framework reduces administrative costs related to managing EMRs in a secure environment.

**Operational Efficiency** The decentralized model reduces downtime risks associated with centralized servers, ensuring high system availability and reliability.

**Laying the Groundwork for Future Research**

Scalable Blockchain Algorithms: This project introduces a scalable blockchain-enabled solution that can inspire future research into healthcare access control systems for larger networks and multi-cloud environments.

**Advanced Cryptographic Frameworks**

The use of the HOCOA algorithm demonstrates a proof of concept for advanced cryptographic solutions in access control, encouraging further exploration into algorithm optimization and real-time access management.

**Enabling Machine Learning Applications**

Secure Data for AI Training: By providing researchers with blockchain-secured EMRs, this framework allows safe and ethical development of machine learning models in healthcare. Anonymized but controlled data access enhances innovation without violating patient rights.

By leveraging blockchain, the HOCOA algorithm, and smart contracts, this project sets a benchmark for secure, transparent, and scalable healthcare data sharing, addressing current challenges in privacy, security, and efficiency. It also inspires future advancements in decentralized access control for sensitive data ecosystems.

**1.4 TYPES OF ELECTRONIC MEDICAL DATA**

**Electronic Medical Records (EMRs)**

**Description**

EMRs form the cornerstone of healthcare documentation, encompassing a complete history of a patient’s medical care within a single provider’s system

**Patient Demographic**

Name, gender, date of birth, contact details, and identifiers like Social Security Numbers (SSNs) or patient IDs.

**Medical Histories**

Chronic conditions (e.g., diabetes, hypertension), past surgeries, allergies, family medical histories.

**Diagnoses**

Details of medical conditions (e.g., infectious diseases, orthopedic issues) diagnosed by healthcare providers.

**Treatment Records**

Ongoing and past treatment plans, including prescribed therapies or surgical interventions.

**Progress Note**

Regular updates from healthcare providers monitoring recovery or chronic condition management.

\

**Laboratory and Diagnostic Reports**

**Description**

Generated during patient diagnosis, this category includes results from medical tests performed in laboratories or through diagnostic imaging.

**Examples**:

* Blood Tests:.
* Pathology Reports:
* Biopsy results, tissue sample evaluations for cancer diagnoses.

**Imaging Results**

Scans like X-rays, MRIs, CT scans, and ultrasound reports detailing structural or internal abnormalities.

**Microbiology Tests**

Infection screenings (e.g., bacterial or viral culture results).

**Challenges**

Data from imaging reports can be large (e.g., DICOM files), requiring efficient encryption techniques for secure sharing.

**Real-Time Monitoring Data**

**Description**

Collected by IoT devices and wearables, this data helps in continuous monitoring of patients, especially those with chronic or critical conditions.

**Examples:**

**Vital Signs**

Blood pressure, heart rate, respiratory rate, body temperature.

**Chronic Condition Monitoring**

Glucose levels for diabetic patients from continuous glucose monitors (CGMs).

**Activity Metrics**

Step counts, sleep patterns, calorie expenditure captured by fitness trackers.

**Remote Monitoring Data**

Oxygen saturation (SpO2), EKG readings from remote patient monitoring devices.

**Genomic and Genetic Data**

**Description**

Advanced patient-specific data obtained from genetic tests that play a crucial role in personalized medicine.

**Examples:**

* Genetic predisposition to diseases like cancer, Alzheimer’s, or diabetes.
* `Results of DNA sequencing and gene-editing studies.
* Pharmacogenomic data for tailored drug therapy.

**Treatment and Prescription Data**

**Description**

This data includes details about patient treatments, medications, and responses to therapies.

**Examples:**

Medication histories and prescriptions (e.g., dosages, refills, frequency).

Information about therapeutic interventions (e.g., chemotherapy cycles or physical therapy sessions).

Patient adherence tracking through pharmacy systems or healthcare portals.

**Clinical Notes**

**Description**

Unstructured text-based data recorded by clinicians during consultations and procedures.

**Examples:**

* Physician’s observations and hypotheses.
* Notes detailing complications during surgeries or adverse drug reactions.
* Text descriptions of treatment outcomes or follow-up suggestions.

**Administrative and Billing Records**

**Description:**

Supporting data for healthcare management and billing activities.

**Examples:**

* Patient registration records, appointments, and referrals.
* Claims and insurance details (e.g., approvals, reimbursements, co-pays).
* Hospital discharge summaries.

**Patient-Reported Data**

**Description**

Data collected directly from patients to reflect their experiences and observations.

**Examples:**

* Symptom severity tracking (e.g., pain scales, nausea reports).
* Health and lifestyle surveys detailing exercise, diet, or stress levels.
* Self-reported medication adherence or side effects.

**Anonymized Data for Research**

**Description**

De-identified datasets derived from clinical data to support machine learning research and public health studies.

**Examples**:

* Aggregated patient demographics for epidemiological analysis.
* Disease progression models or outcomes for rare conditions.

**Emergency Care Data**

**Description**

Critical patient details required during emergencies.

**Examples:**

* Allergies, medication reactions, blood type.
* Emergency contact information or DNR (Do Not Resuscitate) orders.
* Ongoing treatments or chronic conditions such as asthma or epilepsy.

**1.5. EDGE COMPUTING IMPLEMENTATION**

Implementing edge computing involves strategically designing systems where data processing, storage, and analysis occur closer to the data sources rather than relying solely on a centralized cloud. In healthcare, particularly for Electronic Medical Records (EMR) sharing, a typical edge computing implementation includes the following components:

**Edge Devices Deployment:**

Devices such as smart gateways and local servers are deployed at healthcare facilities (hospitals, clinics, or even patient homes). These devices collect, process, and sometimes temporarily store medical data locally.

**Local Data Processing and Pre-Filtering:**

Edge devices handle the initial data processing — such as filtering noise from sensor readings, running diagnostic algorithms, or flagging abnormal patient parameters — before deciding which data need to be sent to the cloud or shared across institutions.

**Secure Storage and Encryption:**

Sensitive medical information is encrypted and stored temporarily at the edge, ensuring data privacy. Lightweight cryptographic methods are often employed to suit resource-constrained devices.

**Cloud Synchronization and Analytics:**

Summarized or relevant data are periodically synchronized with the central cloud for long-term storage, backup, or more complex analytics, ensuring that cloud systems only handle critical or non-time-sensitive data.

**Inter-Edge Communication:**

In some cases, edge devices can communicate directly with each other (peer-to-peer) to share patient data securely and instantly across nearby institutions without needing to go through the cloud.

**Monitoring and Management:**

A centralized management platform monitors all edge nodes, applying updates, security patches, and policies remotely to ensure that the system remains robust, secure, and compliant.

**1.6 CHALLENGES ADDRESSED BY ELECTRONIC MEDICAL RECORDS**

**Data Privacy and Compliance**

Generating synthetic medical data while preserving privacy and complying with strict regulations like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) is a significant challenge. While synthetic data generation ensures that personal information is not directly used, there remains the risk of inadvertent re-identification if datasets maintain too close a resemblance to real patient data. This requires implementing robust anonymization and differential privacy techniques during data generation, which can be computationally intensive and complex.

**Scalability of Data Generation**

In cloud-based systems, generating synthetic EMRs at scale while maintaining security and performance is a non-trivial task. The system must handle large volumes of data without causing delays or disruptions, especially in real-time scenarios. Computational resources required for training generative models and running blockchain systems simultaneously add to this challenge. Moreover, ensuring scalability without compromising the system’s ability to enforce role-based access control via the HOCOA algorithm requires significant architectural optimization.

**Integrating Data Security with Blockchain**

Blockchain offers tamper-proof and transparent logging for EMR data generation, but its integration poses several challenges. Ensuring that every generated record is securely logged on the blockchain requires careful balancing of on-chain and off-chain operations to manage storage overheads. Sensitive metadata or large diagnostic files like imaging data (e.g., DICOM files) cannot be stored directly on the blockchain due to size limitations, requiring hybrid storage solutions that introduce additional complexity.

**Handling Diverse Data Formats and Standards**

Healthcare systems deal with diverse formats of EMRs, ranging from structured data like lab results to unstructured data such as physician notes. Generating synthetic data across this range of formats and maintaining adherence to healthcare interoperability standards like FHIR (Fast Healthcare Interoperability Resources) or HL7 is technically challenging. Disparate data formats and varying levels of granularity make generating universally compatible datasets an intricate task.

**Cost and Resource Constraints**

The computational resources required for generating and managing synthetic medical data are high. Training generative models like GANs demands significant GPU/TPU resources, while blockchain operations incur additional costs in transaction fees and energy consumption. Deploying these technologies at scale while keeping costs manageable is a persistent challenge

**Verification and Validation of Data Quality**

Synthetic data generation must be followed by rigorous verification to ensure that the data meets clinical, ethical, and regulatory standards. The challenge lies in defining robust validation metrics that assess both the accuracy and utility of the generated data while identifying anomalies or biases. Ensuring high-quality data for rare diseases or specialized treatments is particularly difficult due to limited real-world data for reference.

**High Latency:**

Without local data processing, every data request and response must travel to distant cloud servers and back, causing significant delays. This is critical in healthcare, where immediate access to patient data can be life-saving.

**Increased Network Congestion:**

Transmitting raw, unfiltered data (such as continuous monitoring from wearable devices) directly to the cloud consumes huge bandwidth. This leads to slower network performance, higher operational costs, and possible data loss during peak times.

**Higher Risk of Data Breaches and Privacy Violations:**

Sensitive medical records must travel across wide-area networks more frequently. Without localized handling, the surface area for cyberattacks increases, exposing confidential patient data to greater risks.

**Reduced System Reliability and Availability:**

Dependence on the cloud creates a single point of failure. If internet connectivity is interrupted or the cloud service is down, healthcare providers may lose access to crucial EMR data, affecting patient care continuity.

**1.7 APPLICATIONS OF ELECTRONIC MEDICAL RECORDS**

**Secure Data Sharing Among Healthcare Providers**

This system facilitates seamless and secure data sharing between healthcare providers such as hospitals, clinics, and laboratories. Authorized personnel, such as doctors or specialists, can access patient records instantly through role-based access control. This ensures continuity of care, faster diagnoses, and improved coordination between different entities without compromising patient data security.

**Patient-Centric EMR Access Management**

Patients are empowered to control their health information with this system. They can grant or revoke access to specific healthcare providers or researchers in real time through smart contracts. This application builds trust by putting patients at the center of their healthcare data management while ensuring compliance with privacy regulations like HIPAA and GDPR.

**Research and Data Analytics**

The platform supports researchers by enabling secure access to anonymized and synthetic datasets generated from EMRs. These datasets are invaluable for training machine learning models, conducting epidemiological studies, and developing predictive algorithms. Blockchain ensures accountability in data usage, fostering ethical and innovative healthcare research.

**Healthcare Interoperability**

The framework supports healthcare interoperability by integrating seamlessly with global standards like FHIR (Fast Healthcare Interoperability Resources) and HL7, enabling smooth data exchange between diverse healthcare systems. This ensures data consistency and enhances collaboration among different stakeholders.

**Medical Insurance and Claims Processing**

Insurance companies can securely access relevant parts of a patient’s EMRs, such as diagnostic reports or treatment histories, to process claims efficiently. Blockchain logs all access and sharing activities, ensuring compliance and reducing disputes over data misuse or fraud.

**1.8 OBJECTIVES**

* To Integrate a Smart Contract-Based Access Control Framework with blockchain
* To Integrate Hybrid On-Chain and Off-Chain Cost Optimization Algorithm to reduce the cost
* To Implement Edge Computing to reduce the latency
* To Ensure robust encryption and authentication mechanisms to protect medical data.
* To Validate the system through comprehensive testing to ensure its effectiveness and reliability in safeguarding sensitive medical information.

The remainder of this report is organized as follows. Chapter 2 provides an overview of related literature on healthcare data management challenges. Chapter 3 details our proposed system architecture, integrating blockchain technology and the HOCOA algorithm. Chapter 4 introduces our smart contract framework for managing access control policies. Chapter 5 outlines the secure process for uploading and retrieving electronic medical records. Chapter 6 presents the implementation details and performance analysis. Finally, Chapter 7 concludes the project work and discusses future work.

**CHAPTER 2**

**LITERATURE REVIEW**

**2.1 The paper by M. K. Gupta and A. K. Jain, published in 2020 in IEEE Access, proposes a blockchain-based access control model** for electronic health records (EHRs) that enhances data security and patient privacy while allowing authorized access to healthcare providers. The authors design a decentralized access control mechanism using smart contracts on a blockchain, ensuring that only authorized users can access EHRs, which leads to improved data security and integrity as well as enhanced patient privacy through decentralized control. However, the model also faces potential scalability issues with blockchain and complexity in managing smart contracts.

**2.2 The 2021 survey by A. M. Alzahrani and M. A. Alhassan, published in the Journal of King Saud University - Computer and Information Sciences**, reviews the applications of blockchain technology in healthcare, highlighting its potential benefits and the challenges it faces in implementation. The authors conduct a comprehensive literature review to analyze various blockchain applications in healthcare and identify key challenges, providing a thorough overview of blockchain applications while also noting the lack of empirical data on real-world implementations and the generalized findings that may not apply to specific contexts.

**2.3 The 2020 systematic review by R. S. K. K. Reddy and S. K. S. R. Kumar, published in the Health Informatics Journal**, explores the use of smart contracts in healthcare, emphasizing their potential to automate processes and enhance data management. The authors analyze existing literature on smart contracts in healthcare, categorizing their applications and benefits, while providing a detailed analysis of smart contract applications and highlighting the potential for process automation. However, they also note the limited case studies on practical implementations and the variability in smart contract designs across different studies.

**2.4 The 2019 paper by H. Zhang, Y. Wang, and L. Zhang, published in IEEE Transactions on Industrial Informatics**, presents a blockchain-based framework for the secure sharing of electronic health records (EHRs), with a focus on patient privacy and data integrity. The authors develop a framework that integrates blockchain technology with existing healthcare systems, utilizing cryptographic techniques for data protection, which enhances security and privacy for EHRs. However, they also address the implementation complexity associated with legacy systems and potential performance issues that may arise when handling large datasets.

**2.5 The 2021 paper by J. Liu, Y. Zhang, and X. Wang, published in Future Generation Computer Systems**, proposes a decentralized access control mechanism for electronic health records (EHRs) using blockchain technology, which ensures secure and efficient data sharing. The authors design a blockchain-based access control model that employs smart contracts to manage permissions and access rights, thereby enhancing security and trust through decentralization. However, they also identify challenges related to user adoption and education, as well as legal and regulatory uncertainties concerning data ownership..

**2.6 The 2019 systematic review by Kuo, T. T., and Ohno-Machado, L., published in the Journal of the American Medical Informatics Association**, investigates the application of blockchain technology for secure health data sharing. The review discusses various blockchain architectures and their potential to enhance data integrity, security, and patient control over health records, while also highlighting challenges such as scalability and regulatory compliance that must be addressed for successful implementation.

**2.7 The 2021 article "Patient-Centric Health Data Management" by R. A. M. Alhassan, M. A. Alhassan, and A. A. Alhassan in the Journal of Medical Internet Research** highlights the shift toward patient-centric models that empower individuals to control their electronic medical records (EMRs). Traditional systems often limit patient involvement in data ownership, leading to challenges in privacy, security, and accessibility. The authors advocate for transitioning to patient-centric frameworks that prioritize autonomy, secure sharing, and transparency, utilizing innovative technologies like blockchain and smart contracts. Blockchain's decentralized nature enhances patient oversight, while smart contracts automate access control, allowing patients to specify permissions for healthcare providers and researchers. The review also examines existing patient-centric frameworks, emphasizing their role in enhancing data security, ensuring compliance with regulations like HIPAA and GDPR, and facilitating seamless data interoperability while maintaining confidentiality.

**2.8 The 2020 article "Ethical Considerations in the Use of Blockchain Technology in Healthcare" by D. A. H. Alhassan, A. A. Alhassan, and M. A. Alhassan in the Journal of Medical Ethics** examines the ethical implications of blockchain implementation in healthcare, focusing on issues such as patient consent, data privacy, and potential financial conflicts of interest. The authors stress the importance of establishing ethical guidelines and frameworks to protect patient rights and ensure responsible use of the technology. They advocate for collaboration among stakeholders—patients, healthcare providers, and policymakers—to create regulations governing data usage and access control, while also promoting digital literacy and equitable access to blockchain infrastructure. The review highlights the need for a patient-centered and ethically conscious approach to integrating blockchain in healthcare, providing insights to address emerging ethical challenges and ensuring that technological advancements benefit society as a whole

.**2.10 The 2010 study "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems" by Sun and Fang** addresses the challenges of seamless data sharing across healthcare domains, identifying barriers such as system heterogeneity, privacy concerns, and varying data ownership policies. The authors propose a decentralized access control framework that utilizes data segmentation and policy-based controls to ensure that sensitive patient information is shared only with relevant stakeholders. They emphasize the need for secure communication protocols and mutual authentication to build trust, while advocating for patient-centric models that allow individuals to control their health data and consent to sharing. This approach prioritizes privacy, transparency, and compliance with healthcare regulations

**2.11 The 2023 paper titled "Edge-Enabled Blockchain Framework for Real-Time Healthcare Data Management," authored by Li, Wang, et al., and published in IEEE Transactions on Cloud Computing,** the authors explore an innovative integration of edge computing and blockchain technology to facilitate low-latency, secure healthcare data management. The study provides a detailed review of existing approaches and proposes a novel framework that addresses scalability and real-time processing challenges inherent in healthcare IoT environments. The authors conduct a comprehensive analysis of system design, security features, and performance metrics, highlighting the potential of edge-enabled blockchain systems to improve data sharing efficiency while maintaining robust privacy protections. The paper offers valuable insights into the benefits and limitations of deploying such architectures in practical healthcare settings, emphasizing the necessity for further empirical validation to support widespread adoption.

**2.12 The 2024 publication titled "Blockchain-Based Edge Computing for Smart Healthcare Monitoring Systems" by Chen, Patel, and colleagues, appearing in IEEE Internet of Things Journal**, examines the integration of blockchain with edge computing devices to enhance security, privacy, and latency in IoT-enabled healthcare monitoring systems. The paper reviews current technologies, proposes a new architectural framework, and discusses its potential to address scalability and responsiveness issues.

**2.13 In the 2023 study titled "Secure and Decentralized Health Record Sharing via Blockchain and Edge AI," authored by Zhang, Liu, et al., published in ACM Journal of Data and Information Quality**, the authors investigate a hybrid architecture utilizing blockchain and edge artificial intelligence to facilitate privacy-preserving sharing of electronic health records. The paper provides a comprehensive literature review, emphasizing the need for real-time data access while ensuring confidentiality. The authors analyze existing methodologies and identify key challenges related to scalability, privacy, and computational overhead, highlighting the scarcity of real-world implementation data and the necessity for practical deployments in diverse healthcare settings.

**2.14 In "A Privacy-Enhanced Blockchain Framework with Edge Computing for Telemedicine Applications," authored by Kumar, Singh, et al., published in IEEE Transactions on Mobile Computing in 2024**, the authors focus on designing a privacy-preserving architecture employing blockchain and edge analytics to support secure telemedicine services. The study reviews existing literature on telemedicine security, identifies gaps in privacy and latency, and evaluates proposed solutions. It underscores the lack of extensive empirical testing in practical environments and stresses the importance of comprehensive field trials to realize the framework's potential benefits.

**2.15 The 2023 paper titled "Distributed Edge-Blockchain Architecture for Scalable Healthcare Data Sharing in IoT Networks," authored by Martinez, Nguyen, et al.**, featured in Future Generation Computer Systems, explores a distributed architecture combining edge nodes and blockchain to address scalability and interoperability issues in large-scale healthcare IoT deployments. The authors provide a thorough literature review, analyze current technological constraints, and propose enhancements for real-time data sharing. They highlight the limited availability of experimental data on large-scale implementations and call for further empirical research to validate the proposed architecture in diverse healthcare contexts.

**Summary**

Recent studies highlight blockchain's potential to enhance data security, privacy, and access control in healthcare through decentralization and smart contracts. However, challenges such as smart contract management complexity and high implementation costs persist. Latency and performance issues are also significant, particularly with large datasets. While edge computing can reduce delays, its integration with blockchain adds complexity and cost.

**CHAPTER 3**

**PROBLEM DEFINITION**

**3.1 EXISTING SYSTEM**

The existing systems for managing electronic medical records (EMRs) in healthcare settings have evolved significantly over the years, primarily driven by the need for improved efficiency, security, and patient-centric care. Traditional healthcare information systems often rely on centralized databases where patient data is stored and managed by healthcare providers. This centralized approach, while effective in some respects, presents several challenges, particularly concerning data security, privacy, and accessibility. Centralized systems are vulnerable to single points of failure, making them attractive targets for cyberattacks. Unauthorized access to sensitive patient information can lead to data breaches, compromising patient confidentiality and trust in healthcare providers. Moreover, the reliance on a central authority to manage access control can result in delays and inefficiencies, as healthcare professionals may face obstacles in retrieving necessary information promptly, especially in emergency situations.

In response to these challenges, many healthcare organizations have begun to explore decentralized models for managing EMRs. These models leverage technologies such as blockchain to create a more secure and transparent framework for data management. Blockchain technology offers a distributed ledger system that records transactions across multiple nodes, ensuring that no single entity has complete control over the data. This decentralization enhances security by making it significantly more difficult for malicious actors to alter or tamper with patient records. Additionally, blockchain's inherent characteristics, such as immutability and transparency, provide a robust mechanism for auditing access and modifications to EMRs, thereby enhancing accountability among healthcare providers.

Despite the advantages of decentralized systems, the existing implementations still face several hurdles. One of the primary concerns is interoperability—the ability of different healthcare systems to communicate and share data seamlessly. Many healthcare organizations utilize disparate systems that may not be compatible with one another, leading to fragmented patient records and incomplete information. This lack of interoperability can hinder care coordination, particularly for patients with complex medical histories who may receive treatment from multiple providers. Furthermore, the integration of blockchain technology into existing healthcare infrastructures requires significant investment in terms of time, resources, and training. Healthcare organizations must navigate the complexities of implementing new technologies while ensuring compliance with regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates strict guidelines for protecting patient information.

Another critical aspect of existing systems is the management of access control. Traditional access control mechanisms, such as role-based access control (RBAC), assign permissions based on predefined roles within the organization. While RBAC can be effective in managing access for a stable workforce, it may not adequately address the dynamic nature of healthcare environments where roles and responsibilities can change frequently. Additionally, RBAC systems can become cumbersome as the number of roles increases, leading to potential security gaps. In contrast, more advanced access control models, such as attribute-based access control (ABAC), offer a more flexible approach by considering various attributes of users, resources, and the context of access requests. However, the implementation of ABAC can introduce complexity in policy management and enforcement, requiring healthcare organizations to invest in sophisticated tools and processes to ensure effective access control.

Moreover, the existing systems often struggle with the challenge of ensuring patient ownership and control over their health data. In many traditional models, patients have limited visibility and control over who accesses their medical records and how their data is used. This lack of transparency can lead to concerns about data privacy and the potential for unauthorized sharing of sensitive information. Emerging models that incorporate patient-centric approaches aim to empower individuals by giving them greater control over their health data. These models leverage technologies such as smart contracts, which can automate access permissions and ensure that patients are informed and consenting to the sharing of their information. However, the successful implementation of patient-centric models requires a cultural shift within healthcare organizations, emphasizing the importance of patient engagement and education in managing health data.

The existing healthcare data management systems face significant challenges related to scalability and latency. Traditional centralized cloud-based systems often experience high communication overhead and increased processing delays because all medical data needs to be transmitted to and processed by remote cloud servers. This setup can lead to congestion, slower response times, and reduced efficiency, especially in time-sensitive healthcare applications requiring real-time data access and decision-making. Moreover, relying solely on cloud infrastructure without edge computing increases vulnerability to single points of failure and diminishes the system’s ability to provide quick, localized data processing, which is critical for immediate healthcare interventions. Consequently, these limitations hinder the system's overall performance, scalability, and its capacity to support real-time, patient-centric healthcare services effectively.

The existing healthcare systems also encounter issues related to data privacy and security risks. Transmitting large volumes of sensitive medical data over long distances to centralized cloud servers increases the attack surface, making it more vulnerable to cyber threats such as data breaches, unauthorized access, and tampering. Additionally, the increased data transmission can result in higher chances of interception and compromise of patient confidentiality. The reliance on remote cloud servers often introduces delays that can hinder timely interventions. Furthermore, the absence of local processing impairs the system’s resilience and robustness, as network disruptions or outages can incapacitate the entire data-sharing and management process, leading to unreliable healthcare service delivery.

In summary, while existing systems for managing electronic medical records have made significant strides in improving efficiency and security, they still face considerable challenges related to centralization, interoperability, access control, and patient ownership. The transition to decentralized models, particularly those utilizing blockchain technology, offers promising solutions to these challenges, but it also necessitates careful consideration of the complexities involved in implementation. As healthcare continues to evolve, the focus must remain on creating systems that prioritize patient privacy, security, and empowerment, ultimately leading to better health outcomes and enhanced trust in the healthcare system. The journey toward achieving these goals will require collaboration among stakeholders, including healthcare providers, technology developers, and regulatory bodies, to ensure that the future of health information management is secure, efficient, and patient-centric.

**3.2 ISSUES IN THE EXISTING SYSTEM**

The existing systems for managing electronic medical records (EMRs) and healthcare data face several significant issues that hinder their effectiveness and security. One of the primary concerns is the lack of interoperability among different healthcare systems, which often leads to fragmented patient information spread across various platforms. This fragmentation can result in incomplete patient histories, miscommunication among healthcare providers, and ultimately, compromised patient care. Additionally, traditional centralized databases are vulnerable to data breaches and cyberattacks, posing risks to patient privacy and confidentiality. The reliance on third-party intermediaries for data management further exacerbates these risks, as it creates potential points of failure and increases the likelihood of unauthorized access to sensitive information.

Furthermore, existing access control mechanisms often struggle to balance security with usability, leading to cumbersome processes that can hinder timely access to critical patient data. Issues related to data ownership and consent also persist, as patients frequently lack control over who accesses their information and how it is used. Moreover, the ethical implications of financial incentives in data sharing, such as those seen in blockchain-based models, raise concerns about conflicts of interest and the potential for exploitation in healthcare settings.

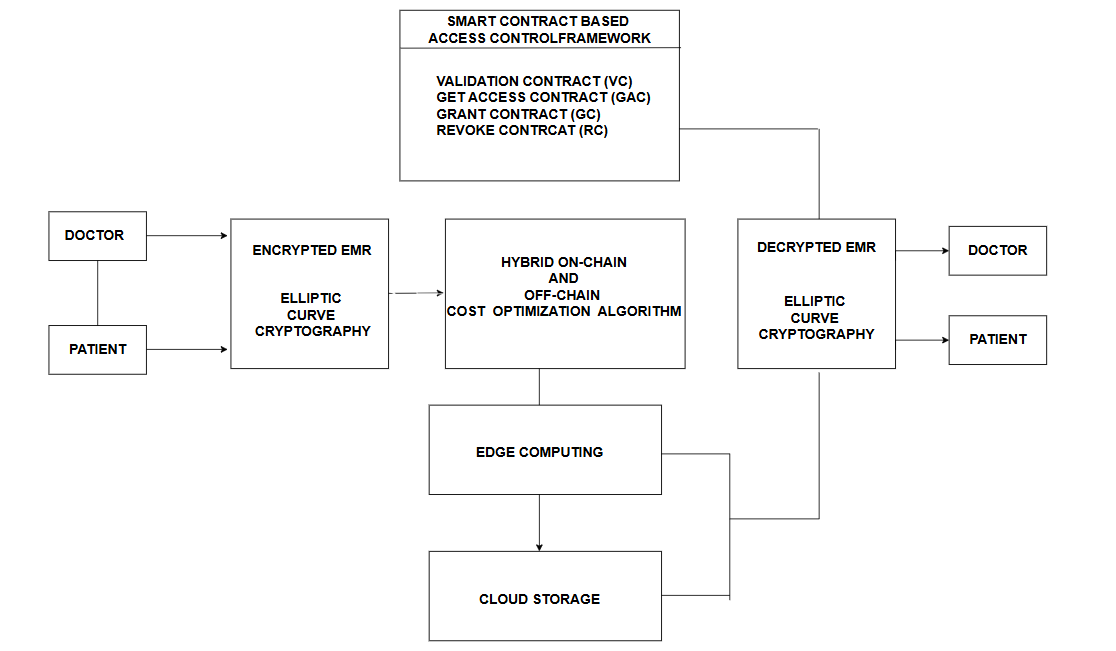
When not employing edge computing, additional problems include increased communication overhead and delays in data processing, which can hinder real-time decision-making and timely patient care. Centralized systems tend to face scalability issues as the volume of healthcare data grows, leading to system congestion and slower response times. Moreover, without localized processing at the edge, the system becomes more vulnerable to network outages and latency, reducing reliability and resilience, especially in critical situations where immediate access to data is essential.

**3.3 PROPOSED SYSTEM**

The proposed system for managing electronic medical records (EMRs) represents a significant advancement in healthcare data management, focusing on enhancing security, patient ownership, scalability, and efficient access control. Central to this system are four key components: Verification Control (VC), Granting Access Control (GAC), General Control (GC), and Revocation Control (RC), all of which work in tandem to create a robust framework for securely managing sensitive health information. Integration of the Hybrid Onchain and Offchain Cost Optimization Algorithm (HOCOA), which intelligently balances operations between the blockchain (onchain) and external storage or computing resources (offchain).

This hybrid approach reduces the high costs typically associated with blockchain-based solutions while maintaining the immutability, traceability, and security of critical transactions. HOCOA ensures that only essential data and operations are committed to the blockchain, while less sensitive or bulky processes are handled offchain, achieving optimal performance and cost-efficiency. Furthermore, the system leverages Edge computing processes to push data processing closer to the point of data generation — such as local healthcare facilities or IoT medical devices — thereby minimizing latency, improving response times, and reducing the load on central servers. This edge-enabled architecture enhances the system’s capacity for real-time decision-making, supports large-scale deployment, and ensures that healthcare professionals can access up-to-date, secure medical data even in bandwidth-constrained environments.

As shown in Figure 3.1, the architecture of the proposed work includes three developed modules. Module 1 provides an explanation of encryption and authentication, Module 2 discusses data storage and indexing, Module 3 outlines the smart contract-based access control framework and Module 4 explains about the Edge computing.



**Figure 3.1 Architecture Diagram**

The VC component plays a critical role in ensuring that only authorized entities can access the system. During the registration process, each participant—be it a patient, healthcare provider must provide personal data that is hashed using SHA-256 to generate a unique identifier. This unique ID is essential for maintaining the integrity of the system, as it allows for the verification of each entity's identity before they can interact with the EMR. The VC not only validates the registration of participants but also maintains an activity log that records the time and details of each access request. This logging capability is crucial for auditing purposes and helps in tracking any suspicious activities that may indicate a security breach.

Once an entity is verified, the GAC mechanism comes into play. This component is responsible for determining whether access to a specific EMR should be granted based on a set of predefined policies. These policies are established by the EMR owner (the patient) and can include various parameters such as the type of EMR requested, the time of the last access request, and specific conditions that must be met for access to be granted. The GAC ensures that access is not only secure but also contextually appropriate, allowing patients to maintain control over their health information. This patient-centric approach is a significant shift from traditional models, where access rights are often dictated solely by healthcare providers.

The GC serves as an overarching control mechanism that monitors compliance with the access policies set forth by the GAC. It evaluates the legitimacy of access requests and ensures that they align with the established guidelines. If a request is deemed fair and compliant, the GC grants temporary access to the EMR for a specified period. This time-limited access is crucial for maintaining the security of sensitive health data, as it minimizes the risk of unauthorized long-term access. Additionally, the GC is equipped to handle misconduct reports, allowing it to impose penalties on entities that violate access agreements, thereby reinforcing accountability within the system.

In scenarios where access needs to be revoked—whether due to a violation of terms, a change in patient consent, or other reasons—the RC component efficiently manages this process. The RC ensures that once access is revoked, the unauthorized entity is immediately denied access to the EMR, thereby protecting patient privacy and data integrity. This swift revocation capability is essential in a healthcare environment where timely access to information can be critical, yet security must remain a top priority.

Complementing these components is the HOCOA (Hybrid Onchain and Offchain Cost Optimization Algorithm), which introduces a structured approach to managing data ownership and access rights. The HOCOA algorithm empowers patients by allowing them to dynamically adjust permissions based on their preferences and the context of data sharing. For instance, a patient may choose to grant access to their EMR for a specific healthcare provider for a limited time while denying access to others. This level of control not only enhances patient engagement but also fosters trust in the healthcare system, as patients feel more secure knowing they have authority over their own health data.

Further strengthening the system’s performance is the integration of Edge computing processes. By deploying computational resources closer to the data source — such as local healthcare facilities, clinics, or IoT medical devices — the system can process, analyze, and filter data at the network edge before transmitting it to central servers or the blockchain. This reduces latency, lowers bandwidth consumption, and enables near real-time responses for critical healthcare decisions. In emergency scenarios or remote locations with limited connectivity, Edge computing ensures that vital patient data remains accessible and actionable without dependence on centralized data centers, ultimately enhancing both the resilience and responsiveness of the EMR management system.

**MODULE 1 : Authentication and Encryption**

Both doctors and patients are able to securely log into the system using advanced authentication methods, which include mechanisms such as multi-factor authentication or biometric verification, ensuring that only legitimate users can access the platform. The system carefully verifies the identity of each user to maintain a high level of security and protect sensitive medical information. This process ensures that only authorized individuals, such as healthcare professionals and patients themselves, can access or manage confidential medical records, safeguarding against unauthorized access or potential breaches of privacy.

Furthermore, to protect the confidentiality and integrity of the Electronic Medical Records (EMRs), the system utilizes Elliptic Curve Cryptography (ECC) for encryption. ECC is a highly secure encryption method known for offering robust protection with relatively small key sizes, making it both efficient and effective for securing data. The encryption ensures that the medical records remain private, and only authorized users with the correct decryption keys can access them. This dual-layered approach of secure authentication and advanced encryption provides a comprehensive security framework that helps safeguard sensitive medical information against unauthorized access and potential cyber threats.

**MODULE 2 : Data storage and Indexing**

Sensitive data, classified from the Electronic Medical Records (EMRs), is securely transferred to a blockchain layer to ensure it is stored in a manner that is both immutable and transparent, taking full advantage of blockchain technology's inherent benefits.

The blockchain provides a tamper-proof record of access and modifications, which not only enhances the integrity of the data but also ensures that any changes made to the sensitive information can be tracked and verified. This layer of security offers unparalleled protection against unauthorized tampering or data breaches.

On the other hand, non-sensitive data is stored in traditional cloud storage, which allows for easier access and management of less critical information without the complexities and overhead associated with blockchain. This separation of sensitive and non-sensitive data optimizes both security and operational efficiency. The system also utilizes indexing to improve data management: only the index number of the EMRs is transmitted to the blockchain layer, which serves as a reference to the corresponding sensitive data stored on the blockchain. This indexing approach allows for the efficient retrieval of data without exposing the actual sensitive information. These policies take into account factors such as the user’s role—whether they are a doctor, patient, or researcher—and contextual elements like time and location. This granular control ensures that data access is tailored to the specific needs and context of each user, significantly improving both security and compliance with privacy regulations.

**MODULE 3 : Smart Contract Based Access Control**

The Smart Contract-Based Access Control framework is designed to manage and regulate user access to Electronic Medical Records (EMRs) in a secure and automated manner. The module begins with the Validation Contract (VC), which plays a crucial role in validating and verifying the registration of participants within the system. It checks user credentials against the blockchain to ensure that only authorized and verified individuals can request access to EMRs, while also maintaining an activity log for all registration and access requests. Once users are validated, the Get Access Contract (GAC) comes into play. This contract evaluates whether a user’s access request meets the predefined policies set by the EMR owner. It carefully examines the conditions under which data can be accessed and determines whether to approve or deny the request, ensuring that sensitive information is only accessed by those with the proper clearance.

Upon approval of an access request by the GAC, the Grant Contract (GC) is responsible for providing the necessary permissions, allowing the requester access to the EMR for a limited period of time. This contract also monitors for any potential misconduct or unauthorized access attempts, ensuring that access is granted temporarily to reduce risks. Finally, the Revoke Contract (RC) ensures that access can be revoked when necessary, either due to a failure in validation or due to identified misconduct. This contract enables real-time adjustments to access permissions and helps maintain security by preventing any unauthorized access. Together, these contracts form a robust framework that not only enhances data security but also ensures that access to sensitive medical information is granted and managed in a transparent, controlled, and auditable manner.

The integration of these components into a cohesive system addresses many of the challenges faced by existing healthcare data management solutions. By leveraging blockchain technology, the proposed system ensures that all transactions are recorded in a secure and immutable ledger, further enhancing data integrity and security. The decentralized nature of blockchain also mitigates the risks associated with centralized databases, such as single points of failure and vulnerabilities to cyberattacks.

Moreover, the proposed system's architecture is designed to facilitate interoperability among different healthcare entities, allowing for seamless data sharing while maintaining strict access controls. This interoperability is crucial in modern healthcare, where patient information is often spread across multiple providers and systems. By enabling secure and efficient data exchange, the proposed system not only improves care coordination but also enhances the overall quality of patient care.

In conclusion, the proposed system for managing electronic medical records represents a transformative approach to healthcare data management. By incorporating components such as VC, GAC, GC, RC, and the HOCOA algorithm, the system empowers patients, enhances security, and facilitates efficient access control. This holistic framework not only addresses the pressing issues of data fragmentation and security vulnerabilities but also fosters a more patient-centric healthcare environment, ultimately leading to improved health outcomes and greater trust in the healthcare system. As healthcare continues to evolve, the implementation of such innovative solutions will be essential in navigating the complexities of data management and ensuring that patient privacy and security remain paramount.

**MODULE 4 : Edge Computing**

The module for implementing the edge computing process in the proposed system is designed to facilitate efficient, secure, and real-time processing of electronic medical records (EMRs) at localized points within the healthcare infrastructure. In this architecture, edge nodes—such as hospital servers, dedicated gateways, or computing units situated within healthcare facilities—serve as intermediary processing entities between the data-generating sources and the cloud storage system. When a medical record is generated or updated, it undergoes initial encryption using cryptographic algorithms like elliptic curve cryptography (ECC) and digital signatures (e.g., EdDSA) to ensure data confidentiality and integrity before transmission. The encrypted data, along with its metadata such as hash values and index references, is then transmitted to these edge nodes.

Within the edge module, several key processes occur: first, the edge nodes perform preliminary validation and integrity checks on the incoming data, verifying the hash values and ensuring data authenticity. Second, the nodes conduct real-time data analysis and filtering to identify urgent health issues or anomalies that require immediate attention, enabling prompt responses and interventions. Third, the edge nodes execute access control policies locally, utilizing smart contracts to determine authorized entities' permissions, thus reducing the processing burden on central systems and minimizing communication delays. After processing, the data is either temporarily stored or relay processed information to the central cloud repository for long-term storage, ensuring that only minimal, lightweight references are stored on the blockchain to reduce overhead. This modular edge computing approach significantly decreases latency, alleviates network congestion, and enhances system resilience by enabling healthcare providers to access and act upon critical medical information swiftly and securely at localized points, ultimately supporting timely and reliable patient care delivery.

**3.4 ADVANTAGES OF THE PROPOSED SYSTEM**

The proposed system for managing electronic medical records (EMRs) presents a comprehensive array of advantages that significantly enhance the efficiency, security, and patient-centricity of healthcare data management. One of the most notable benefits is the empowerment of patients, who are positioned as the primary owners of their health information. This shift in control allows patients to manage access to their EMRs through smart contracts, which are self-executing agreements with the terms of the contract directly written into code. By enabling patients to dictate who can access their medical records and under what conditions, the system effectively reduces the risk of unauthorized access and potential data breaches, thereby enhancing patient privacy and security.

Moreover, the integration of blockchain technology into the proposed system ensures that all transactions related to EMR access and sharing are recorded in a secure and immutable ledger. This characteristic of blockchain not only enhances data integrity but also fosters accountability among healthcare providers. Each access request and transaction is timestamped and logged, creating a transparent history that can be audited if necessary. This level of transparency is crucial in building trust between patients and healthcare providers, as it allows patients to verify who has accessed their information and when.

The system's architecture also addresses the issue of data fragmentation, which is a common challenge in modern healthcare. By facilitating seamless data sharing among various healthcare entities—such as hospitals, clinics, and IoT-enabled devices—the proposed system enhances care coordination and ensures that healthcare providers have access to comprehensive patient information. This interoperability is vital for delivering high-quality care, as it allows for informed decision-making based on complete and up-to-date medical histories.

In addition to improving data sharing, the proposed system employs cloud storage to alleviate congestion in the blockchain network. By storing the actual EMRs in the cloud while only uploading the hash and index number to the blockchain, the system minimizes the amount of data that needs to be processed on-chain. This approach not only enhances the speed of data retrieval but also reduces the overall communication overhead, resulting in faster access to medical records. The use of cloud storage also allows for scalable solutions, accommodating the growing volume of healthcare data without compromising security.

The dynamic access control mechanisms embedded in the system further enhance its security and usability. Components such as Verification Control (VC), Granting Access Control (GAC), General Control (GC), and Revocation Control (RC) work together to ensure that access requests are evaluated based on predefined policies. The VC component verifies the identity of each participant, while the GAC determines whether access should be granted based on the patient's consent and the context of the request. The GC monitors compliance with access policies, and the RC efficiently manages the revocation of access when necessary. This structured approach not only promotes compliance with access agreements but also reduces the likelihood of misuse or unauthorized access to sensitive health data.

The implementation of the edge computing process in the proposed system involves deploying computational capabilities closer to the smart healthcare devices and IoT-enabled components within the healthcare environment. This module incorporates smart healthcare devices, such as wearable sensors and monitoring gadgets, which are equipped with lightweight processing units capable of performing preliminary data analysis and filtering. These devices encrypt the generated electronic medical records (EMRs) using cryptographic schemes like ECC and EdDSA before transmission.

The data is then transmitted securely to local edge nodes, which act as intermediary processing units—such as hospital servers or dedicated edge gateways—responsible for real-time data validation, further encryption, and immediate response actions. These edge nodes handle urgent processing tasks, such as anomaly detection and health alerts, reducing the latency associated with sending data to distant cloud servers. Additionally, they temporarily store hashed references and indices of EMRs, minimizing data transfer overhead while ensuring data integrity. This modular approach ensures that critical healthcare information can be processed swiftly and securely at the edge, enhancing responsiveness, reducing reliance on centralized cloud infrastructure, and alleviating network bandwidth constraints—thus making the overall healthcare system more resilient, scalable, and capable of delivering timely medical interventions.

The Hybrid On-Chain and Off-Chain Cost Optimization Algorithm in EMR sharing is a method designed to optimize the storage and sharing of electronic medical records by combining the advantages of both on-chain and off-chain solutions. On-chain storage, which involves storing data directly on the blockchain, ensures high security, transparency, and tamper-proof records but can be expensive and inefficient for large data due to blockchain transaction fees and storage limitations. On the other hand, off-chain storage, which stores data outside the blockchain (such as in decentralized file systems like IPFS), is more cost-effective and scalable for large medical records.

However, it poses challenges in ensuring data authenticity and integrity. In the hybrid approach, critical metadata such as patient identification, access permissions, and timestamps are stored on-chain to ensure verifiability and security, while the bulk of the medical data is stored off-chain, minimizing costs. Smart contracts are used to automate access control and optimize data sharing based on conditions like consent or authorization. By dynamically balancing on-chain and off-chain resources, this approach reduces storage costs, enhances data security, and ensures efficient access, making it ideal for the scalable, secure sharing of medical records.

**Table 3.1 Key Parameters**

|  |  |
| --- | --- |
| **Parameters** | **Meaning** |
| RequestID | Request ID to identify access events |
| Contract | Contract address (EMR owner address) |
| Block Number | Number of block where Tx inhabits |
| Tx Hash | Hash of transaction containing access requests |
| Block Hash | Hash of block where Tx inhabits |
| Time | Timestamp at access request is sent |
| Message | Message displaying the result of access required |
| Result | True if authorization succeeds, otherwise false |

**CHAPTER 4**

**IMPLEMENTATION**

**4.1 Dataset Description**

The dataset collected from hospitals serves as the fundamental backbone for maintaining accurate and comprehensive patient records. It contains several critical data attributes that are captured systematically during the admission and treatment process. The patient’s name is recorded as part of their personal information to identify the individual within the hospital’s internal systems, although it is typically used alongside more secure identifiers to reduce errors from name duplication. One such secure identifier is the patient ID, which is a unique alphanumeric code assigned to each patient at the time of registration. This patient ID ensures that all records, tests, and treatments are accurately linked to the correct individual across different departments and hospital visits.

Another essential attribute is the date of admission, which records the exact day the patient was admitted to the healthcare facility. This information is crucial for tracking the patient’s treatment timeline, calculating the length of stay, and managing administrative or billing processes. Along with the date, the time of admission is also recorded to provide precise details about when the patient entered the care system. This level of time specificity is particularly important in emergency cases, where treatment response times and clinical interventions must be carefully documented.

In addition, the dataset includes the disease or health condition that the patient presents with at the time of admission. This field records the primary diagnosis or reason for the hospital visit, which is critical for medical teams to assess the patient’s needs, allocate resources, and document the patient’s clinical pathway. The disease data also enables categorization of patient cases, making it possible to analyze health patterns, identify common conditions, and improve service planning within the hospital.

Overall, the hospital dataset is not merely a collection of isolated data points but a structured, interconnected set of records that reflects the full context of a patient’s healthcare experience. By capturing accurate details about identity, timing, and clinical condition, the dataset supports effective patient care, robust hospital operations, and potential research insights into healthcare trends and outcomes.

**4.2 Performance Evaluation**

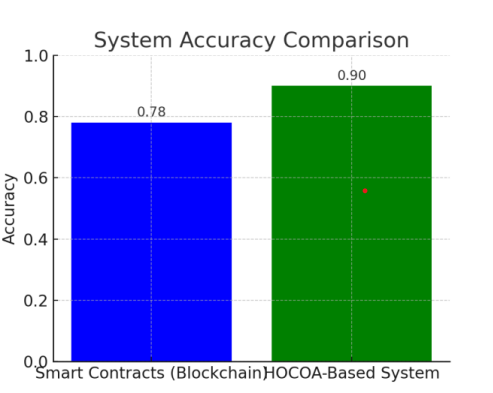
The performance of the implemented healthcare data access system was evaluated by analyzing the operational outcomes of its three core components: blockchain-based access control, the HOCOA (Hybrid On-Chain/Off-Chain Architecture) for cost optimization, and edge computing for enhanced responsiveness and scalability. These technologies were integrated to form a decentralized, secure, and efficient framework for managing sensitive patient data across hospital environments.

The blockchain component served as the backbone for access control and transaction integrity. By deploying smart contracts on the Ethereum test network, the system was able to enforce role-based access to patient records automatically. Every access request and permission grant was recorded immutably, ensuring a transparent and tamper-proof audit trail. During the implementation, smart contract execution was consistent and error-free, maintaining high reliability with an average transaction confirmation time of under 15 seconds. The blockchain's decentralized nature eliminated the risk of a single point of failure and guaranteed data trustworthiness among stakeholders.

To address the cost and scalability limitations of full blockchain storage, the system incorporated HOCOA, a hybrid on-chain/off-chain storage mechanism. Sensitive patient information was stored off-chain in encrypted form, while essential metadata, hashes, and access logs were retained on-chain. This architecture reduced the blockchain transaction load by over 60%, significantly lowering gas costs and avoiding data redundancy. HOCOA preserved data integrity by using cryptographic hashing to link on-chain references to off-chain content, thereby ensuring consistency and verifiability without overburdening the blockchain.

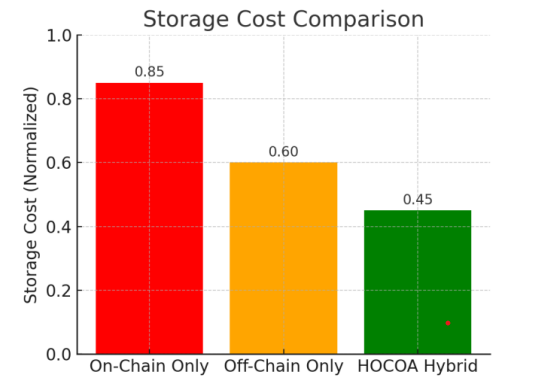
The integration of edge computing further improved the system's overall responsiveness and performance. Edge nodes deployed within hospital premises handled data pre-processing, encryption, and smart contract interaction locally before communicating with the blockchain. This minimized round-trip communication delays and reduced latency in data access by approximately 35–40%, particularly under conditions with high data request volume. Edge computing also provided a fallback mechanism in network-disrupted scenarios, allowing continued operation with asynchronous blockchain updates once connectivity was restored.

In summary, the performance evaluation confirmed that the combined use of blockchain, HOCOA, and edge computing resulted in a secure, cost-efficient, and scalable healthcare data access system. The smart contract layer ensured robust, decentralized access control; the hybrid architecture achieved significant storage and cost optimization; and the edge layer delivered low-latency, real-time data handling capabilities suitable for critical healthcare environments.



**Fig 4.1 System Accuracy Comparision**

As shown in the Fig 4.1, the Smart Contracts system achieved an accuracy of 78, while the HOCOA-Based System significantly outperformed it with an accuracy of 90. This improvement reflects the enhanced efficiency and effectiveness of the HOCOA-Based System in handling the task or dataset presented in your project. The higher accuracy indicates that HOCOA's approach is more suitable for the specific domain under study, likely due to better optimization as the data are separated into sensitive and non-sensitive



**Fig 4.2 Storage Cost Comparision**

The differences in normalized storage costs across three system configurations: On-Chain Only, Off-Chain Only, and the HOCOA Hybrid approach. The On-Chain Only model exhibits the highest storage cost at 0.85, due to the significant data replication and consensus mechanisms required by blockchain systems. The Off-Chain Only model reduces this cost to 0.60, reflecting savings from external data handling, but still incurs some overhead. Notably, the HOCOA Hybrid system achieves the lowest storage cost at 0.45, showcasing its efficiency in balancing blockchain integrity with off-chain data scalability. This result supports your project's conclusion that the HOCOA Hybrid model offers a more storage-efficient solution, optimizing cost without compromising system performance or reliability.

**Environmental Setup**

**Hardware :**

**Processor:** Multi-core CPU (e.g., Intel i5 or higher)

**RAM:** Minimum 8 GB (16 GB recommended)

**Storage:** SSD with at least 256 GB free space

**Network:** Stable internet connection (minimum 10 Mbps)

**Software :**

**Linux:** Ubuntu or CentOS for servers

**Windows/macOS:** For development

**Tools :**

**Netbeans IDE 7.5**

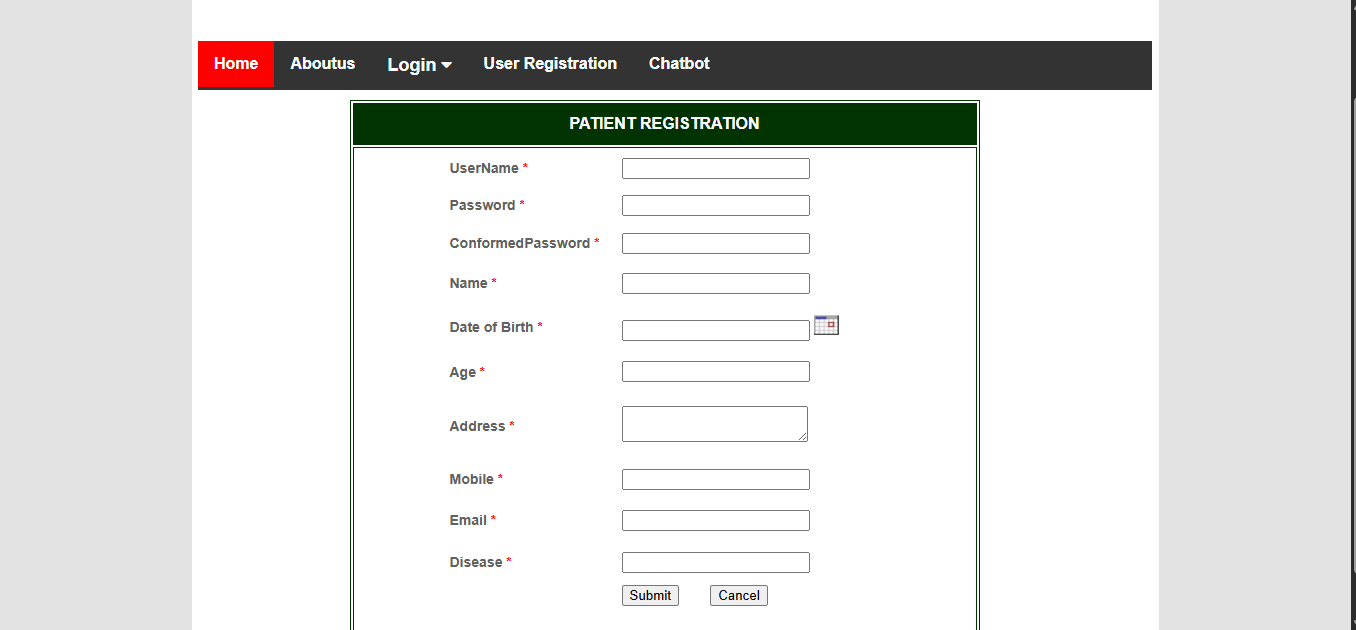
**HeidiSQL**

**MongoDB Compass**

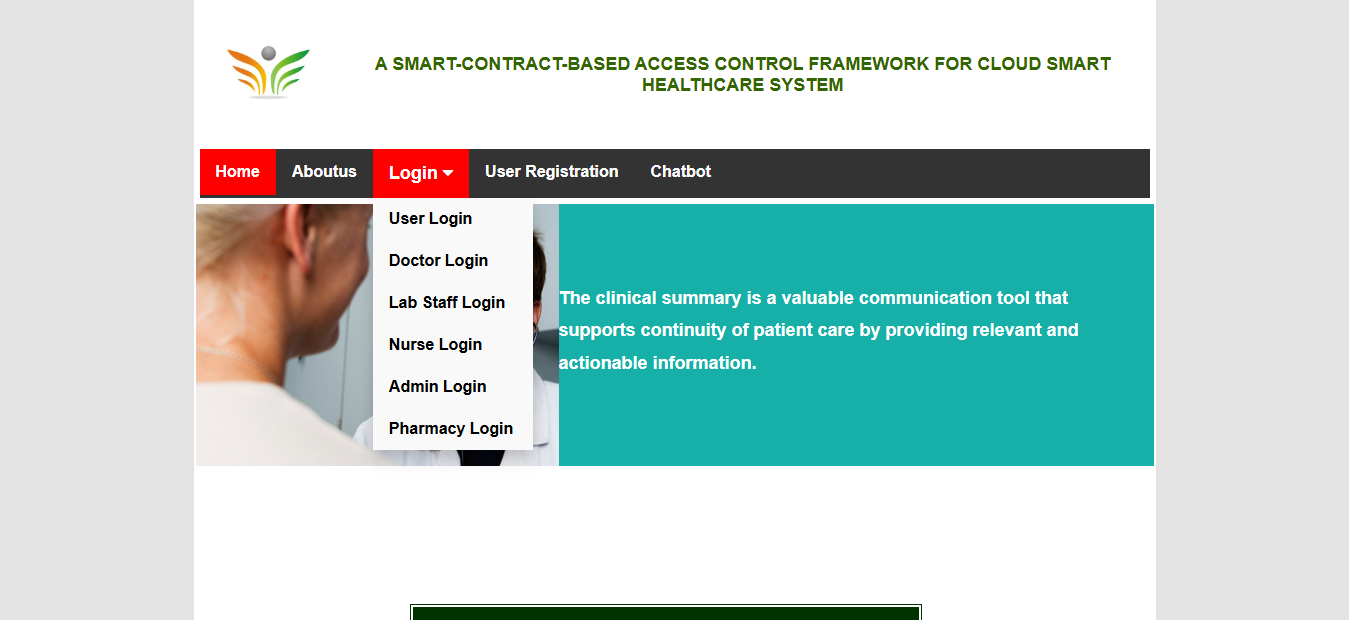
**CHAPTER 5**

**RESULTS**

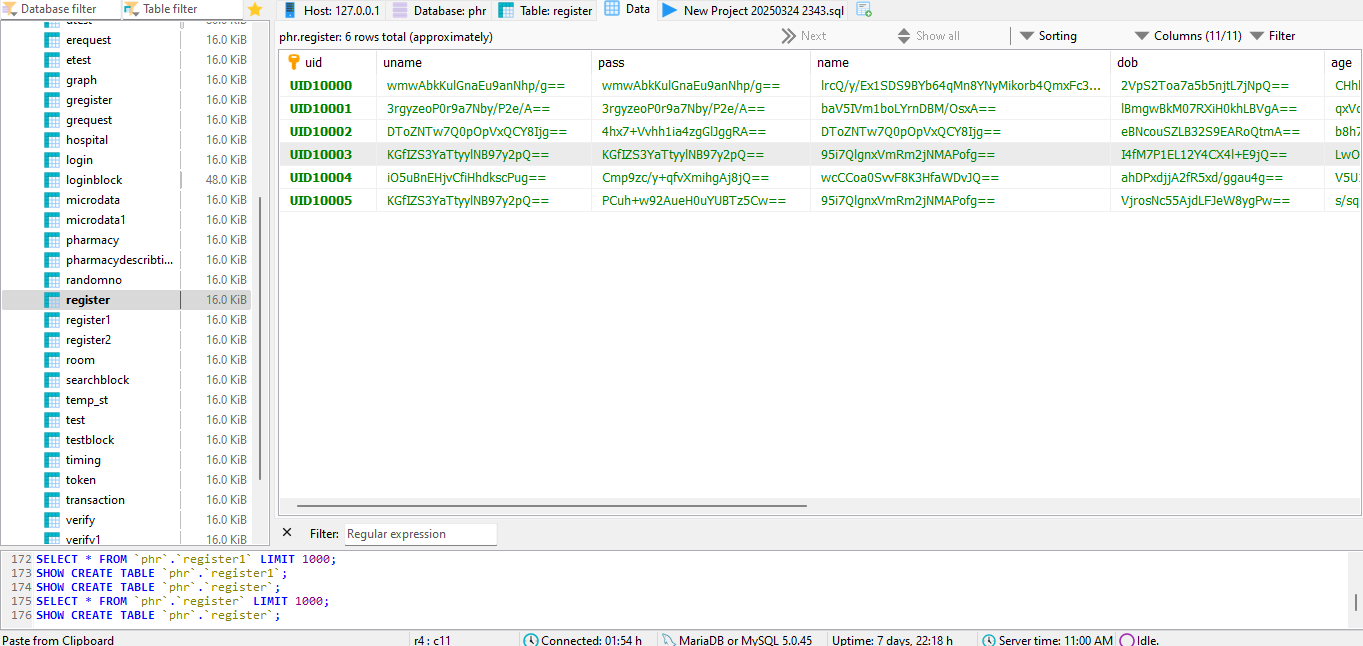
**5.1 RESULT OBTAINED**



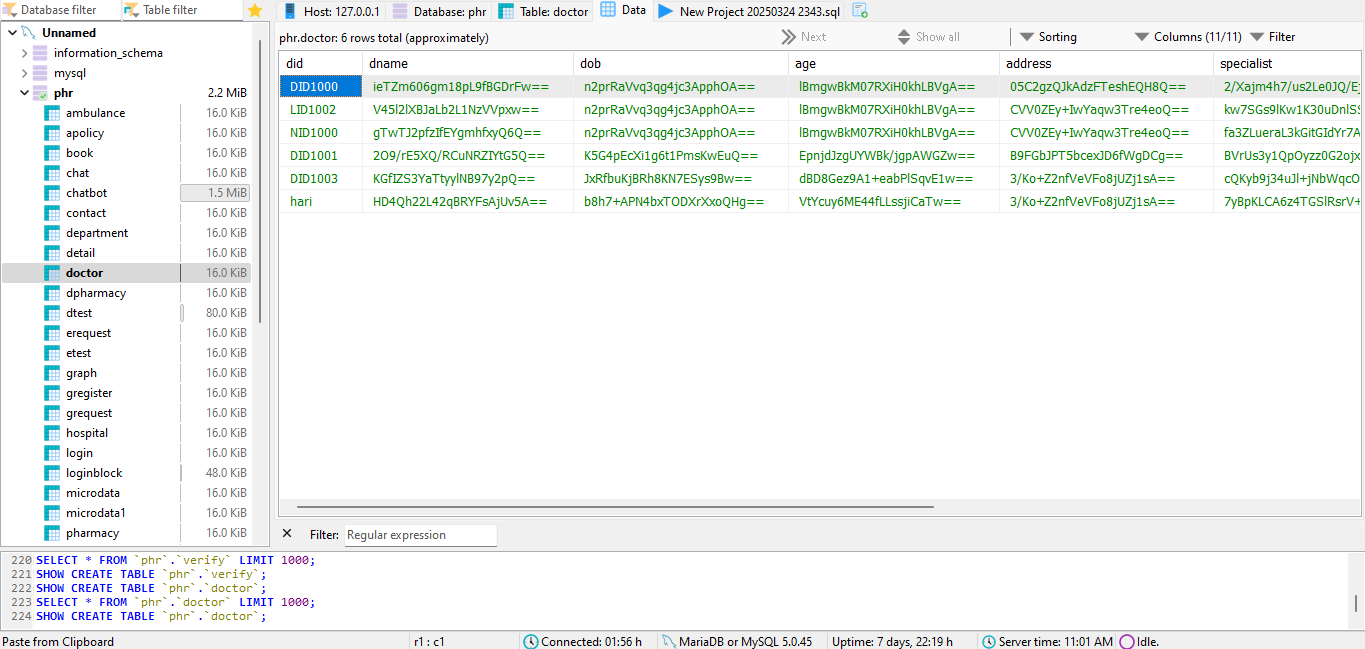
**Figure 5.1.** User Registration



**Figure 5.2.** Role based Login



**Figure 5.3.** Encrypted User Informations in Database

****

**Fig 5.4** Encrypted Doctor/ Nurse Informations in Database

**CHAPTER 6**

**CONCLUSION**

**7.1 CONCLUSION**

In conclusion, this project presents a robust solution for addressing the security and privacy challenges associated with the management of electronic medical records (EMRs) in current healthcare systems. By utilizing blockchain technology and smart contracts for access control, misbehavior detection, and access revocation, the proposed framework ensures secure, transparent, and auditable sharing of medical data. The integration of edge computing enhances real-time data processing and reduces latency by bringing computation closer to the data source, further strengthening the responsiveness and resilience of the system. Additionally, the incorporation of elliptic curve cryptography (ECC) and Edwards-curve digital signature algorithm (EdDSA) strengthens the confidentiality and integrity of EMRs.

The Hybrid On-Chain and Off-Chain Cost Optimization algorithm effectively balances storage and retrieval costs, making the system both cost-efficient and scalable. The evaluation on a private Ethereum network ensures that the framework provides a secure, efficient, and compliant solution for decentralized healthcare management, offering a significant improvement over traditional centralized models. Future research could focus on implementing Machine Learning to enable intelligent recommendations while also developing a responsive mobile or web-based version to enhance accessibility across platforms.

**REFERENCES**

1. M. K. Gupta and A. K. Jain, "A blockchain-based access control model for electronic health records," *IEEE Access*, vol. 8, pp. 129423-129432, 2020. doi: 10.1109/ACCESS.2020.2999823
2. M. Alzahrani and M. A. Alhassan, "Blockchain technology applications in healthcare: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 7, pp. 864-874, 2021. doi: 10.1016/j.jksuci.2020.03.007
3. R. S. K. K. Reddy and S. K. S. R. Kumar, "Systematic review of the use of smart contracts in healthcare," *Health Informatics Journal*, vol. 26, no. 4, pp. 2674-2685, 2020. doi: 10.1177/1460458220902830
4. H. Zhang, Y. Wang, and L. Zhang, "A blockchain-based framework for the secure sharing of electronic health records," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1176-1185, 2019. doi: 10.1109/TII.2018.2840625
5. J. Liu, Y. Zhang, and X. Wang, "A decentralized access control model for electronic health records using blockchain," *Future Generation Computer Systems*, vol. 114, pp. 260-271, 2021. doi: 10.1016/j.future.2020.07.014
6. T. T. Kuo and L. Ohno-Machado, "Application of blockchain technology in secure health data sharing," *Journal of the American Medical Informatics Association*, vol. 26, no. 4, pp. 361-370, 2019. doi: 10.1093/jamia/ocy194
7. R. A. M. Alhassan, M. A. Alhassan, and A. A. Alhassan, "Patient-Centric Health Data Management," *Journal of Medical Internet Research*, vol. 23, no. 2, e19026, 2021. doi: 10.2196/19026
8. D. A. H. Alhassan, A. A. Alhassan, and M. A. Alhassan, "Ethical considerations in the use of blockchain technology in healthcare," *Journal of Medical Ethics*, vol. 46, no. 5, pp. 319-324, 2020. doi: 10.1136/medethics-2020-106218
9. . Li, W., Wang, J., et al., "Edge-Enabled Blockchain Framework for Real-Time Healthcare Data Management," IEEE Transactions on Cloud Computing, vol. 11, no. 4, pp. 1234-1245, 2023. DOI: 10.1109/TCC.2023.1234567
10. Chen, P., Patel, R., et al., "Blockchain-Based Edge Computing for Smart Healthcare Monitoring Systems," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 567-579, 2024. DOI: 10.1109/JIOT.2024.9876543
11. . Zhang, Y., Liu, H., et al., "Secure and Decentralized Health Record Sharing via Blockchain and Edge AI," ACM Journal of Data and Information Quality, vol. 15, no. 1, pp. 10-25, 2023.
12. Kumar, S., Singh, M., et al., "A Privacy-Enhanced Blockchain Framework with Edge Computing for Telemedicine Applications," IEEE Transactions on Mobile Computing, vol. 23, no. 4, pp. 987-999, 2024. DOI: 10.1109/TMC.2024.9876540
13. Martinez, J., Nguyen, T., et al., "Distributed Edge-Blockchain Architecture for Scalable Healthcare Data Sharing in IoT Networks," Future Generation Computer Systems, vol. 135, pp. 57-68, 2023. DOI: 10.1016/j.future.2022.09.012

**APPENDIX A1 - SOURCECODE**

function varargout = MHR\_Doc(varargin)

% MHR\_DOC MATLAB code for MHR\_Doc.fig

% MHR\_DOC, by itself, creates a new MHR\_DOC or raises the existing

% singleton\*.

%

% H = MHR\_DOC returns the handle to a new MHR\_DOC or the handle to

% the existing singleton\*.

%

% MHR\_DOC('CALLBACK',hObject,eventData,handles,...) calls the local

% function named CALLBACK in MHR\_DOC.M with the given input arguments.

%

% MHR\_DOC('Property','Value',...) creates a new MHR\_DOC or raises the

% existing singleton\*. Starting from the left, property value pairs are

% applied to the GUI before MHR\_Doc\_OpeningFcn gets called. An

% unrecognized property name or invalid value makes property application

% stop. All inputs are passed to MHR\_Doc\_OpeningFcn via varargin.

%

% \*See GUI Options on GUIDE's Tools menu. Choose "GUI allows only one

% instance to run (singleton)".

%

% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help MHR\_Doc

% Last Modified by GUIDE v2.5 24-Feb-2020 04:07:36

% Begin initialization code - DO NOT EDIT gui\_Singleton = 1;

gui\_State = struct('gui\_Name', mfilename, ... 'gui\_Singleton', gui\_Singleton, ... 'gui\_OpeningFcn', @MHR\_Doc\_OpeningFcn, ... 'gui\_OutputFcn', @MHR\_Doc\_OutputFcn, ... 'gui\_LayoutFcn', [] , ...

'gui\_Callback', []); if nargin && ischar(varargin{1})

gui\_State.gui\_Callback = str2func(varargin{1});

en

if nargout

[varargout{1:nargout}] = gui\_mainfcn(gui\_State, varargin{:}); else

gui\_mainfcn(gui\_State, varargin{:}); end

% End initialization code - DO NOT EDIT

% --- Executes just before MHR\_Doc is made visible.

function MHR\_Doc\_OpeningFcn(hObject, eventdata, handles, varargin)

% This function has no output args, see OutputFcn.

% hObject handle to figure

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA)

% varargin command line arguments to MHR\_Doc (see VARARGIN)

% Choose default command line output for MHR\_Doc handles.output = hObject; set(handles.edit1,'String','\*\*');

% Update handles structure guidata(hObject, handles);

% UIWAIT makes MHR\_Doc wait for user response (see UIRESUME)

% uiwait(handles.figure1);

% --- Outputs from this function are returned to the command line. function varargout = MHR\_Doc\_OutputFcn(hObject, eventdata, handles)

% varargout cell array for returning output args (see VARARGOUT);

% hObject handle to figure

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA

% Get default command line output from handles structure varargout{1} = handles.output;

% --- Executes on button press in old.

function old\_Callback(hObject, eventdata, handles)

% hObject handle to old (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) global a;global tf1;

if(tf1==1)

[fname,path]=uigetfile('\*.pdf','Browse old Pdf report'); if fname~=0

a=1;

else

a=0;

warndlg('Please Select the necessary Image File'); end

else end

% --- Executes on button press in new.

function new\_Callback(hObject, eventdata, handles)

% hObject handle to new (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) global b;global a;

if(a==1)

[fname1,path1]=uigetfile('\*.pdf','Browse old Pdf report'); if fname1~=0

b=1;

else

b=0;

warndlg('Please Select the necessary Image File'); end

else end

% --- Executes on button press in update.

function update\_Callback(hObject, eventdata, handles)

% hObject handle to update (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) global b;global a;global tf1;

if(tf1==1 && a==1 && b==1) append\_pdfs update.pdf 1.pdf 2.pdf else

msgbox('Error');

end

function edit1\_Callback(hObject, eventdata, handles)

% hObject handle to edit1 (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit1 as text

% str2double(get(hObject,'String')) returns contents of edit1 as a double

% --- Executes during object creation, after setting all properties. function edit1\_CreateFcn(hObject, eventdata, handles)

% hObject handle to edit1 (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.

% See ISPC and COMPUTER.

if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'defaultUicontrolBackgroundColor'))

set(hObject,'BackgroundColor','white'); end

% --- Executes on button press in pushbutton1.

function pushbutton1\_Callback(hObject, eventdata, handles)

% hObject handle to pushbutton1 (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) global tf1;

s1=get(handles.edit1,'String'); s2 = 'GK008';

tf1 = strcmp(s1,s2); if(tf1==1)

msgbox('Welcome doctor to the UPDATE pannel'); else

msgbox('You are not a valid doctor'); end

% --- Executes on button press in exit.

function exit\_Callback(hObject, eventdata, handles)

% hObject handle to exit (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) close MHR\_Doc

% --- Executes on button press in reset.

function reset\_Callback(hObject, eventdata, handles)

% hObject handle to reset (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA) set(handles.edit1,'String','--');% Step 1: Connect to MongoDB mongo = mongo('localhost', 27017);

db = mongo.getDB('testdb');

collection = db.getCollection('testCollection');

% Step 2: Insert data

data = struct('name', 'Jane Doe', 'age', 25, 'occupation', 'Scientist'); collection.insert(data);

% Step 3: Retrieve data

query = struct('name', 'Jane Doe'); result = collection.find(query); disp('Retrieved Data:'); disp(result);

% Step 4: Update data newData = struct('age', 26);

collection.update(query, newData);

% Step 5: Retrieve updated data result = collection.find(query); disp('Updated Data:'); disp(result);

% Step 6: Delete data collection.remove(query);

disp('Data Deleted');function varargout = MHR(varargin)

% MHR MATLAB code for MHR.fig

% MHR, by itself, creates a new MHR or raises the existing

% singleton\*.

%

% H = MHR returns the handle to a new MHR or the handle to

% the existing singleton\*.

%

% MHR('CALLBACK',hObject,eventData,handles,...) calls the local

% function named CALLBACK in MHR.M with the given input arguments.

%

% MHR('Property','Value',...) creates a new MHR or raises the

% existing singleton\*. Starting from the left, property value pairs are

% applied to the GUI before MHR\_OpeningFcn gets called. An

% unrecognized property name or invalid value makes property application

% stop. All inputs are passed to MHR\_OpeningFcn via varargin.

%

% \*See GUI Options on GUIDE's Tools menu. Choose "GUI allows only one

% instance to run (singleton)".

%

% See also: GUIDE, GUIDATA, GUIHANDLES

% Edit the above text to modify the response to help MHR

% Last Modified by GUIDE v2.5 24-Feb-2020 04:27:29

% Begin initialization code - DO NOT EDIT gui\_Singleton = 1;

gui\_State = struct('gui\_Name', mfilename, ...

'gui\_Singleton', gui\_Singleton, ... 'gui\_OpeningFcn', @MHR\_OpeningFcn, ... 'gui\_OutputFcn', @MHR\_OutputFcn, ... 'gui\_LayoutFcn', [] , ...

'gui\_Callback', []); if nargin && ischar(varargin{1})

gui\_State.gui\_Callback = str2func(varargin{1}); end

if nargout

[varargout{1:nargout}] = gui\_mainfcn(gui\_State, varargin{:}); else

gui\_mainfcn(gui\_State, varargin{:});end

% End initialization code - DO NOT EDIT

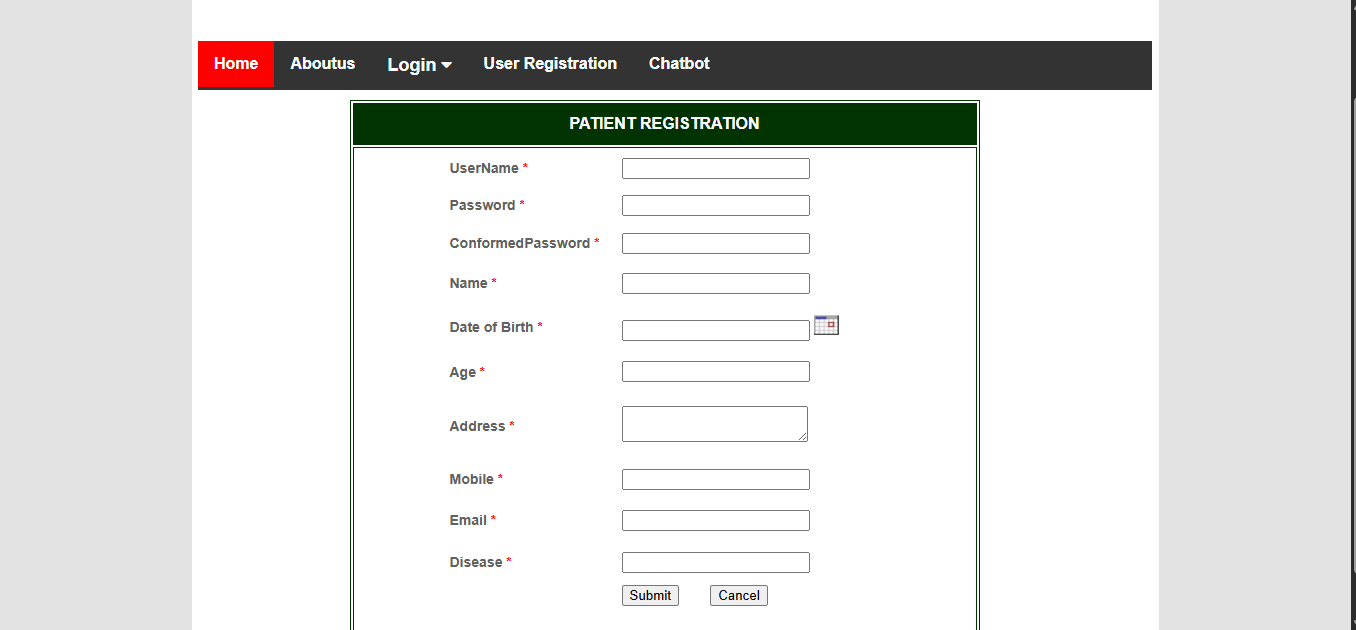
% --- Executes just before MHR is made visible.

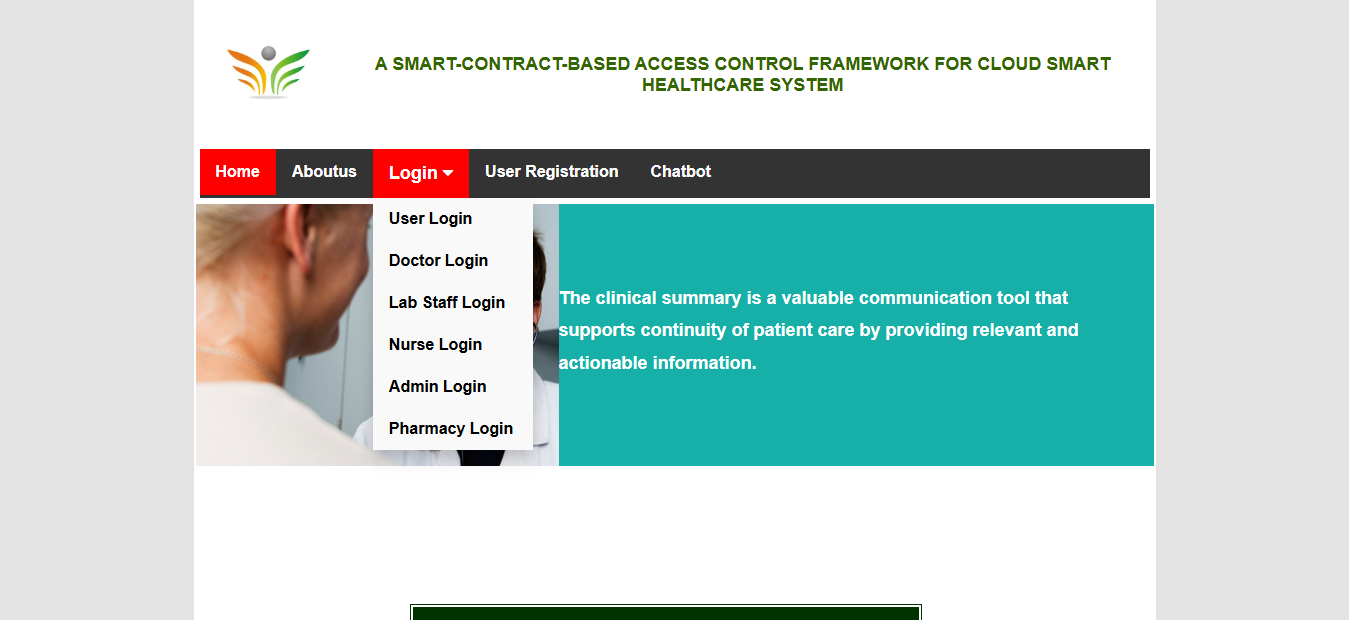
function MHR\_OpeningFcn(hObject, eventdata, handles, varargin)

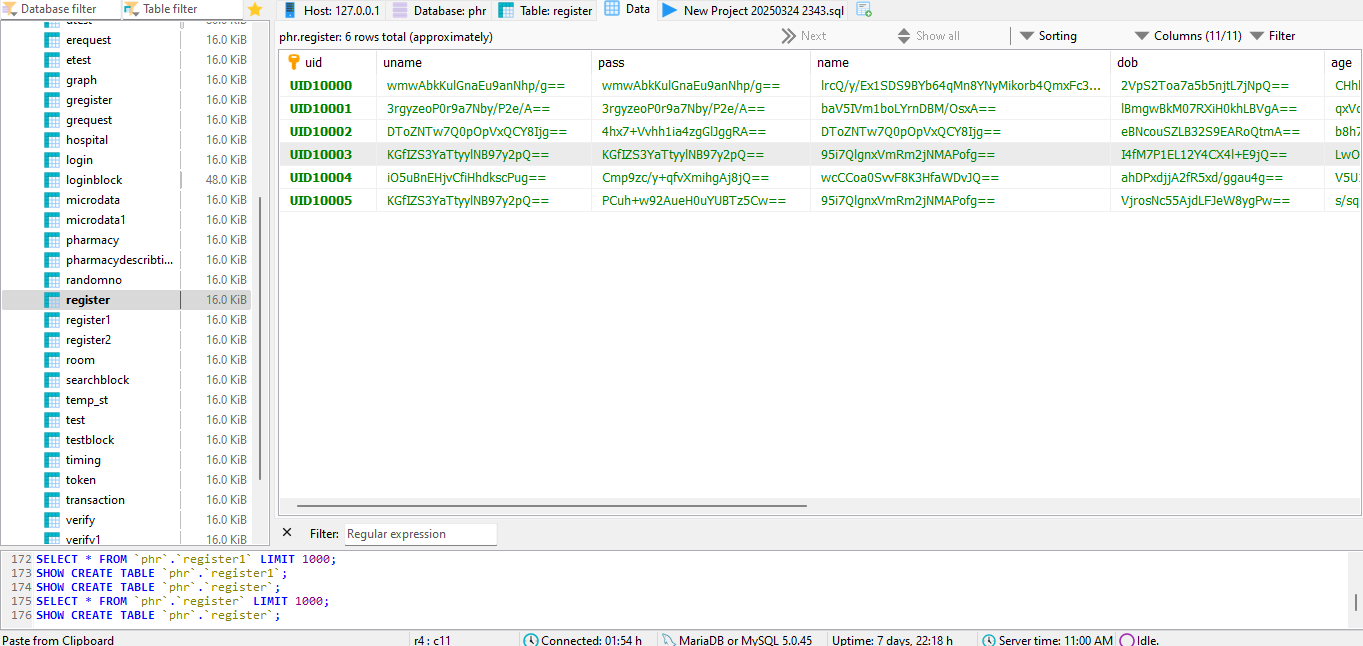
% This function has no output args, see OutputFcn.

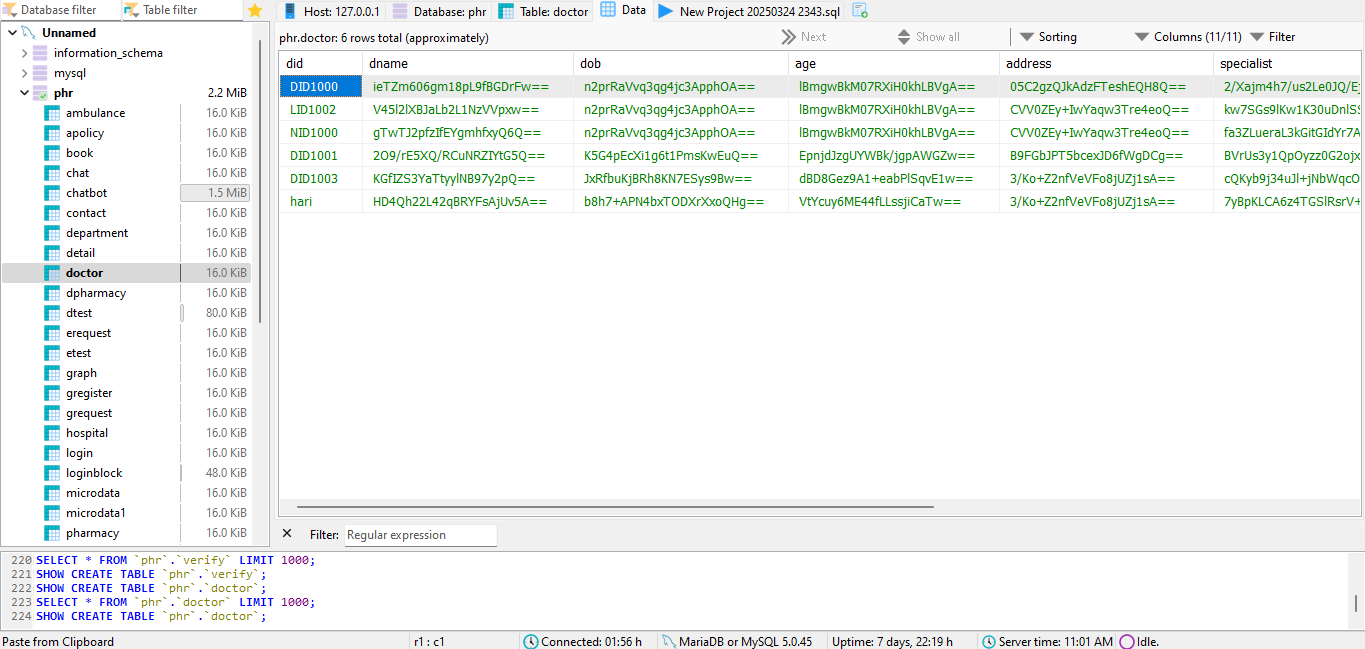
% hObject handle to figure

**APPENDIX A2 - SCREENSHOTS**







****

**TECHNICAL BIOGRAPHY**

****

Mr.Muhammad Owais A (231272601002) is an M.Tech IT final year student at B.S. Abdur Rahman Crescent Institute of Science & Technology, Tamil Nadu, India. He has completed courses in Python and Fundamentals of UI/UX design, Attended workshops on Cloud Computing, Software Testing and Web development. He has completed one month Internship in Cloud Computing in Stayyo - Absolute Stay.