

**Healthcare Consultancy Using Blockchain**

### Design & developed by

2111CS040041 – K. Akhil

2111CS040040 – D. Jathin

2111CS040001 – Md. Reyaz

**Guided By**

## Dr. G. Vasavi (Associate professor)

### Department of Computer Science & Engineering (Cyber Security) IV YR - I SEM

**Malla Reddy University, Hyderabad 2021-2025**



Department of Computer Science & Engineering (Cyber Security)

# CERTIFICATE

This is to certify that this is the Bonafide record of the application development entitled “**Healthcare Consultancy using Blockchain”,** submitted by **Md. Reyaz (2111CS040001), D. Jathin (2111CS040040), K. Akhil (2111CS040041)**, B. Tech IV year

I semester, Department of CSE (CS) during the year 2023-24. The results embodied in this report have not been submitted to any other university or institute for the award of any degree or diploma.

##### Internal Guide Head of the Department

**Dr. G. Vasavi Dr. G. Anand Kumar**

##### (Associate Professor) CSE (Cyber Security)

**External Examiner**

# DECLARATION

We hereby declare that the project report entitled “**Healthcare Consultancy using Blockchain**” has been carried out by us and this work has been submitted to **the Department of Computer Science and Engineering (Cyber Security), Malla Reddy University, Hyderabad**. We further declare that this project work has not been submitted in full or part for the award of any other degree in any other educational institutions.

Place:

Date:

K. Akhil 2111CS040041

D. Jathin 2111CS040040

Md. Reyaz 2111CS040001

# ACKNOWLEDGEMENT

We extend our sincere gratitude to all those who have contributed to the completion of this project report. Firstly, we would like to extend our gratitude to **Dr. V. S. K Reddy, Vice- Chancellor**, for his visionary leadership and unwavering commitment to academic excellence.

We would also like to express our deepest appreciation to our project guide **Dr. G. Vasavi , Associate Professor**, whose invaluable guidance, insightful feedback, and unwavering support have been instrumental throughout this project for successful outcomes.

We extend our gratitude to our **PRC convenor, Dr. G. Latha**, for giving valuable inputs and timely guidelines to improve the quality of our project through a critical review process. We thank our project coordinator, Mrs. Geetha yadav, for his timely support.

We are also grateful to our **Dr. G. Anand Kumar, Head of the Department of Cyber Security & IOT** for providing us with the necessary resources and facilities to carry out this project.

My heartfelt thanks also go to **Dr. Harikrishna Kamatham, Dean School of Engineering** for his guidance and encouragement.

We are deeply indebted to all of them for their support, encouragement, and guidance, without which this project would not have been possible.

##### K. Akhil 2111CS040041

**D. Jathin 2111CS040040**

**Md. Reyaz 2111CS040001**

**ABSTRACT**

The power of machine learning in understanding the patterns in data, analyzing and making decisions, has shown its importance in various sectors. Machine Learning requires reasonable amount of data to make accurate decisions. Data sharing and reliability of data is very crucial in machine learning in order to improve its accuracy. The decentralized database in Blockchain Technology emphasizes on data sharing. The consensus in Blockchain technology makes sure that data is legitimate and secured. The convergence of these two technologies can give highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology.

### INDEX

**Contents Page No.**

|  |  |  |
| --- | --- | --- |
| 1. | Introduction | 1-3 |
|  | 1.1 Problem Definition & Description | 1 |
|  | 1.2 Objectives of the Project | 2 |
|  | 1.3 Scope of the Project | 2-3 |
| 2. | System Analysis | 4-12 |
|  | 2.1 Existing System | 4-6 |
|  | 2.1.1 Background & Literature Survey | 5 |
|  | 2.1.2 Limitations of Existing System | 5-6 |
|  | 2.2 Proposed System | 6-7 |
|  | 2.2.1 Advantages of Proposed System |  |
|  | 2.3 Software & Hardware Requirements | 7-9 |
|  | 2.3.1 Software Requirements | 7-8 |
|  | 2.3.2 Hardware Requirements | 8-9 |
|  | 2.4 Feasibility Study | 9-12 |
|  | 2.4.1 Technical Feasibility | 9-11 |
|  | 2.4.2 Robustness & Reliability | 11-12 |
|  | 2.4.3 Economic Feasibility | 12 |
| 3. | Architectural Design | 13-21 |
|  | 3.1 Modules Design | 13-14 |
|  | 3.1.1 User Management module | 13 |
|  | 3.1.2 Authentication module | 13 |
|  | 3.1.3 Risk Assessment module | 13 |
|  | 3.1.4 Logging and Monitoring module | 14 |

* 1. [Method & Algorithm design 14](#_bookmark0)
     1. [User Management module 14](#_bookmark1)
     2. [Authentication module 14](#_bookmark2)
     3. [Algorithm Considerations 14](#_bookmark3)
     4. [Reporting & Monitoring methods 14](#_bookmark4)
  2. [Project Architecture 15-21](#_bookmark5)
     1. [Architectural Diagram 15](#_bookmark6)
     2. [Data Flow Diagram 16-17](#_bookmark7)
     3. [Class Diagram 16](#_bookmark8)
     4. [Use case Diagram 18-20](#_bookmark9)
     5. [Sequence Diagram 20](#_bookmark10)
     6. [Activity Diagram 21](#_bookmark11)

1. Implementation & Testing 22-43
   1. Coding Blocks 24-41

|  |  |  |  |
| --- | --- | --- | --- |
|  | 4.1.1 | Code Block 1 | 22-27 |
|  | 4.1.2 | Code Block 2 | 27-28 |
|  | 4.1.3 | Code Block 3 | 29-35 |
| 4.2 | Sample Code | | 35-37 |
| 4.3 | Execution Flow | | 38 |
| 4.4 | Testing |  | 38-39 |

1. Results
   1. Resulting Screens 40-46
2. Conclusions & Future Scope 47-48
   1. Conclusions 47
   2. Future Scope 47-48

|  |  |
| --- | --- |
| **List of Figures** | **page no** |
| 3.3.1 Architectural Diagram | 15 |
| 3.3.2 Data Flow Diagram | 16 |
| 3.3.3 Class Diagram | 17 |
| 3.3.4 Use Case Diagram | 18 - 20 |
| 3.3. Sequence Diagram | 20 |
| 3.3.6 Activity Diagram | 21 |

**List of Screen shots**

* + 1. Patient Registration 40
    2. Admin Login 40
    3. Admin Home 41
    4. Patient Activation 41
    5. Doctor Registration 41
    6. Patient login 42
    7. Patient Home Page 42
    8. Prescription 42
    9. Doctor Response 43
    10. Patient Transaction 43
    11. Doctor Login 43
    12. Doctor Home Page 44
    13. Analyze Symptoms 44
    14. View 44
    15. Transactions 45
    16. Admin View Transaction 45
    17. Transaction Manager 45

# CHAPTER – 1

## INTRODUCTION

Blockchain technology has emerged as a transformative solution in various sectors, including healthcare, due to its decentralized and secure nature. In healthcare, the significance of data cannot be overstated—it plays a crucial role in diagnosis, treatment, research, and overall patient care. However, traditional centralized data storage systems face challenges related to security, accessibility, and reliability.

By adopting blockchain technology, healthcare institutions can address these challenges effectively. Patient data, such as medical records, test results, and treatment plans, can be securely stored on a blockchain network. The decentralized nature of blockchain ensures that data is not stored in a single location, reducing the risk of data breaches and unauthorized access.

Moreover, blockchain technology provides a transparent and tamper-proof system. Each transaction or update to the data is recorded as a block, cryptographically linked to the previous block, forming a chain of immutable records. This feature ensures the integrity and trustworthiness of the data, making it ideal for sensitive healthcare information.

One of the key advantages of blockchain in healthcare is improved data accessibility and interoperability. Healthcare providers, researchers, and authorized stakeholders can access relevant patient data securely, regardless of their location or the systems they use. This seamless data exchange promotes better collaboration, timely decision-making, and improved patient outcomes.

Furthermore, blockchain technology enables the implementation of smart contracts in healthcare. Smart contracts are self-executing agreements based on predefined rules. In the context of healthcare, these contracts can automate processes such as insurance claims, billing, and consent management. Automation reduces administrative burdens, minimizes errors, and enhances operational efficiency.

### Problem Definition & Description Problem Definition :

In this proposal, the initial approach of charging fees in bitcoins for accessing patient records posed challenges such as potential misuse of patient data and increased costs for users. As a solution, the focus shifted from public to private blockchain networks in healthcare. Gem Health Network, utilizing Ethereum Blockchain Technology, emerged to facilitate secure information sharing among different entities. This transition enabled transparent access to the latest treatment information, preventing the use of outdated data and providing insights into past interactions between patients and physicians.

### Problem Description :

Moreover, blockchain's decentralized design pattern, initially popularized by Bitcoin, has evolved to meet the privacy needs of businesses. Permissioned blockchain networks offer a shared platform for multiple organizations to securely exchange business information while maintaining data privacy and security. Key components of such networks include a shared ledger, peer network for transaction validation, membership/certificate authority for user authentication, and smart contracts for automated business logic execution.

Machine learning has also emerged as a powerful tool in healthcare, offering capabilities such as treatment identification, personalized patient suggestions, and outbreak prediction. Techniques like tokenization and machine learning algorithms such as SVM classifier and Naive Bayes have been employed to analyse symptoms and provide accurate disease summaries. Additionally, machine learning models can offer lifestyle suggestions based on patients' medical history and current health status. Predictive models, such as Neural Network with SVM, have been utilized to forecast disease outbreaks by considering factors like rainfall, temperature, and past reported cases.

### Objectives of the Project :

Blockchain technology, coupled with machine learning models, presents innovative solutions to various challenges in healthcare. By issuing digital certificates to authenticate users, blockchain ensures secure transactions and data access while maintaining privacy and integrity. This authentication mechanism enables users to sign transactions, providing legitimacy and access rights to the ledger.

The integration of blockchain and machine learning offers several benefits:

1. **Data Availability:** Every authenticated user has a copy of the shared ledger, addressing the data acquisition problem. Machine learning models can directly access reliable data from the ledger, enhancing reliability and accuracy.
2. **Real Data Training:** With access to real data, machine learning models can be trained effectively, improving efficiency and reducing costs associated with centralized data repositories.
3. **Personalized Lifestyle Advice:** By analysing suggestions given to patients with similar symptoms, machine learning models can provide personalized lifestyle advice, enhancing patient care.
4. **Disease Identification and Treatment Suggestions:** Using natural language processing, trained models can identify diseases and offer treatment suggestions based on patient inquiries.
5. **Clinical Suggestions for Doctors:** Machine learning models can analyse patient symptoms and provide clinical suggestions to healthcare providers, improving diagnostic accuracy and treatment outcomes.
6. **Outbreak Prediction:** By analysing test reports and other relevant data stored in the blockchain, machine learning models can predict disease outbreaks and provide timely recommendations to healthcare professionals.
7. **Equipment Maintenance Prediction:** Machine learning models can predict the need for maintenance or replacement of medical equipment based on usage patterns and performance data stored in the blockchain.

However, certain considerations must be addressed:

1. **Data Integrity:** As blockchain ledgers are append-only, manual errors in data entry could occur. Proper oversight or additional privileges may be required to address this issue.
2. **Database Size:** The storage of transaction history in blockchain increases database size over time, potentially posing challenges in scalability and management. Strategies for efficient data storage and retrieval may be necessary to mitigate this issue.

### Scope of the Project :

The scope of a project aimed at integrating Blockchain Technology into Healthcare Systems can be

quite broad, as it touches on a wide range of critical aspects such as data security, privacy, interoperability, patient care, and the management of healthcare resources. Below is a breakdown of the potential scope, highlighting key objectives, deliverables, and technologies involved.

##### Key Areas of Focus:

**Patient Data Security:** Blockchain can create a secure, tamper-proof system for managing electronic health records (EHRs), ensuring only authorized access.

**Data Sharing and Interoperability:** Blockchain can allow seamless sharing of patient data between different healthcare providers without needing a central authority.

**Smart Contracts:** Automating tasks like insurance claims, medical billing, and prescriptions with blockchain-based smart contracts, making processes faster and more accurate.

**Supply Chain Transparency:** Blockchain can track the movement of pharmaceuticals and medical supplies, ensuring authenticity and reducing counterfeit products.

**Clinical Trials and Research Integrity:** Blockchain can ensure transparency and prevent manipulation of clinical trial data.

##### Technologies Used:

* Blockchain platforms like Ethereum or Hyperledger.
* Cryptography for securing data.
* APIs to integrate with existing healthcare systems.

##### Challenges:

* Ensuring regulatory compliance (e.g., HIPAA, GDPR).
* Ensuring scalability and seamless integration with existing systems.

##### Key Deliverables:

1. A blockchain-based system for managing EHRs securely.
2. Smart contracts to automate healthcare processes.
3. A supply chain tracking solution for pharmaceuticals.
4. An interoperability framework for data exchange.

##### Timeline:

1. **Research & Design**: 2-3 months
2. **Development & Testing**: 4-6 months
3. **Pilot Deployment**: 2-3 months
4. **Scaling & Evaluation**: 3-6 months

# CHAPTER – 2

## System Analysis

The advances in the Information and Communications Technology (ICT) brought many benefits to the healthcare area, specially to digital storage of patients' health records. However, it is still a challenge to have a unified viewpoint of patients' health history, because typically health data is scattered among different health organizations. Furthermore, there are several standards for these records, some of them open and others proprietary. Usually, health records are stored in databases within health organizations and rarely have external access. This situation applies mainly to cases where patients' data are maintained by healthcare providers, known as EHRs (Electronic Health Records). In case of PHRs (Personal Health Records), in which patients by definition can manage their health records, they usually have no control over their data stored in healthcare providers' databases. Thereby, we envision two main challenges regarding PHR context: first, how patients could have a unified view of their scattered health records, and second, how healthcare providers can access up-to-date data regarding their patients, even though changes occurred elsewhere.

For addressing these issues, this work proposes a model named OmniPHR, a distributed model to integrate PHRs, for patients and healthcare providers use. The scientific contribution is to propose an architecture model to support a distributed PHR, where patients can maintain their health history in a unified viewpoint, from any device anywhere. Likewise, for healthcare providers, the possibility of having their patient’s data interconnected among health organizations. The evaluation demonstrates the feasibility of the model in maintaining health records distributed in an architecture model that promotes a unified view of PHR with elasticity and scalability of the solution. Cybercriminals have begun to target the healthcare industry with ransomware, malware that encrypts an infected device and any attached devices or network drives. After encryption, cybercriminals demand a ransom before releasing the devices from encoding. Without adequate disaster recovery and backup plans, many businesses are forced to pay the ransom. We examined the extent of recent ransomware infections in healthcare settings, the risk liabilities and costs associated with such infections, and possible risk mitigation tactics. The methodology of this study was a literature review. The review was limited to sources published in English from 2005 to 2017.

Financial costs associated with business recovery after ransomware attacks on healthcare facilities are significant and are growing in both magnitude and scope. Other risks are a loss of future business and reputation damage. Research has suggested that the best plan of action is to have a proper business continuity and disaster plan with adequate data backups and to be vigilant in educating employees about the sources of ransomware to prevent potential attacks. Healthcare is one of the most vulnerable sectors of cyber-attacks. As it continues to expand exponentially and moves to digitally-enabled healthcare services, cyber-criminals are trying to take advantage of the weaknesses and security vulnerabilities correlated with these shifts. As a result of technical developments, a multitude of highly powerful risks such as Ransomware is facing the healthcare sector. Ransomware is cyber-attack targeting companies and household users and has increased lately due to its productive results. It conflicts have significantly improved over the last few years. The study shows an exhaustive survey on Ransomware attacks and fixes these attacks. The main aim of this study is to classify the solution strategies for Ransomware attacks in healthcare that used to prevent the Ransomware, such as Blockchain technology, Software define network technology, Machine Learning, and other tools as well as to highlight many issues faced by researchers during the process of discovering a way to solve Ransomware attacks in health care systems.

* + V. P. Aggelidis and P. D. Chatzoglou, ‘‘Using a modified technology acceptance model in hospitals,’’ Int. J. Med. Informat., vol. 78, no. 2, pp. 115–126, 2009.
  + V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, ‘‘A hierarchical multi blockchain for fine grained access to medical data,’’ IEEE Access, vol. 8, pp. 134393– 134412, 2020.
  + M.Marwan,A.A.Temghart,F.Sifou,andF.AlShahwan,‘‘Adecentralized blockchainbased architecture for a secure cloud-enabled IoT,’’ J. Mobile Multimedia, vol. 2020, pp. 389– 412, Nov. 2020.
  + R. H. Hylock and X. Zeng, ‘‘A blockchain framework for patient centered health records and exchange (HealthChain): Evaluation and proof-of-concept study,’’ J. Med. Internet Res., vol. 21, no. 8, Aug. 2019, Art. no. e13592.
  + T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, ‘‘Blockchain for the meta verse: A review,’’ 2022, arXiv:2203.09738.

### Existing System

* + 1. **Background & Literature Survey :**

In present systems there is hardly remote locations lack access to medical services, forcing people to travel long distances for treatment.

* Even in urban areas, immediate medical service isn't always available, leading to communication gaps between patients and doctors.
* Patients often experience long wait times to communicate with doctors.
* Confidentiality of data is a major concern in ml communication.
* Systems addressing these issues are termed Health Information Exchange (HIE) systems.

### Limitations of Existing System :

While traditional healthcare systems have improved over the years, they still face several limitations that blockchain technology aims to address.

##### Data Security and Privacy Concerns

* + **Problem**: Current healthcare systems often rely on centralized databases, which are vulnerable to cyberattacks and data breaches. Unauthorized access to sensitive patient data (like medical records) can occur if systems are not properly secured.
  + **Impact**: This compromises patient privacy and can lead to identity theft, fraud, or misuse of health information.

##### Lack of Interoperability

* + **Problem**: Different healthcare providers use incompatible systems, making it difficult to share patient data securely and efficiently. Each organization has its own electronic health records (EHR) systems, leading to fragmented and siloed information.
  + **Impact**: This creates delays in treatment, duplicate tests, and administrative inefficiencies, especially in emergencies when rapid access to complete patient history is critical.

##### Inefficient and Manual Processes

* + **Problem**: Many healthcare processes (such as insurance claims, billing, and prescription management) are still manual or semi-automated, involving paperwork or slow systems prone to errors.
  + **Impact**: This results in administrative overhead, fraud, billing errors, and delays in payments or services. It also increases costs and workload for healthcare professionals.

##### Inconsistent Medical Supply Chain

* + **Problem**: The pharmaceutical and medical equipment supply chains are often opaque, making it hard to trace the origin and authenticity of products. Counterfeit drugs and medical supplies are major concerns.
  + **Impact**: This undermines patient safety and can lead to the use of ineffective or dangerous products.

##### Data Integrity Issues in Clinical Trials

* + **Problem**: Clinical trial data is often manually recorded, and there is a risk of manipulation or falsification of results.
  + **Impact**: This threatens the credibility of scientific research, the approval of new drugs, and the overall safety of patients in clinical trials.

##### Regulatory and Compliance Challenges

* + **Problem**: Healthcare data must comply with strict regulations (e.g., HIPAA in the U.S., GDPR in the EU). Existing systems may struggle to ensure full compliance, particularly in terms of data access, encryption, and auditability.
  + **Impact**: Non-compliance can result in legal penalties and fines, and it can undermine patient trust in the healthcare system.

##### Limited Patient Control Over Their Own Data

* + **Problem**: In existing systems, patients typically have limited control or visibility over how their health data is shared or used by healthcare providers.
  + **Impact**: This can lead to lack of trust and concerns over data privacy, especially when patients are unaware of how their data is being accessed or used for research, billing, or treatment.

### Proposed System :

* + 1. **Advantages of Proposed System :**

##### Advantages of Proposed System

The integration of **blockchain technology** into healthcare systems offers several advantages that address the limitations of existing systems.

##### Enhanced Data Security and Privacy:

**Advantage:** Blockchain offers strong encryption and decentralized data storage, making it far

more secure than centralized databases.

**Impact:** Patient data is stored in a tamper-proof, immutable ledger that cannot be altered without consensus from network participants, ensuring data integrity and reducing the risk of breaches or unauthorized access. Patients can control access to their own data, ensuring privacy.

##### Improved Interoperability

**Advantage:** Blockchain enables seamless and secure data sharing across different healthcare organizations and systems without needing a central authority.

**Impact:** Healthcare providers, labs, and insurance companies can access accurate and real-time data, reducing information silos. This ensures that medical professionals have the most up-to-date patient information, leading to better-coordinated care and faster, more informed decision-making.

##### Automation and Efficiency with Smart Contracts

**Advantage:** Smart contracts automate processes like insurance claims, billing, and medication prescriptions, reducing reliance on manual systems.

**Impact:** This reduces administrative overhead, human error, and fraud, making processes faster and more efficient. For example, insurance claims can be automatically validated and paid, streamlining reimbursements and ensuring faster transactions.

##### Transparency and Traceability in the Supply Chain

**Advantage:** Blockchain allows for end-to-end traceability of pharmaceuticals, medical supplies, and equipment.

**Impact:** All products in the supply chain can be tracked in real-time from manufacturer to patient, ensuring authenticity and preventing the distribution of counterfeit drugs. This enhances patient safety and improves trust in healthcare products.

##### Enhanced Data Integrity in Clinical Trials

**Advantage:** Blockchain provides an immutable record of clinical trial data, ensuring that the information remains accurate and unaltered.

**Impact:** This ensures the transparency and integrity of clinical research, preventing data manipulation and increasing trust in the results. It also makes it easier for regulatory bodies to audit and verify clinical trial data, improving the approval process for new treatments and drugs.

### Software & Hardware Requirements:

* + 1. **Software Requirements:**

##### Blockchain Platform/Framework:

* + - * **Ethereum**: A widely-used blockchain platform for developing decentralized applications

(DApps) and smart contracts.

* + - * **Hyperledger Fabric**: An enterprise-grade permissioned blockchain framework, ideal for healthcare systems that require secure and private data handling.

##### Smart Contract Development:

* + - * **Solidity (for Ethereum)**: A programming language used to write smart contracts on the Ethereum blockchain.
      * **Chaincode (for Hyperledger Fabric)**: The equivalent of smart contracts in Hyperledger, written in Go or JavaScript.
      * **Rust or C++ (for Solana)**: Programming languages for writing smart contracts on Solana.

##### Distributed Ledger Technology (DLT) Tools:

* + - * **IPFS (InterPlanetary File System)**: A distributed file storage system for storing patient data or medical records off-chain while keeping references on-chain, ensuring scalability and efficiency.
      * **Arweave**: A permanent, decentralized storage solution ideal for healthcare data that needs to be preserved immutably.

##### Databases & Storage Systems:

* + - * **SQL/NoSQL Databases**: For storing metadata, transaction logs, and non-sensitive data (e.g., MySQL, PostgreSQL, MongoDB).
      * **Blockchain Nodes**: Each healthcare provider and participant in the blockchain network may require local nodes for maintaining and validating transactions on the blockchain.

##### Healthcare Data Interoperability Tools:

* + - * **FHIR (Fast Healthcare Interoperability Resources)**: A standard for exchanging healthcare data, supported by many blockchain platforms for improving data interoperability.
      * **HL7**: Another standard used in healthcare data sharing.
      * **APIs**: Custom APIs for integrating existing healthcare systems (e.g., EHRs, patient management software) with blockchain networks

### Hardware Requirements :

##### Servers for Blockchain Nodes:

* + **High-Performance Servers**: Servers that can handle the processing load of blockchain transactions and smart contract execution. These should have:
    - **CPU**: Multi-core processors (e.g., Intel Xeon, AMD EPYC) for handling concurrent transactions and smart contract operations.
    - **RAM**: A minimum of 16 GB (preferably 32 GB or more for high-traffic systems).
    - **Storage**: SSD storage (at least 1 TB) for fast data retrieval and processing of blockchain records.
    - **Network**: High-speed internet connection with low latency (e.g., 1 Gbps or more) for seamless data sharing and transaction validation.

##### Patient Data Storage:

* + **Cloud Storage**: For storing large medical records securely off-chain (e.g., Amazon S3, Microsoft Azure, or Google Cloud).
  + **On-Premise Data Centers**: For institutions that prefer to store critical patient data on their premises, suitable for HIPAA-compliant environments.

##### Hardware Security Modules (HSMs):

* + For secure management of cryptographic keys used for data encryption and digital signatures. This is essential for maintaining confidentiality and integrity in patient data exchanges.

##### End-User Devices:

* + **Workstations**: Computers or laptops for healthcare providers (doctors, nurses, admins) to access and manage the blockchain system.
  + **Mobile Devices**: Smartphones and tablets for patients and healthcare providers to interact with the system through apps, including accessing EHRs, prescription history, etc.
  + **IoT Devices**: For real-time health data collection (e.g., wearable devices or sensors) that can interface with the blockchain network to automatically record health information.

##### Network Infrastructure:

* + **Routers/Switches**: High-performance networking equipment to ensure reliable and fast communication between blockchain nodes and other connected healthcare systems.
  + **VPNs**: Virtual Private Networks for secure communication between remote healthcare providers and the blockchain network.
  + **Firewalls**: To protect the blockchain network and connected devices from external attacks and ensure secure data transmission.

### Feasibility Study :

* + 1. **Technical Feasibility :**

The **technical feasibility** of implementing a **blockchain-based healthcare system** hinges on several factors, including technology maturity, scalability, integration with existing systems, and the ability to handle complex healthcare data. This section evaluates the key technical aspects that determine whether the proposed blockchain solution can be successfully implemented in healthcare environments.

##### Blockchain Technology Readiness

* + - * **Maturity of blockchain platforms :**

Leading blockchain platforms like **Ethereum**, **Hyperledger Fabric**, and **Corda** have matured significantly in recent years. These platforms are widely used in industries such as finance and supply chain management, making them well-suited for handling healthcare data. For example:

* + - * + **Hyperledger Fabric** offers a permissioned blockchain, ideal for private and secure healthcare environments.
        + **Ethereum** supports **smart contracts** that automate transactions, which can be used for tasks like insurance claims and billing.
        + **Corda** focuses on maintaining privacy and allows organizations to share only necessary data, a key requirement in healthcare.

These platforms are stable and have established ecosystems, making them viable for use in healthcare systems.

##### Blockchain Consensus Mechanisms:

Consensus algorithms like **Proof of Authority (PoA)** (for Hyperledger Fabric) and **Proof of Stake (PoS)** (for Ethereum) are well-suited for enterprise use. These mechanisms are efficient and secure for permissioned blockchain systems, where speed and privacy are essential.

##### Data Security and Privacy

* + - * **Encryption**:

Blockchain’s inherent security features, such as **hashing** and **encryption** (AES-256), make it a suitable technology for securing sensitive healthcare data. Data on the blockchain can be encrypted, ensuring that even if data is intercepted, it remains unreadable to unauthorized parties.

##### Private vs Public Blockchain :

Given the sensitive nature of healthcare data, **permissioned blockchains** (e.g., Hyperledger Fabric) are more appropriate than public blockchains (like Ethereum) because they offer better control over who can participate in the network and access data. Private blockchains ensure that patient information is shared only with authorized entities, enhancing privacy.

##### Digital Identity :

**Blockchain-based identity management** systems can be used to securely store and verify patient identities. With the help of **Public Key Infrastructure (PKI)**, patients and healthcare providers can interact securely, ensuring that only the right people have access to sensitive data.

In summary, **blockchain technology** offers a technically feasible solution for modernizing

healthcare systems, improving data security, reducing fraud, and ensuring better patient care. The technology is mature, scalable, and well-suited to the complex needs of the healthcare industry.

### Robustness & Reliability :

When considering the implementation of blockchain in healthcare, robustness and reliability are crucial factors to ensure the system is secure, functional, and sustainable over time. This section evaluates how blockchain technology addresses the demands of healthcare systems with regard to system stability, fault tolerance, uptime, and resilience to attacks or failures.

##### Robustness of Blockchain Technology

**Blockchain’s robustness** refers to the ability of the technology to function effectively under varying conditions, maintain data integrity, and ensure that the system can handle high demand without failure.

##### Immutability:

* + - * + **Key Feature**: Blockchain records are immutable, meaning once data is written to the blockchain, it cannot be altered or deleted. This ensures that healthcare data, such as patient medical records or clinical trial data, remains unmodified and reliable.
        + **Impact**: This immutability enhances data integrity and prevents unauthorized changes, tampering, or manipulation, which is particularly important for regulatory compliance in healthcare.

##### Decentralization:

* + - * + **Key Feature**: Blockchain is a **decentralized** technology, meaning there is no central authority that controls the data. Instead, a distributed network of nodes maintains the blockchain.
        + **Impact**: This decentralization ensures that the system is more robust against single points of failure. Even if one node or server fails, the network can continue operating, making the system more resilient to outages or attacks. For healthcare, this means that patient data can be securely accessed by authorized parties, even in the event of a server failure.

##### Fault Tolerance:

* + - * + **Key Feature**: Blockchain networks are fault-tolerant due to the replication of data across multiple nodes. In permissioned blockchains like **Hyperledger Fabric** or **Corda**, data is maintained by multiple validators/nodes, and consensus mechanisms ensure the network remains functional even if some nodes fail.
        + **Impact**: Healthcare applications require continuous uptime, especially when dealing with critical patient data or treatment records. Blockchain ensures fault tolerance, meaning if a part of the network fails, the system will still function and continue processing transactions.

##### Consistency:

* + - * + **Key Feature**: Blockchain ensures data consistency across all nodes in the network.

Once a transaction is validated and recorded, it is propagated to all participants.

* + - * + **Impact**: In healthcare, ensuring consistency is vital for accurate patient records, as discrepancies in patient data across different healthcare providers can lead to misdiagnoses or incorrect treatments.

Overall, blockchain's **robustness** and **reliability** make it a strong candidate for improving the security, efficiency, and transparency of healthcare systems, while ensuring the continuous availability of critical data.

### Economic Feasibility :

**Economic feasibility** refers to the **cost-effectiveness** of adopting a blockchain-based healthcare system. It evaluates whether the benefits derived from blockchain implementation justify the initial and ongoing costs, and if the system is financially sustainable over time. In the context of healthcare, economic feasibility also involves considering long-term savings, the efficiency of operations, and potential for innovation in patient care and administrative processes.

This section outlines the **cost considerations**, **potential savings**, and **economic benefits** of implementing blockchain technology in healthcare.

Moreover, the planned utilization of freely available resources underscores the project's ability to leverage existing tools and technologies without incurring additional costs. By harnessing these resources, the project can allocate financial resources more efficiently, directing them towards areas of critical importance such as development and implementation.

##### Conclusion: Economic Feasibility

Blockchain implementation in healthcare offers both **high initial costs** and **ongoing operational costs**, particularly for technology infrastructure, integration, and compliance. However, the long- term **economic benefits**—including reduced administrative costs, decreased fraud, enhanced data sharing, and better patient outcomes—offer the potential for significant **cost savings**.

* + - * **Initial Investment**: $200,000 to $1,000,000 (depending on scale)
      * **Ongoing Operational Costs**: $50,000 to $250,000 annually (for maintenance, data storage, compliance)
      * **Potential Savings**: $500,000 to $2,000,000 annually (from fraud reduction, administrative cost savings, improved data sharing)

Ultimately, the **economic feasibility** of a blockchain-based healthcare system is **high** for large and mid-sized healthcare organizations, with **positive ROI** and a relatively short payback period, especially if the system is scaled across multiple stakeholders (e.g., hospitals, insurance providers, and patients). The technology offers long-term financial sustainability by driving efficiencies and reducing fraud and errors in a complex, data-intensive industry.

* 1. **Modules Design:**

# CHAPTER – 3

## Architectural Design

### User Management module :

##### Functions:

Handles user registration, login, and profile management. Stores user credentials securely (hashed passwords).

##### Security Considerations :

* Implement strong password hashing algorithms (e.g., SHA 256).
* Enforce password complexity requirements.

### Authentication module :

##### Functions:

* Authenticates users based on username/password

##### Security Considerations :

* Employ secure communication protocols for all authentication requests.
* Implement rate limiting to prevent brute-force attacks.
* Enforce one-time passwords (OTP) for stronger user authentication.

### Risk Assessment module :

##### Functions:

Analyses user login attempts for potential anomalies (e.g. login failure). Leverages machine learning models trained on historical data to identify suspicious behaviour. Scores login attempts based on risk.

##### Data Sources :

* User provided details (Email, Username – Password,)
* Third-party security reports (if applicable)
* User login attempts (successful and failed)

##### Security Considerations :

* Regularly update the risk assessment model with new data and security threats.
* Ensure data privacy by anonymizing sensitive user information used for training

### Logging and Monitoring module :

##### Functions:

Logs all user login attempts (successful and failed), MFA usage, and security events. Provides real-time monitoring dashboards to identify suspicious activity and potential breaches.

##### Security Considerations :

* Stores the User password with encryption into the database.
* Security question is provided by the user so the answer can only be known by authentic user.

### Method & Algorithm design :

### User Management module :

##### Registration:

Users provide username, password, and contact information (phone number, email) during account creation. Password hashing with a secure algorithm (e.g., SHA-256) should be used for password storage, never storing plain text passwords.

### Authentication module :

**Login Process**: User enters username and password. The system verifies the password against the hashed password stored for that user.

### Algorithm Considerations :

**Password Hashing Algorithm:** Use a secure, well-established hashing algorithm like SHA 256 for password storage. These algorithms make it computationally expensive to crack passwords.

### Reporting & Monitoring methods :

**Logging:** Log all login attempts (successful/failed), MFA usage data and security events (e.g., suspicious login attempts).

**Reporting:** Generate reports on login activity, successful/failed MFA attempts, and potential security threats.

**Alerting:** Implement an alerting system that sends notifications for suspicious activity or potential security breaches based on pre-defined rules (e.g., multiple failed login attempts from unknown locations).

### Project Architecture :

### Architectural Diagram :

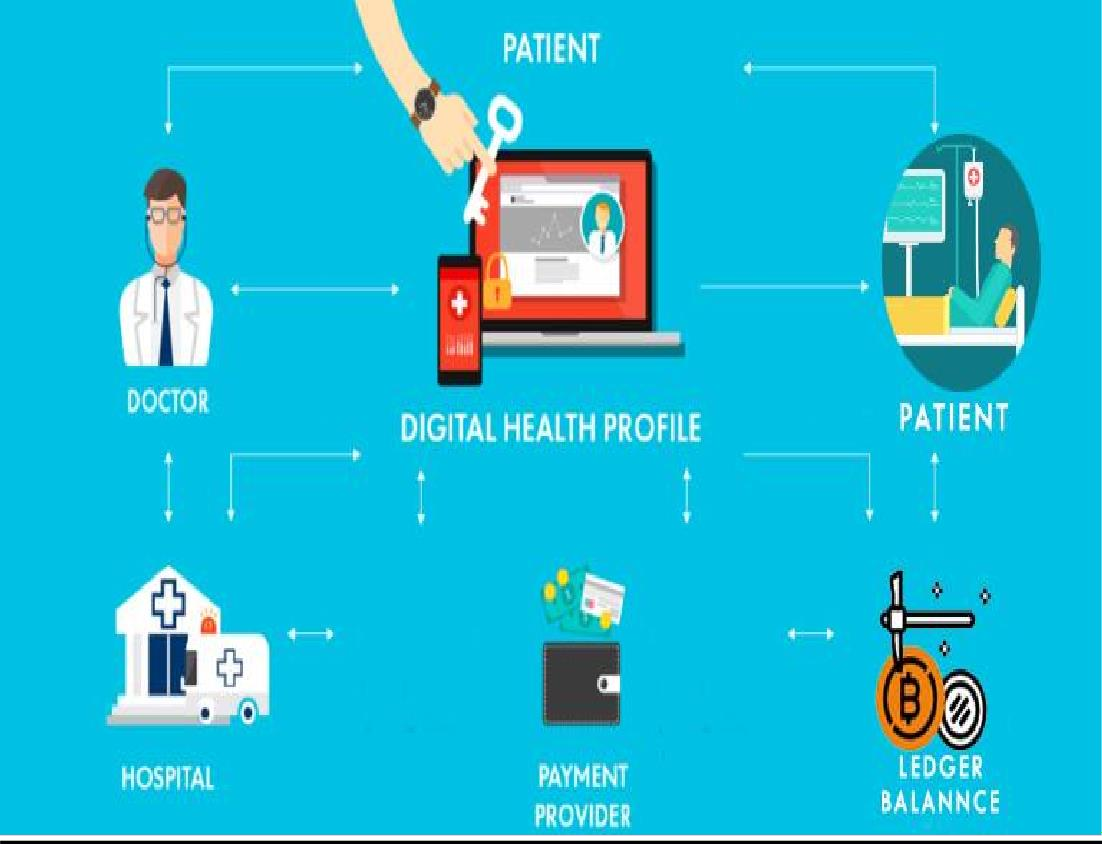


fig 3.3.1 Architecture Diagram

* + - * The user arrives at the website’s homepage.
      * They are presented with two options: sign up or sign in.
      * If the user chooses to sign up, they are directed to a new doctor/patient registration form.
      * On the sign-up form, the user enters their details including their first name, last name, email address, username, password and confirms their password.
      * After completing the form, the user’s information is validated.
      * The flowchart shows two possible outcomes after validation. One path indicates that the user receives a confirmation email. It is unclear from this flowchart which path a user would follow.
      * Once the user’s details are confirmed, their information is saved to a database.
      * The user is then directed to the website’s homepage.
      * The user can now sign out if they wish to do so.

### Data Flow Diagram :

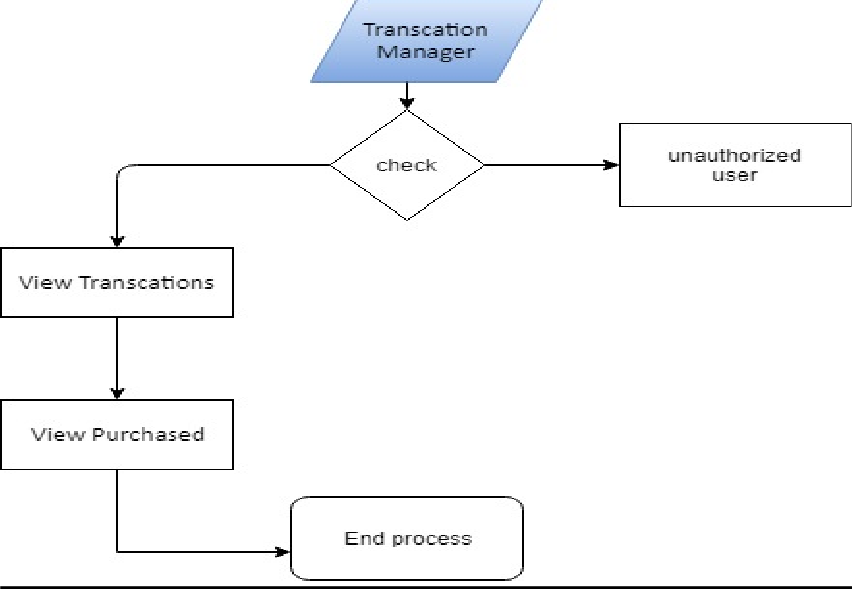
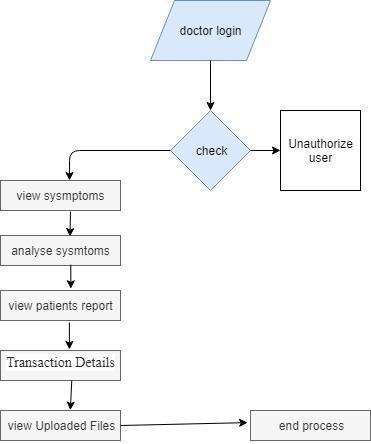
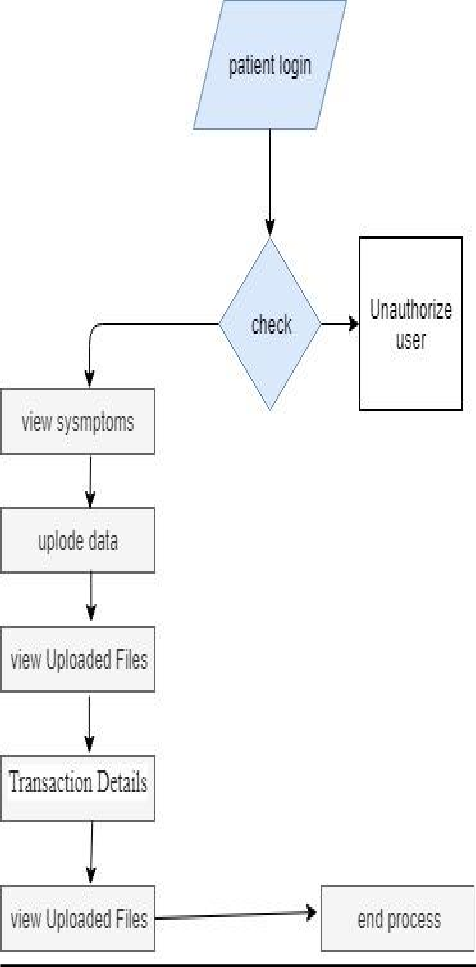


fig 3.3.2 Data Flow Diagram

* + - * The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
      * The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
      * DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
      * DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

### Class Diagram :

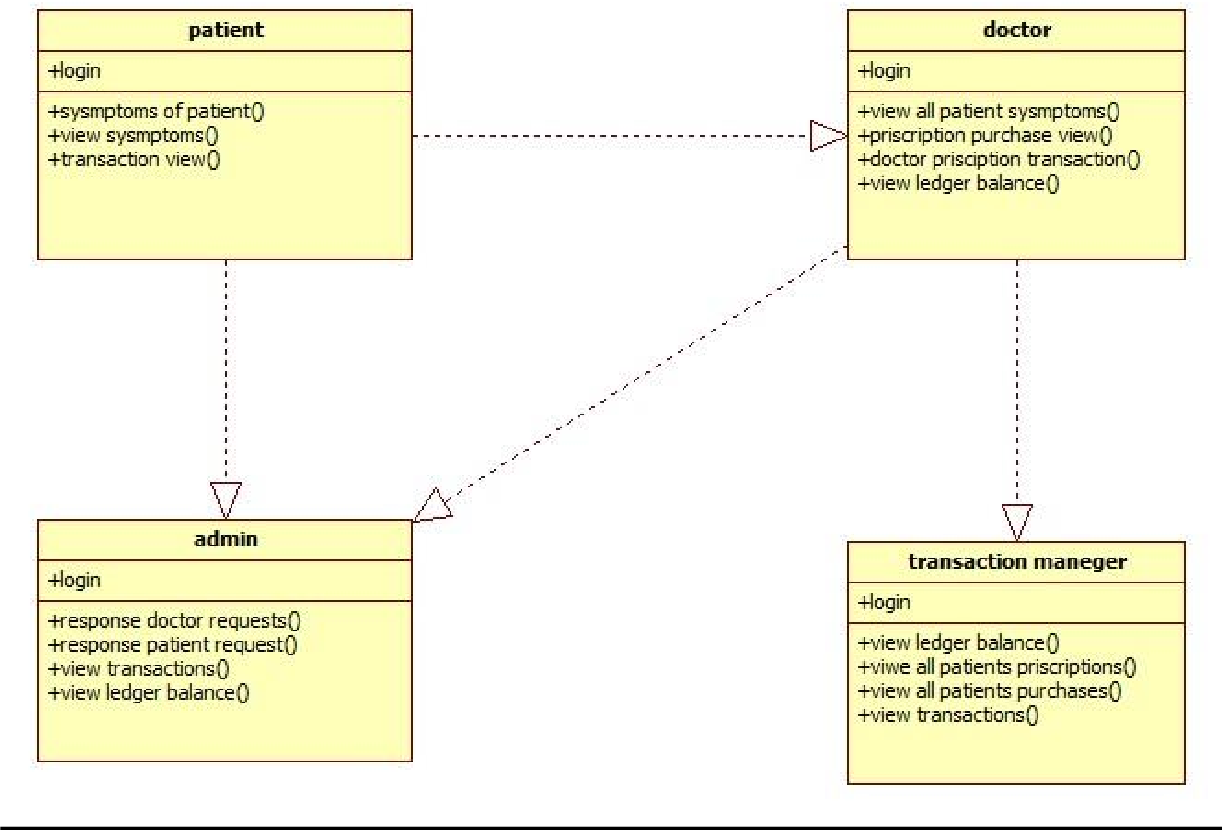
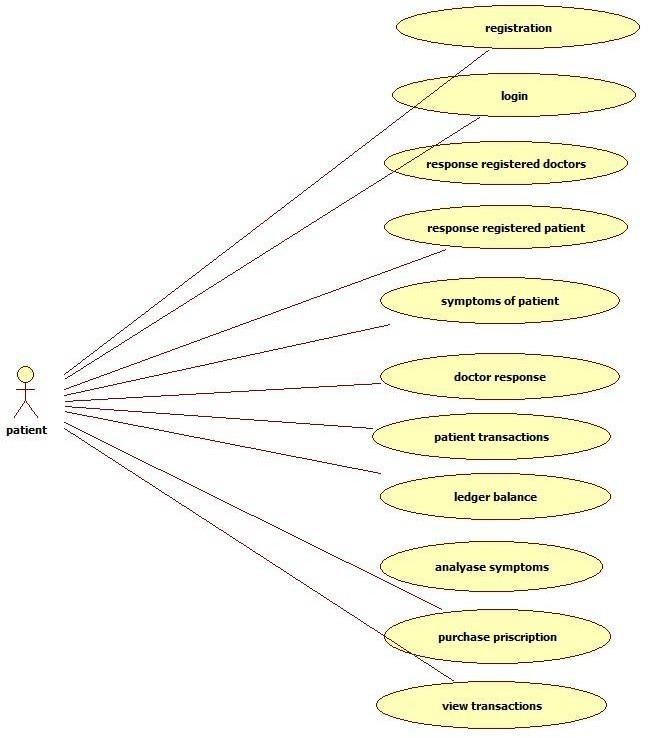
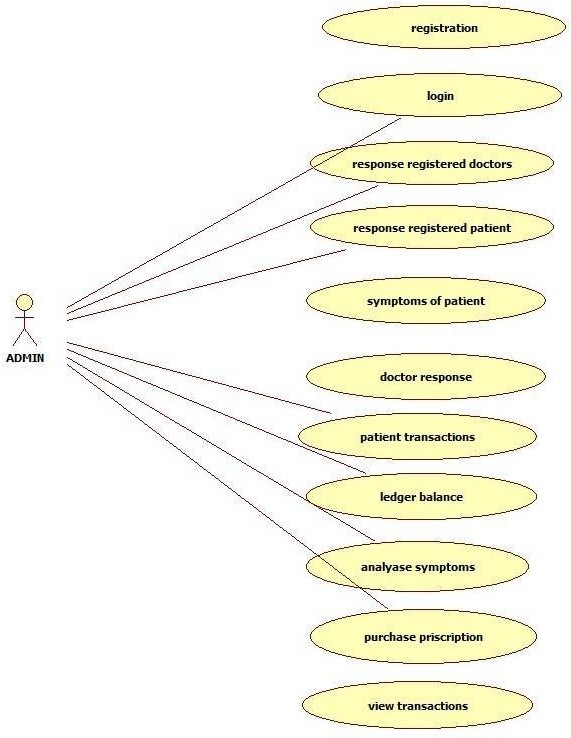
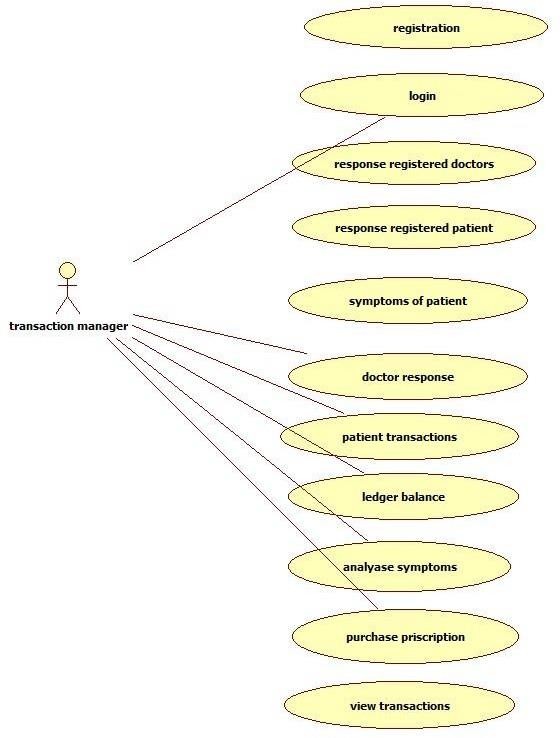


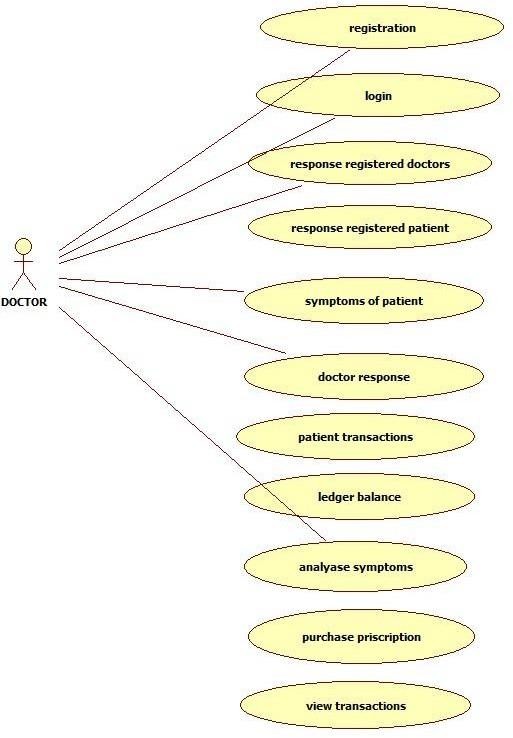
fig 3.3.3 Class Diagram

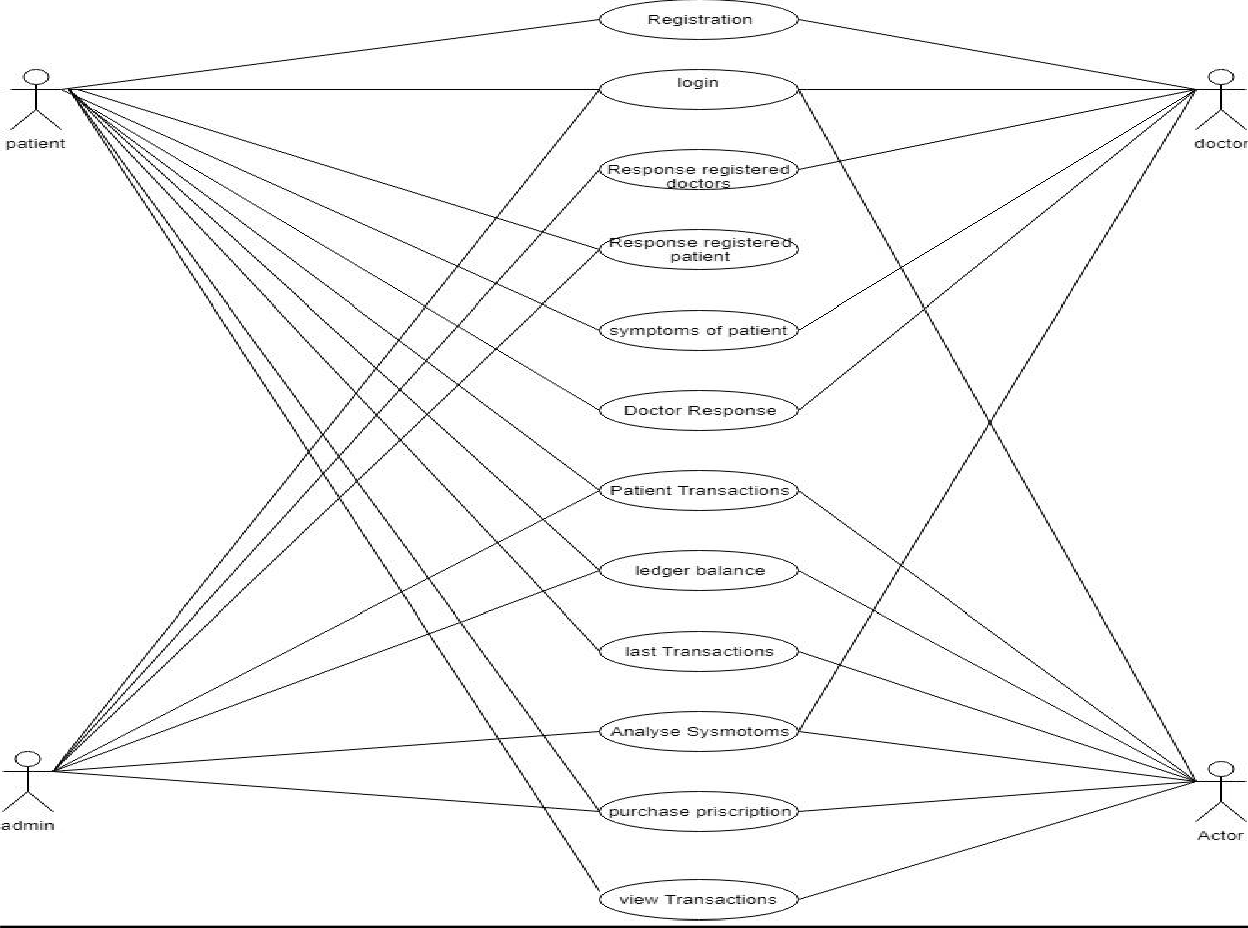
### Use case Diagram :











* + 1. **Sequence Diagram :**

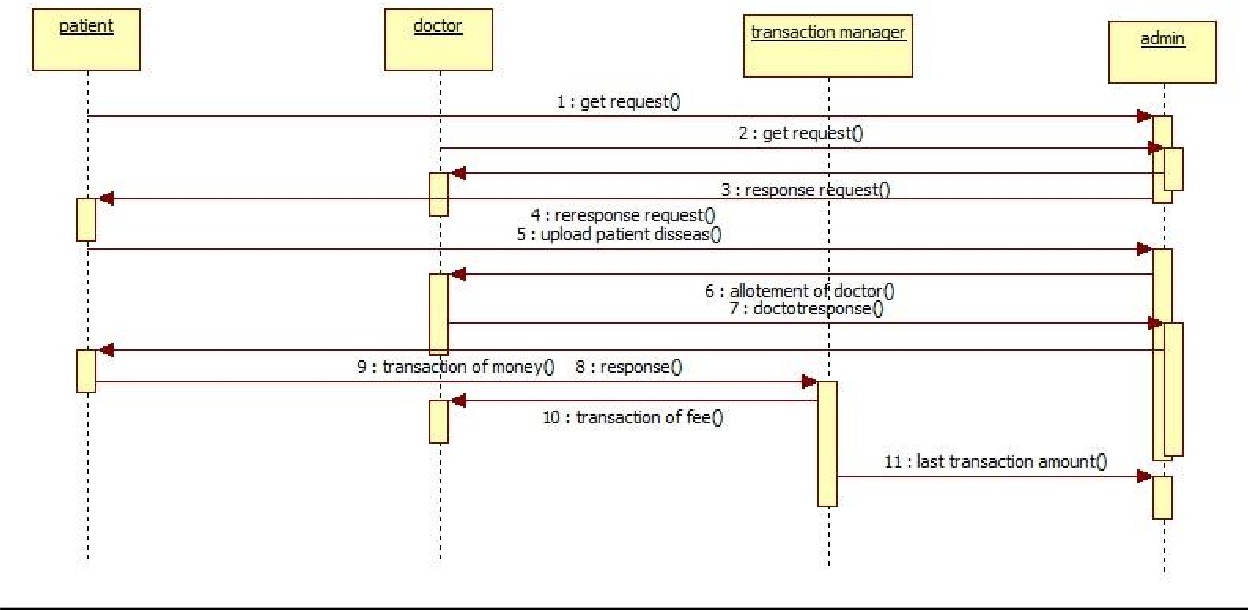


fig 3.3.5 Sequence Diagram

### Activity Diagram :

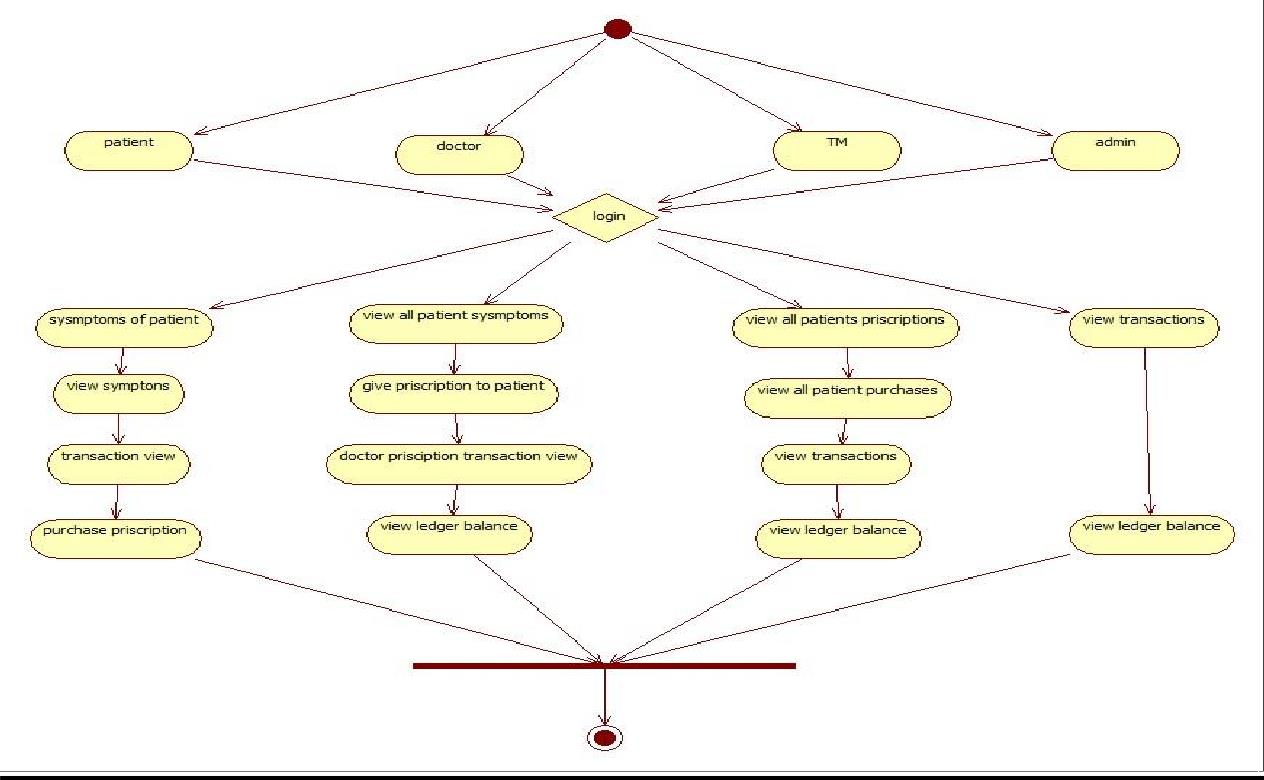


fig 3.3.6 Activity Diagram

### Coding Blocks :

* + 1. **Code Block 1 : Sign – up :**

##### Patient registration :

def patientregister(request): if request.method=='POST':

# CHAPETR - 4

## Implementation & Testing

form=patientregistrationform(request.POST) if form.is\_valid():

print('Am Not Human but no humanity') form.save()

messages.success(request, 'Youhavebeen successfullyregistered') return HttpResponseRedirect('patient')

else:

print("Invalid form") else:

form = patientregistrationform()

return render(request,'patientregister.html',{'form':form})

##### patient login :

def patientlogincheck(request): if request.method == "POST":

usid = request.POST.get('username') pswd =request.POST.get('password') try:

check =patientregistrationmodel.objects.get(loginid=usid, password=pswd) request.session['userid'] = check.id

request.session['loggeduser'] =check.name print("patient id ",check.id)

status = check.status

if status == "activated":

return render(request,'patients/patientpage.html') else:

messages.success(request, 'YourAccount Notyet activated') return render(request,'patient.html')

return render(request,'patients/patientpage.html') except:

pass

messages.success(request, 'Invalid User id and password') return render(request,'patient.html')

##### Doctorregistration :

def doctorregistration(request): if request.method=='POST':

form =doctorregistrationform(request.POST) if form.is\_valid():

form.save()

messages.success(request, 'Youhavebeen successfullyregistered') return HttpResponseRedirect('doctor')

else:

print("Invalid Form") else:

form = doctorregistrationform()

return render(request,'doctorregister.html',{'form':form})

##### Doctor login :

def doctorlogincheck(request):

if request.method == "POST":

usid = request.POST.get('loginid') pswd =request.POST.get('password') try:

check = docotrtregistrationmodel.objects.get(loginid=usid, password=pswd) request.session['docid'] = check.id

request.session['loggeddoc'] =check.doctorname status = check.status

print("Doc id ",check.id) if status == "activated":

return render(request,'doctors/doctorspage.html') else:

messages.success(request, 'YourAccount Not at activated') return render(request,'doctor.html')

return render(request,'doctors/doctorspage.html') except Exception as e:

print('Exception is ',str(e)) messages.success(request, 'Invalid Login Details') return render(request,'doctor.html')

##### Admin actions :

def adminlogin(request):

return render(request,'adminlogin.html') def adminloginaction(request):

if request.method == "POST":

if request.method == "POST":

usid = request.POST.get('username') pswd = request.POST.get('password') if usid == 'admin' and pswd == 'admin':

return render(request,'admins/adminhome.html') else:

messages.success(request, 'Invalid user id and password') return render(request,'adminlogin.html')

def viewadminpatientspage(request):

patientdata = patientregistrationmodel.objects.all()

#return HttpResponse("Redirect toAdmin View Patients")

return render(request,'admins/viewppatientsdata.html',{'object':patientdata}) def viewadmindoctorspage(request):

docotrtdata = docotrtregistrationmodel.objects.all() #return HttpResponse("Redirect toAdmin View Patients")

return render(request,'admins/viewdoctordata.html',{'object':docotrtdata}) #return render(request,'adminactivateDoctors.html')

def viewadmintransactionspage(request):

ledbal =transactionsstore.objects.aggregate(Sum('ledgerbalance')) x = ledbal.get("ledgerbalance sum")

x = round(x,2)

print("Total Ledger Balance",x) id = request.session['docid']

obj=transactionsstore.objects.last() print("The Last Transactin ID ",obj)

print("Latest Ledger Balance ",obj.ledgerbalance) userdata = transactionsstore.objects.all() lststate = {

'ledbalance':x

}

return render(request,"admins/viewadmintransactionspage.html",{'object':userdata,'dph':lststate,'dpdet':obj})

# return HttpResponse("Redirect to Transaction Page")

#return render(request,'adminaviewtransactions.html') def logout(request):

return render(request,'home.html')

##### Activation of Account byAdmin :

def activatepatients(request): if request.method=='GET':

pid = request.GET.get('pid') authkey =random\_with\_N\_digits(8) status = 'activated'

print("PID = ",pid,authkey,status) patientregistrationmodel.objects.filter(id=pid).update(authkey=authkey , status=status) patientdata = patientregistrationmodel.objects.all()

#return HttpResponse("Redirect toAdmin View Patients")

return render(request,'admins/viewppatientsdata.html',{'object':patientdata}) def activatedoctors(request):

if request.method=='GET': pid =request.GET.get('pid')

authkey =random\_with\_N\_digits(8) status = 'activated'

print("PID = ",pid,authkey,status) docotrtregistrationmodel.objects.filter(id=pid).update(authkey=authkey , status=status) docotordata = docotrtregistrationmodel.objects.all()

#return HttpResponse("Redirect toAdmin View Patients")

return render(request,'admins/viewdoctordata.html',{'object':docotordata})

##### Transaction Manager :

def trnxviewtransaction(request): if request.method=='GET':

ledbal = transactionsstore.objects.aggregate(Sum('ledgerbalance'))

x = ledbal.get("ledgerbalance sum") x = round(x,2)

print("Total Ledger Balance",x) id = request.session['docid']

obj=transactionsstore.objects.last() print("The Last Transactin ID ",obj)

print("Latest Ledger Balance",obj.ledgerbalance) userid = request.session['userid']

userdata=transactionsstore.objects.filter(docid=id) lststate = {

'ledbalance':x

}

return render(request,"admins/trnxviewtransac.html",{'object':userdata,'dph':lststate,'dpdet':obj}) def trnxviewpurchase(request):

docdataset = doctorreplaysysmptoms.objects.filter(status='purchase')

return render(request,"admins/trnxviewpurchase.html",{'object':docdataset})

* + 1. **Code Block 2 :**

##### Urls.py :

from django.contrib import admin

from django.conf.urls import url,include

from .views import home,trnxmngrloginaction,trnxviewtransaction,trnxviewpurchase from .views import

patient,patientregister,doctor,doctorregistration,adminlogin,txmanagerlogin,adminloginaction from .views import viewadminpatientspage,viewadmindoctorspage,viewadmintransactionspage,logout,activatepatien ts,activatedoctors

from patients.urls import urlpatterns as patients\_urlpattern from patients.views import

patientlogincheck,patientsendsymptoms,patientsymtomsanalysis,patientsymptomsview,checkand

pay,transactionmanagement,patientpurchaseblkmodel from doctors.views import

doctorlogincheck,doctoranalyzesysmptoms,DoctorsSendPriscription,DoctorPriscription,purchase viewbydoctor,doctorviewtransaction

urlpatterns = [

#url(r'^patients/',include((patients\_urlpattern,'patients'),namespace='patients'),name='patients'), url(r'^admin/', admin.site.urls),

url(r'^$',home, name="home"), url(r'^patient/', patient, name="patient"), url(r'^home/',home, name="home"),

url(r'^patientregister/',patientregister, name="patientregister"), url(r'^doctor/',doctor, name="doctor"), url(r'^doctorregistration/',doctorregistration, name="doctorregistration"), url(r'^adminlogin/',adminlogin, name="adminlogin"), url(r'^txmanagerlogin/',txmanagerlogin, name="txmanagerlogin"), url(r'^adminloginaction/',adminloginaction,name="adminloginaction"),

url(r'^viewadminpatientspage/',viewadminpatientspage,name="viewadminpatientspage"), url(r'^viewadmindoctorspage/',viewadmindoctorspage,name="viewadmindoctorspage"),

url(r'^viewadmintransactionspage/',viewadmintransactionspage,name="viewadmintransactionspa ge"),

url(r'^logout/',logout,name="logout"), #url(r'^activatepatients/',activatepatients,name="activatepatients") url(r'^activatepatients/$', activatepatients, name="activatepatients"), url(r'^activatedoctors/$', activatedoctors, name="activatedoctors"), url(r'^trnxmngrloginaction/',trnxmngrloginaction,name="trnxmngrloginaction"), url(r'^trnxviewtransaction/',trnxviewtransaction,name="trnxviewtransaction"), url(r'^trnxviewpurchase/',trnxviewpurchase,name="trnxviewpurchase"), url(r'^patientlogincheck/', patientlogincheck, name="patientlogincheck"), url(r'^patientsendsymptoms/', patientsendsymptoms, name="patientsendsymptoms"),

url(r'^patientsymtomsanalysis/', patientsymtomsanalysis, name="patientsymtomsanalysis"), url(r'^patientsymptomsview/',patientsymptomsview, name="patientsymptomsview"), url(r'^checkandpay/',checkandpay, name="checkandpay")

url(r'^transactionmanagement/', transactionmanagement, name="transactionmanagement"), url(r'patientpurchaseblkmodel/',patientpurchaseblkmodel, name="patientpurchaseblkmodel"), url(r'^doctorlogincheck/',doctorlogincheck, name="doctorlogincheck"), url(r'^doctoranalyzesysmptoms/',doctoranalyzesysmptoms,name="doctoranalyzesysmptoms"), url(r'^DoctorsSendPriscription/',DoctorsSendPriscription, name="DoctorsSendPriscription"), url(r'^DoctorPriscription/',DoctorPriscription,name="DoctorPriscription"), url(r'^purchaseviewbydoctor/',purchaseviewbydoctor,name="purchaseviewbydoctor"), url(r'^doctorviewtransaction/',doctorviewtransaction,name="doctorviewtransaction"),

]

### Code Block 3 :

##### Home.html :

{% extends 'base.html' %}

{% block contents%}

<div class="jumbotron">

<div class="container">

<h1 class="display-3">Securing Data with Blockchain and AI</h1>

<p>The power of machine learning in understanding the patterns in data, analyzing and making decisions, has shown its importance in various sectors. Machine Learning requires reasonable amount of data to make accurate decisions. Data sharing and reliability of data is very crucial in machine learning in order to improve its accuracy. The decentralized database in Blockchain Technology emphasizes on data sharing. The consensus in Blockchain technology makes sure that data is legitimate and secured. The convergence of these two technologies can give highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology. This paper gives an overview of how combining these two technologies can help in healthcare sectors. </p>

<p><a class="btn btn-primary btn-lg" href="https://ieeexplore.ieee.org/document/8701230" role="button">Learn more &raquo;</a></p>

</div>

</div>

<div class="container">

<!-- Example row of columns -->

<div class="row">

<div class="col-md-4">

<h2>INTRODUCTION</h2>

<p>Data is a very important resource in machine learning. The data can also be used in preprocessing techniques for improving research environments. The data can be gathered from interviews, questionnaire, surveys, and studies or generated electronically over the internet. The quality as well as quantity of data improves efficiency, classification and prediction rate in machine learning. Machine Learning models have proved their significance in various sectors like healthcare, transportation, e-commerce, and marketing. It can be used for prediction and detection of diseases like cancer, diabetes etc. in healthcare. </p>

</div>

<div class="col-md-4">

<h2>PERMISSIONED BLOCKCHAIN</h2>

<p>The blockchain design pattern was made famous by Bitcoin but Bitcoin is an application of blockchain technology. The blockchain technology has gone far beyond. In bitcoin transactions any node can join the network without any permission. To adopt the decentralized benefits of blockchain technology, business enterprises also needed certain level of privacy.

Multiple organizations can come to a common shared platform where they can exchange business information with one another in shared and secured manner. The decentralized database where transactions get recorded in append only shared ledger has many advantages in healthcare industry. Inmedical treatment, the complete history of patient is very important and value is added when same information is accessed by different parties. The permissioned blockchain network will have following components </p>

</div>

<div class="col-md-4">

<h2>MACHINE LEARNING IN HEALTHCARE</h2>

<p>Machine learning has been extensively used to benefit healthcare. Machine Learning can be used in identification of Treatment, give personalized suggestion to Patient, Outbreak Prediction etc.. User can get disease summary on the basis of symptoms entered [10].

Tokenization, removal of stop words and stemming are used as preprocessing. Many techniques have been done in this area which include SVM classifier, Naive Bayes and Decision Trees. The best result obtained has the accuracy percentage of 98.51%. The machine learning algorithm can also give lifestyle suggestion to Patient on the basis of current medical situation and medical history. </p>

</div>

</div>

{% endblock %}

##### Patient.html:

{% extends 'base.html' %}

{% block contents%}

<div class="jumbotron">

<div class="container">

<h1 class="display-3">Securing Data with Blockchain and AI</h1>

<p>The power of machine learning in understanding the patterns in data, analyzing and making decisions, has shown its importance in various sectors. Machine Learning requires reasonable amount of data to make accurate decisions. Data sharing and reliability of data is very crucial in machine learning in order to improve its accuracy. The decentralized database in Blockchain Technology emphasizes on data sharing. The consensus in Blockchain technology makes sure that data is legitimate and secured. The convergence of these two technologies can give highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology. This paper gives an overview of how combining these two technologies can help in healthcare sectors. </p>

<p><a class="btn btn-primary btn-lg" href="https://ieeexplore.ieee.org/document/8701230" role="button">Learn more &raquo;</a></p>

</div>

</div>

<div class="container">

<!-- Example row of columns -->

<div class="row">

<div class="col-md-4">

<h2>Patient Login</h2>

<p>

<form action="{% url 'patientlogincheck' %}" class="form-inline my-2 my-lg-0" method="POST">

{% csrf\_token %}

<input name="username" class="form-control mr-sm-2" type="text"

placeholder="User Login Id" aria-label="Search"><br/>

<input name="password" class="form-control Password" type="password" placeholder="Password" aria-label="Search"><br/>

<button class="btn btn-outline-success my-2 my-sm-0" type="submit">Login</button>

</form>

<center>

{% if messages %}

{% for message in messages %}

<font color='RED'> {{ message }}</font>

{% endfor %}

{% endif %}

</center>

<a class="nav-link" href="{% url 'patientregister' %}">Patients Register</a>

</p>

</div>

</div>

{% endblock %}

##### Doctor.html:

{% extends 'base.html' %}

{% block contents%}

<div class="jumbotron">

<div class="container">

<h1 class="display-3">Securing Data with Blockchain and AI</h1>

<p>The power of machine learning in understanding the patterns in data, analyzing and making decisions, has shown its importance in various sectors. Machine Learning requires reasonable amount of data to make accurate decisions. Data sharing and reliability of data is very crucial in machine learning in order to improve its accuracy. The decentralized database in Blockchain Technology emphasizes on data sharing. The consensus in Blockchain technology makes sure that data is legitimate and secured. The convergence of these two technologies can give highly accurate results in terms of machine learning with the security and reliability of Blockchain Technology. This paper gives an overview of how combining these two technologies can help in healthcare sectors. </p>

<p><a class="btn btn-primary btn-lg" href="https://ieeexplore.ieee.org/document/8701230" role="button">Learn more &raquo;</a></p>

</div>

</div>

<div class="container">

<!-- Example row of columns -->

<div class="row">

<div class="col-md-4">

<h2>Doctor Login</h2>

<p>

<form action="{% url 'doctorlogincheck' %}" class="form-inline my-2 my-lg-0" method="POST">

{% csrf\_token %}

<input name="loginid" class="form-control mr-sm-2" type="text" placeholder="User Login Id" aria-label="Search"><br/>

<input name="password" class="form-control Password" type="password" placeholder="Password" aria-label="Search"><br/>

<button class="btn btn-outline-success my-2 my-sm-0" type="submit">Login</button>

</form>

<center>

{% if messages %}

{% for message in messages %}

<font color='RED'> {{ message }}</font>

{% endfor %}

{% endif %}

</center>

<a class="nav-link" href="{% url 'doctorregistration' %}">Doctor Register</a>

</p>

</div>

</div>

{% endblock %}

##### Txn.html:

{% load static %}

<!doctype html>

<html lang="en">

<head>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

<meta name="description" content="">

<meta name="author" content="Mark Otto, Jacob Thornton, and Bootstrap contributors">

<meta name="generator" content="Jekyll v3.8.5">

<title>BlockChain Machine Learning · Bootstrap</title>

<link rel="canonical" href="https://getbootstrap.com/docs/4.3/examples/jumbotron/">

<!-- Bootstrap core CSS -->

<link href=" {% static 'css/bootstrap.min.css' %}" rel="stylesheet" >

<style>

.bd-placeholder-img { font-size: 1.125rem; text-anchor: middle;

-webkit-user-select: none;

-moz-user-select: none;

-ms-user-select: none; user-select: none;

}

@media (min-width: 768px) {

.bd-placeholder-img-lg { font-size: 3.5rem;

}

}

</style>

<!-- Custom styles for this template -->

<link href=" {% static 'css/jumbotron.css'%}" rel="stylesheet">

</head>

<body>

<nav class="navbar navbar-expand-md navbar-dark fixed-top bg-dark">

<a class="navbar-brand" href="#">Securing Data with Blockchain and AI</a>

<button class="navbar-toggler" type="button" data-toggle="collapse" data- target="#navbarsExampleDefault" aria-controls="navbarsExampleDefault" aria- expanded="false" aria-label="Toggle navigation">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbarsExampleDefault">

<ul class="navbar-nav mr-auto">

<li class="nav-item ">

<a class="nav-link" href="#"> Home </a>

</li>

<li class="nav-item">

<a class="nav-link" href="{% url 'trnxviewpurchase' %}">View Purchased</a>

</li>

<li class="nav-item">

<a class="nav-link" href="{% url 'logout' %}">Log out</a>

</li>

</ul>

<form class="form-inline my-2 my-lg-0">

<input class="form-control mr-sm-2" type="text" placeholder="Search" aria- label="Search">

<button class="btn btn-outline-success my-2 my-sm-0" type="submit">Search</button>

</form>

</div>

</nav>

<main role="main">

{% block contents %}

<!-- Main jumbotron for a primary marketing message or call to action -->

{% endblock %}

<hr>

</div> <!-- /container -->

</main>

<footer class="container">

<p>&copy; Company 2017-2019</p>

</footer>

<script src="{% static 'js/jquery-3.3.1.slim.min.js' %}" ></script>

<script>window.jQuery || document.write('<script src="/docs/4.3/assets/js/vendor/jquery- slim.min.js"><\/script>')</script><script src="{% static 'js/bootstrap.bundle.min.js' %}"

></script></body>

</html>

##### Admin.html :

{% extends 'base.html' %}

{% block contents%}

<div class="jumbotron">

<div class="container">

<h1 class="display-3">Securing Data with Blockchain and AI</h1>

<p><a class="btn btn-primary btn-lg" href="https://ieeexplore.ieee.org/document/8701230" role="button">Learn more &raquo;</a></p>

</div>

</div>

<div class="container">

<!-- Example row of columns -->

<div class="row">

<div class="col-md-4">

<h2>Admin Login</h2>

<p>

<form action="{% url 'adminloginaction' %}" class="form-inline my-2 my-lg-0" method="POST" >

{% csrf\_token %}

<input class="form-control mr-sm-2" type="text" name="username" placeholder="Admin Login Id" aria-label="Search"><br/>

<input class="form-control Password" type="password" name="password" placeholder="Password" aria-label="Search"><br/><br/><br/>

<button class="btn btn-outline-success my-2 my-sm-0" type="submit">Login</button><br/>

</form>

<center>

{% if messages %}

{% for message in messages %}

<font color='RED'> {{ message }}</font>

{% endfor %}

{% endif %}

</center>

</p>

</div>

</div>

{% endblock %}

### Sample Code :

##### Manage.py:

#!/usr/bin/env python import os

import sys

if name == ' main ':

os.environ.setdefault('DJANGO\_SETTINGS\_MODULE', 'converginblockchain.settings') try:

from django.core.management import execute\_from\_command\_line except ImportError as exc:

raise ImportError(

"Couldn't import Django. Are you sure it's installed and "

"available on your PYTHONPATH environment variable? Did you " "forget to activate a virtual environment?"

) from exc execute\_from\_command\_line(sys.argv)

##### Testme.py :

# Untested! class Disease:

def init (self, name, symptoms): self.name = name self.symptoms = symptoms

known\_diseases = [

Disease('cold', set("sore throat|runny nose|congestion|cough|aches".split("|"))), Disease('flu', set("fever|headache|muscle aches|returning fever".split("|"))), Disease('ebola', set("tiredness|death|bruising over 90% of body|black blood".split("|"))),

Disease('spondylosis', set("Tingling|numbness|weakness|Abnormal reflexes|muscle spasms".split("|"))),

Disease('alcohol misuse', set("antisocial behaviour|impulsivity|self-harm|loneliness".split("|"))),

Disease('stroke', set("Numbness|arm|Confusion|Difficulty speaking|difficulty walking|slurred speech".split("|"))),

Disease('Lower respiratory infections', set("phlegm|fever|difficulty breathing|a blue tint to the skin|chest pain|wheezing".split("|"))),

Disease('pulmonary', set("dyspnea|Fatigue|fainting spells|Chest pressure|Swelling".split("|"))),

Disease('bronchus', set("Cough with blood|Wheezing|Shortness of breath|Chest pain|Flushing".split("|"))),

Disease('Diabetes', set("thirst and hunger|urination|Weight loss or gain|Fatigue|Nausea|Blurred vision".split("|"))),

Disease('Alzheimer', set("Memory loss|Vision loss|Misplacing items|Difficulty making decisions|meaningless repetition ".split("|"))),

Disease('Dehydration', set("vomiting|sweating|Individuals |dry mouth|lethargy|dizziness".split("|"))),

Disease('Tuberculosis', set("Coughing|Chest pain|weight loss|Fatigue|Fever|Night sweats|Chills".split("|"))),

Disease('Cirrhosis', set("jaundice|Weakness|Loss of appetite|Itching|Easy bruising|dark urine".split("|"))),

Disease('Plague', set("diarrhoea|nausea|nausea|malaise|delirium|shortness of breath|tender lymph node".split("|")))

]

# note: for Python 2, use "raw\_input" instead of input

symptoms = input("Please enter symptoms separated by commas: ") symptoms = symptoms.lower()

symptoms = symptoms.split(",") possible = []

for symptom in symptoms:

for disease in known\_diseases:

if symptom in disease.symptoms: possible.append(disease.name)

if possible:

print("You may have these diseases:") print(\*possible)

else:

print("Good news! You're going to have a disease named after you!")

### Execution Flow :

1. The user arrives at the website’s homepage.
2. They are presented with two options: sign up or sign in.
3. If the user chooses to sign up, they are directed to a new user registration form.
4. On the sign-up form, the user enters their credentials including their username and password.
5. The user creates an account by entering their details.
6. After completing the form, the user’s information is validated.
7. Once the user’s details are confirmed, their information is saved to a database.
8. The user is then directed to the website’s homepage.
9. The user can now sign out if they wish to do so.
   1. **Testing :**

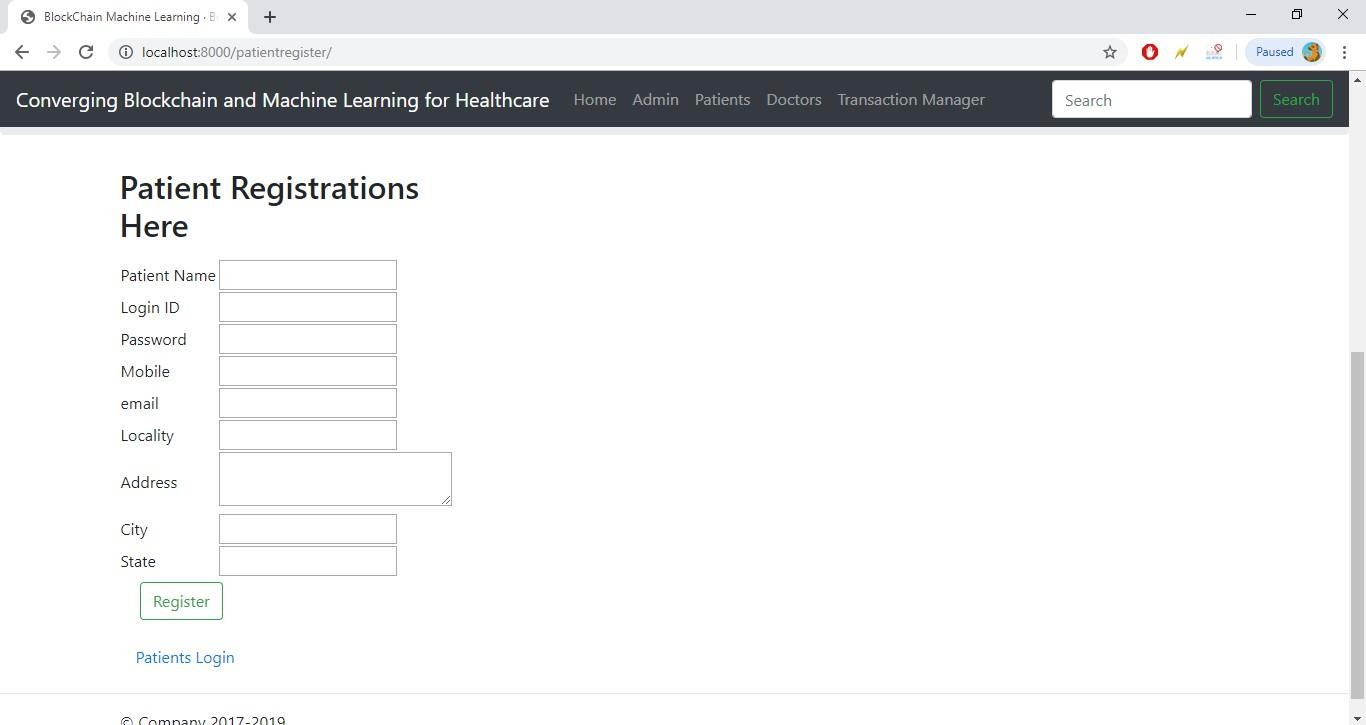
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.no | Test Case | Excepted Result | Result | Remarks (IF fails) |
| 1. | DOCTOR REGISTERED | If DOCTOR  registration successfully. | Pass | If DOCTOR is not registered. |
| 2. | DOCTOR LOGIN | If DOCTOR name and password is  correct then it will getting valid page. | Pass | If DOCTOR name or password is not correct. |
| 3. | PATIENT REGISTRATION | If PATIENT is  registered successfully. | Pass | If PATIENT is not registered. |
| 4. | PATIENT LOGIN | PATIENT name and password is correct then getting valid page. | Pass | If PATIENT name or password is wrong. |
| 5. | ADMIN | DOCTOR rights and PATIENT  rights will be accepted here. | Pass | If DOCTOR and PATIENT are not registered. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | PATIENT UPLOAD DATA | Choose or select PATIENT DATA  and upload in  ADMIN. | Pass | If PATIENT is not select or upload the DATA. |
| 7. | VIEW DOCTOR UPLOADED DATAS | DOCTOR uploaded PATIENT DATA  details are available here | Pass | If PATIENT DATA  is not uploaded in ADMIN. |
| 8. | PATIENT VIEW DOCTOR DATAS | DOCTOR uploaded PATIENT DATA  details are available here and we can view PATIENT DATA | Pass | If PATIENT DATA  is not uploaded in ADMIN. |
| 9. | PATIENT INBOX | All the details about PATIENT DATA | Pass | If PATIENT DATA  is not available. |
| 10. | TRANSACTION MANAGER | Receive payments from patients, calculate ledger amount details, last transaction amount  requested PATIENT DATA | Pass | If DATA is not available. |

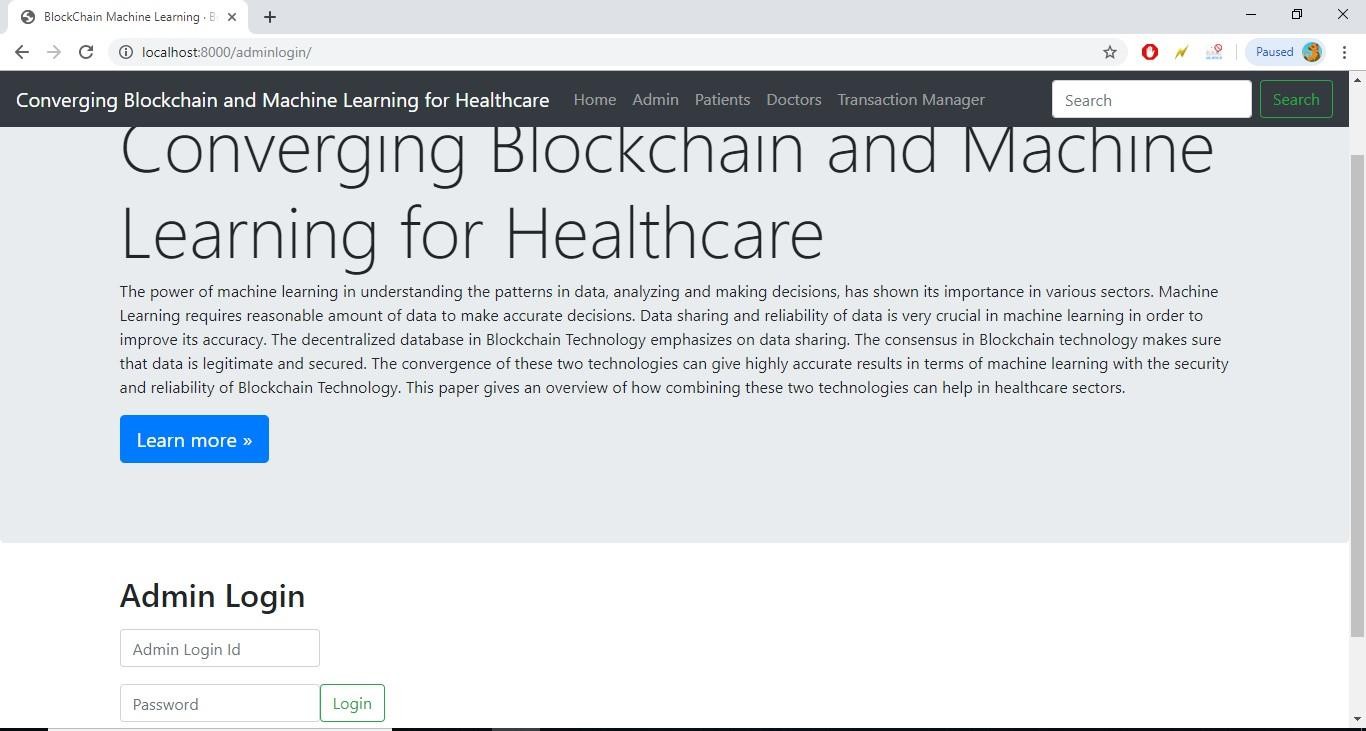
# CHAPTER - 5

## RESULTS

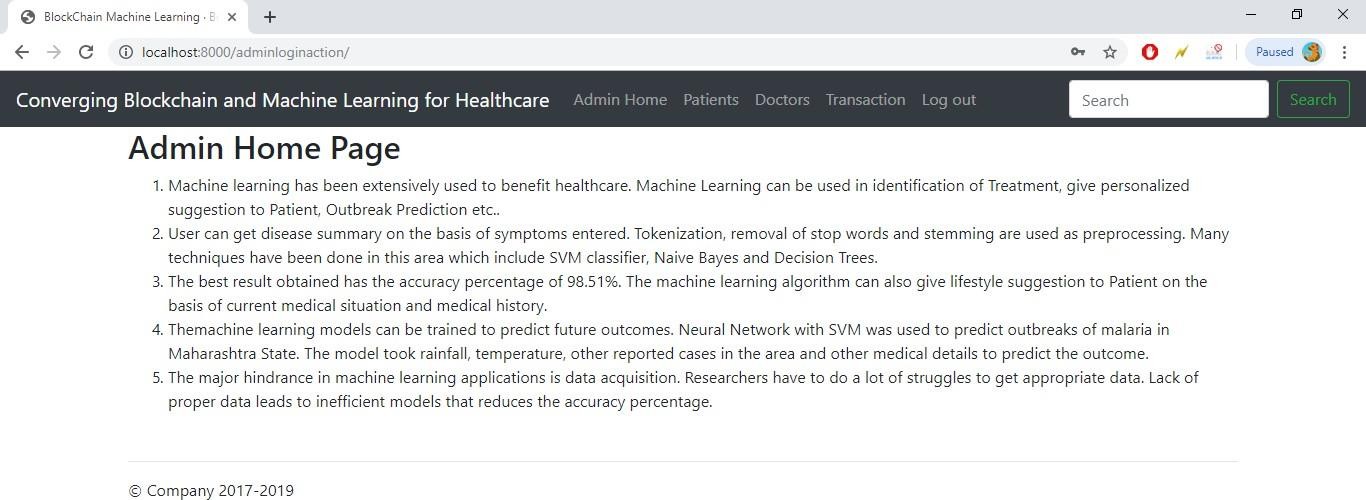
### Patient Registration:



**Admin Login:**



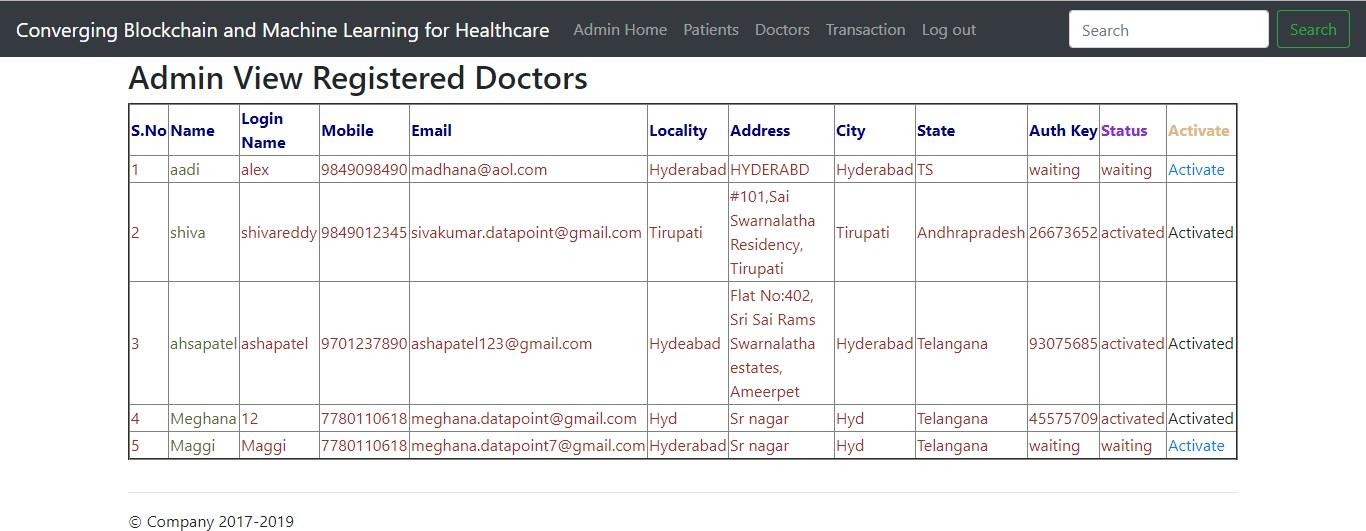
### Admin Home:



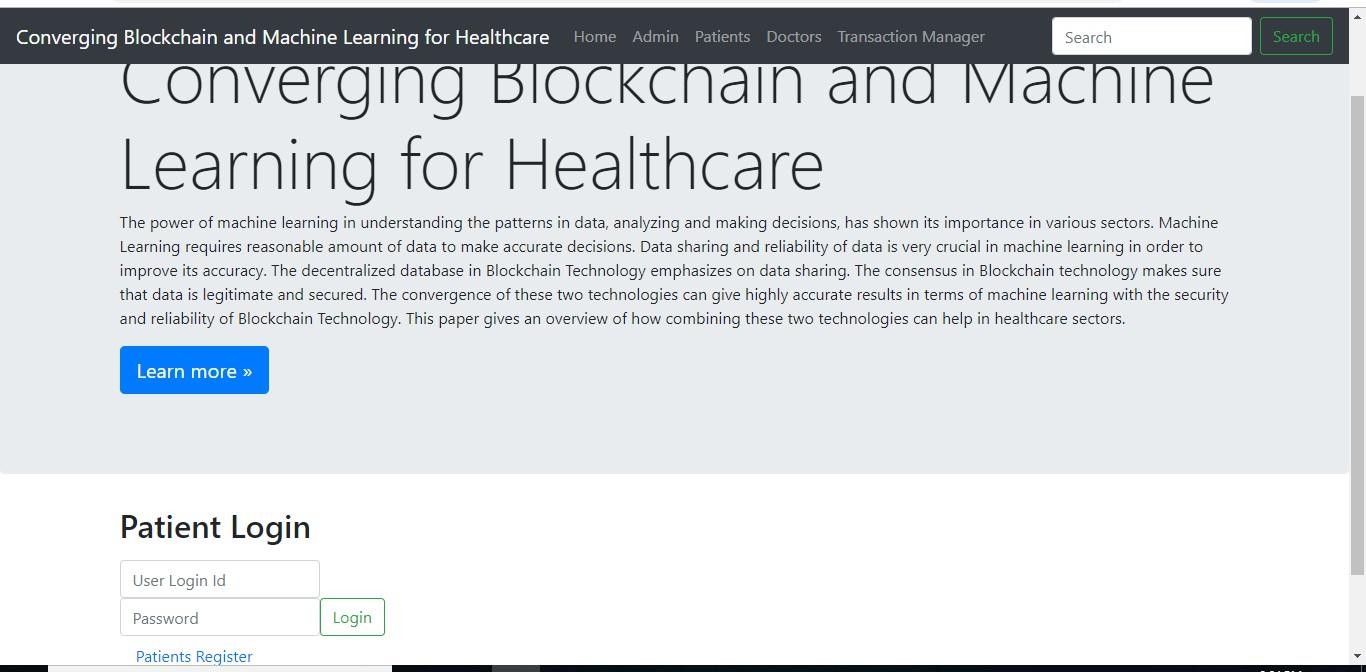
**Patient Activation:**



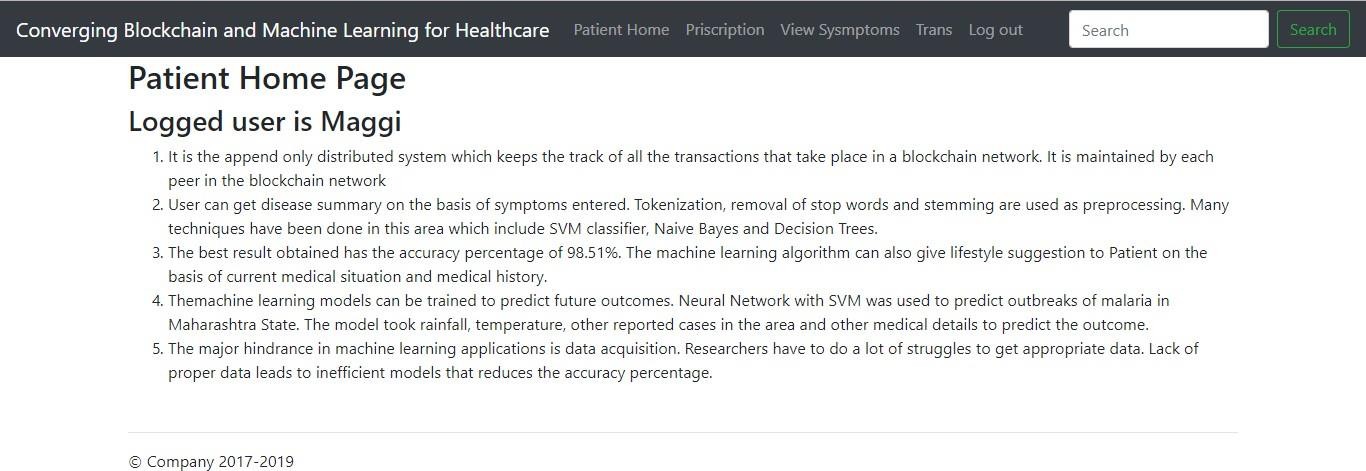
### Doctor Activation:



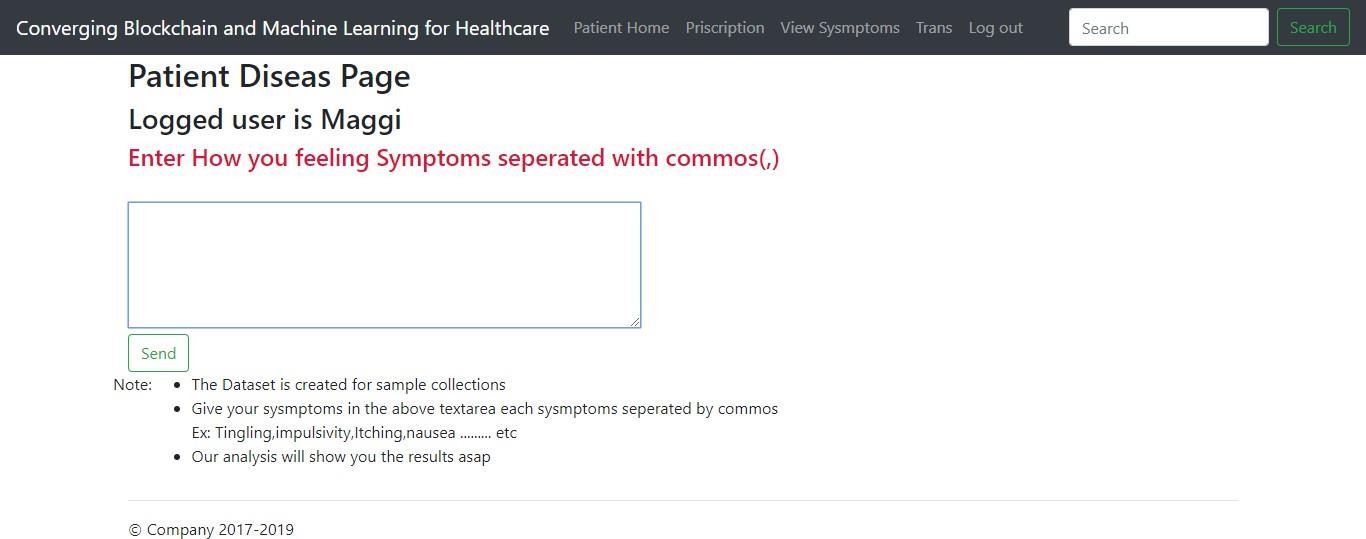
**Patient Login:**



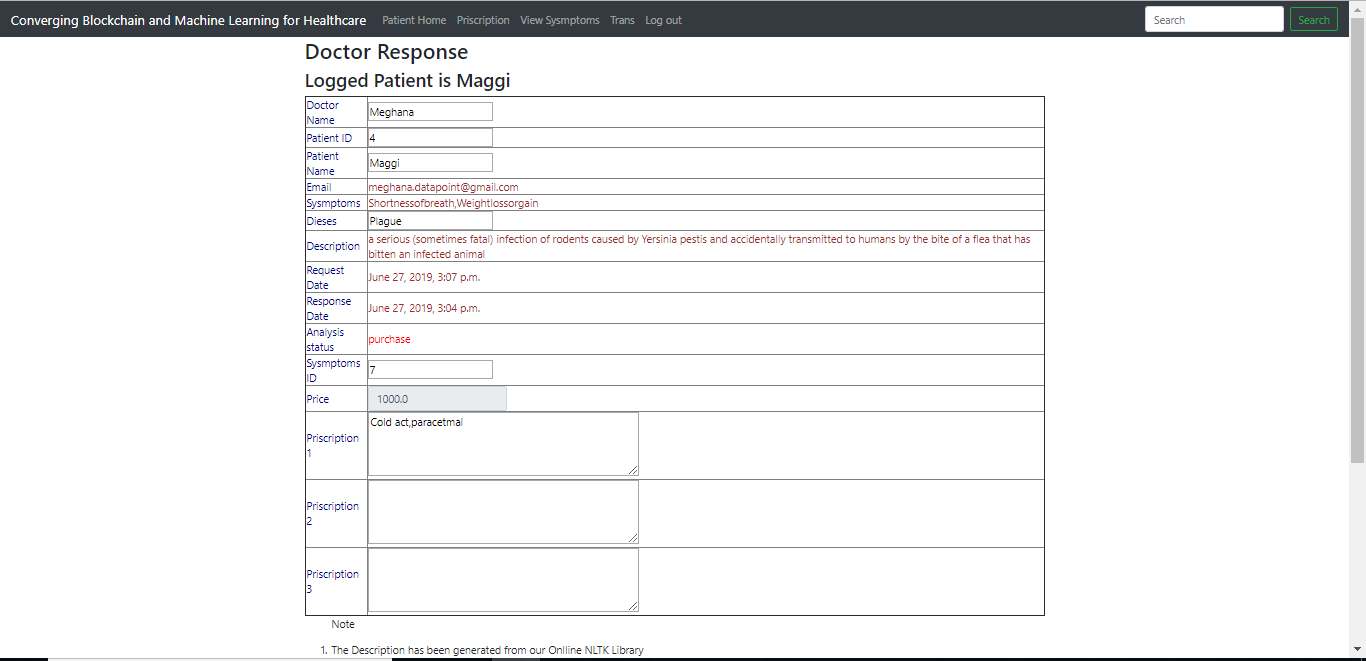
### Patient Home Page:



**Prescription:**



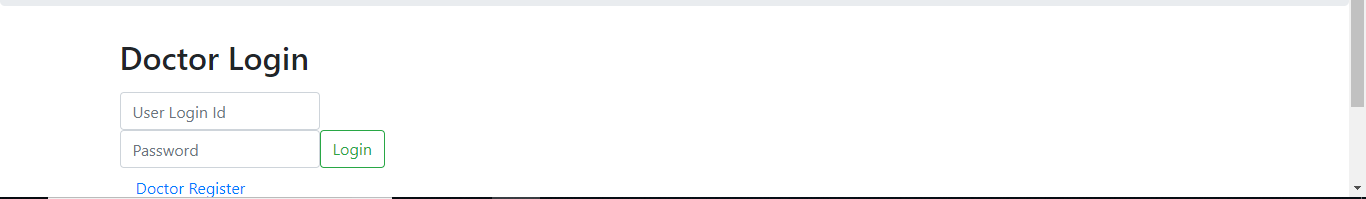
### Doctor Response:



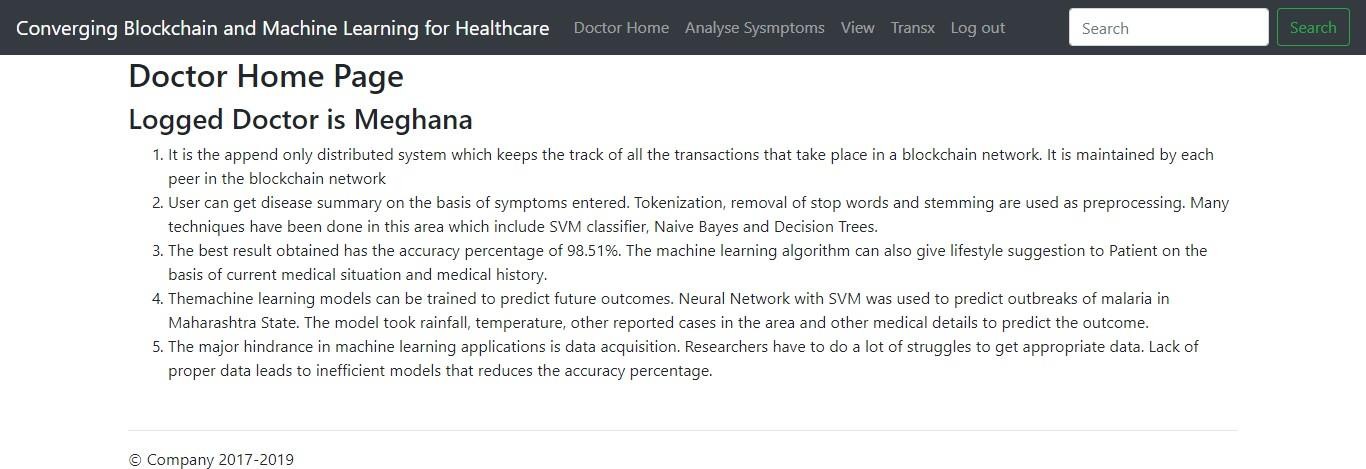
**Patient Transactions:**



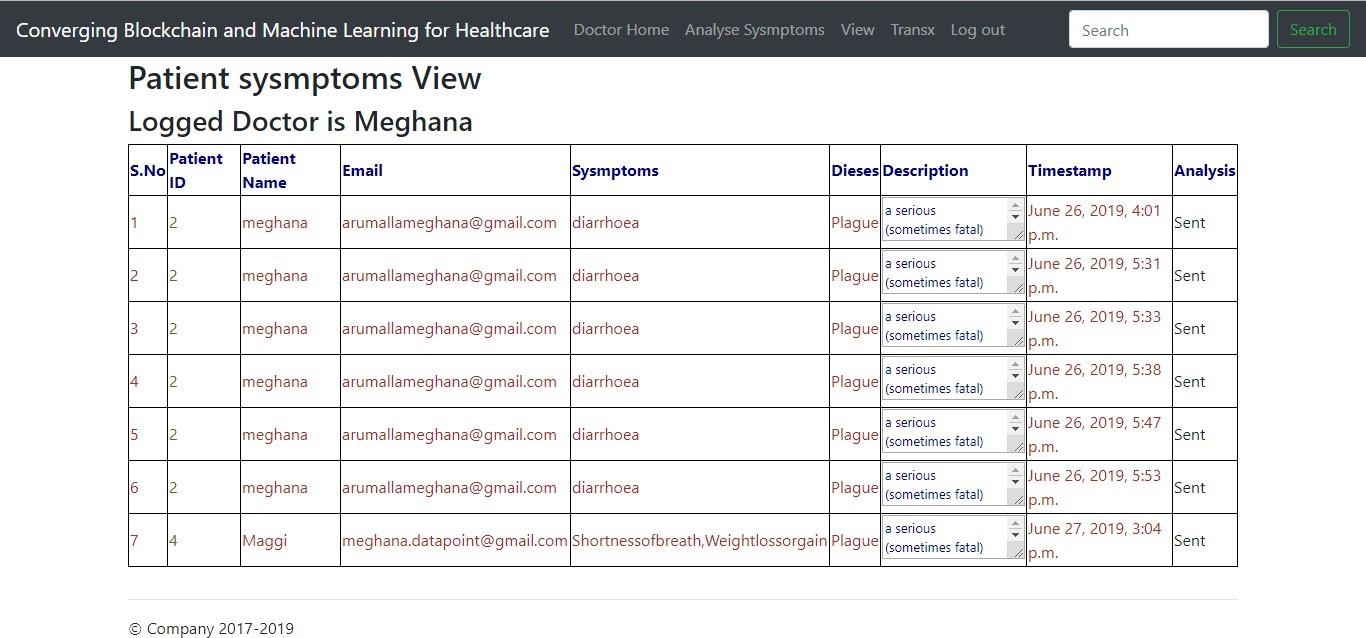
### Doctor Login:



**Doctor Home Page:**



### Analyze Symptoms:



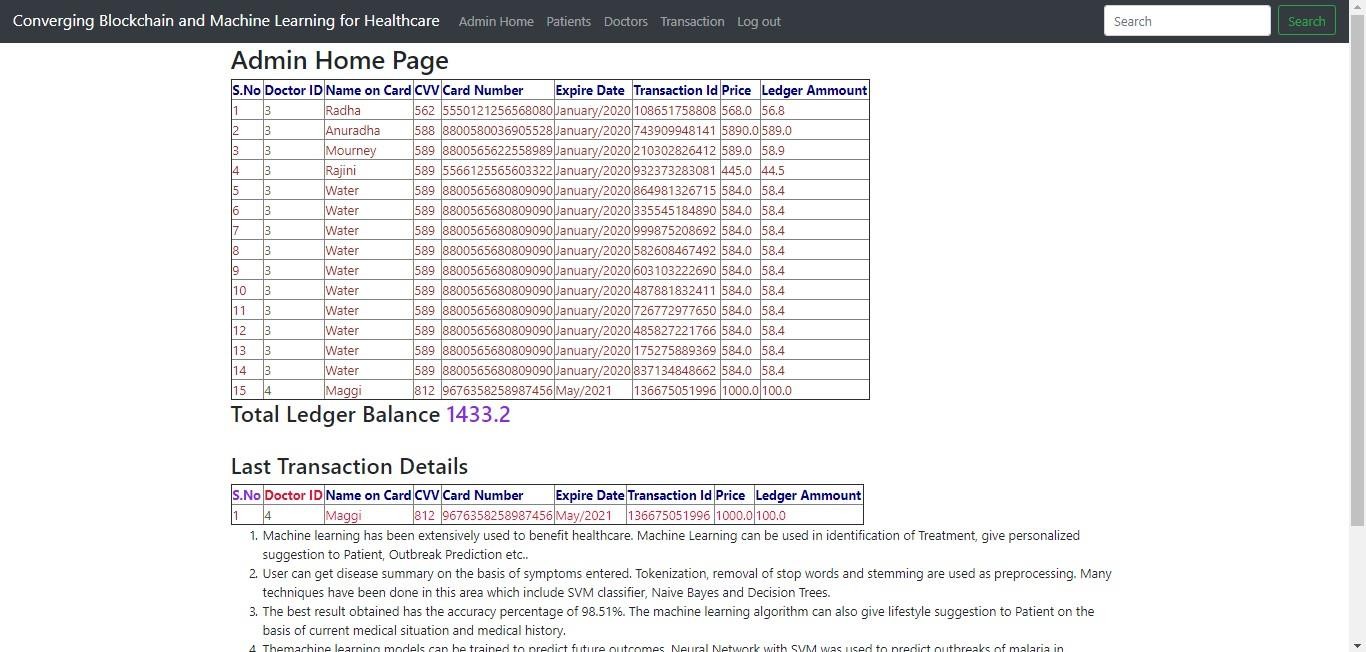
**View :**



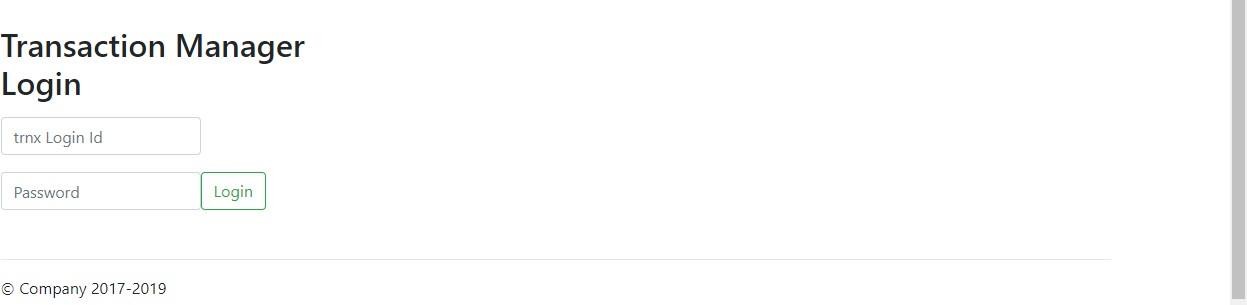
### Transactions:

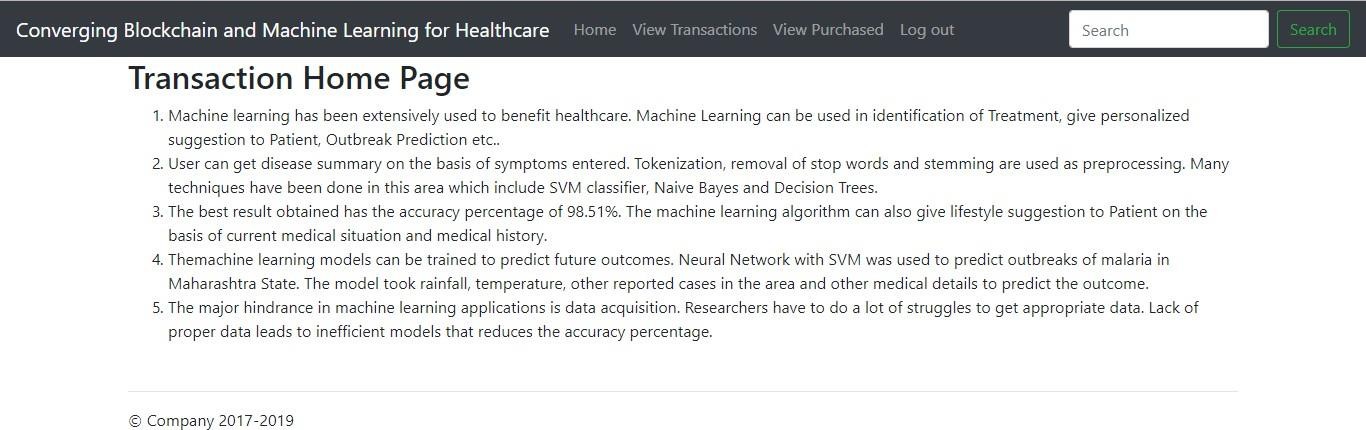


**Admin View Transactions:**

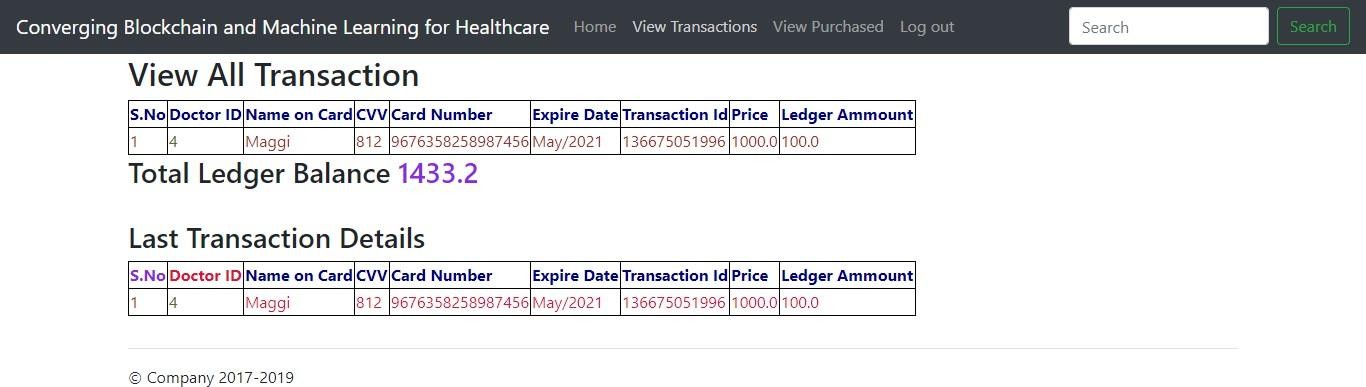


### Transaction Manager:





**View Transactions:**



### View Purchased:



* 1. **CONCLUSON:**

# CAHPTER – 6

## Conclusions & Future Scope

Blockchain Technology gives great number of opportunities if utilized properly and is seen beyond bitcoin. With blockchain, the dominance of central authority could be eliminated and so the commission. Machine Learning models can directly fed with data (however the rights will be managed by central authority). This will increase the accuracy and efficiency of machine learning models and so their usability. Healthcare industry directly correlates with the life of a person. This could help patients as well as doctors. In terms of future scope, the practical implementation of this model will be there. This model can be further extended for Inventory or prevent fraud.

### Future Scope :

##### Advanced AI Chatbot Capabilities

* + **Natural Language Processing (NLP)**: Improve the chatbot to handle more complex interactions using NLP models like GPT or BERT. This would allow it to understand and respond to users' queries more accurately.
  + **Integration with Salesforce Data**: Make the chatbot capable of retrieving and updating Salesforce records (e.g., student details, course registrations, appointment scheduling) directly through user interaction.
  + **Multilingual Support**: Enable the chatbot to communicate in multiple languages to cater to a diverse user base.

##### Personalized Student and Consultant Portals

* + **User Dashboard**: Develop personalized dashboards for students, consultants, and administrators. This could include upcoming appointments, course progress, or recent interactions.
  + **Recommendations**: Implement AI-driven recommendations for students on courses, consultants, and resources based on their history and preferences.
  + **Progress Tracking**: Allow students to track their academic progress, attendance, and grades through the platform.

##### Insurance Module Enhancements

* + **Integration with Insurance Providers**: Connect the insurance module to external APIs of insurance providers to automate the process of policy recommendations and claims.
  + **AI-Powered Claims Processing**: Use AI to process insurance claims and validate documents automatically, reducing manual work and errors.
  + **User Notifications**: Set up automated notifications for policy renewals, premium due dates, and claims status updates.

##### Scalability and Cloud Integration

* + **Cloud Deployment**: Migrate the application to a cloud platform (like AWS or Azure) for better scalability, availability, and performance.
  + **Microservices Architecture**: Refactor the project into microservices for scalability and maintainability. This way, each module (chatbot, insurance, student management) can be independently scaled.
  + **Salesforce Integration Enhancements**: Deepen integration with Salesforce by leveraging its capabilities like Einstein AI for predictive analytics, automated workflows, and dashboards.

##### Data Analytics and Reporting

* + **Data Visualization**: Add data visualization tools for reporting student performance, consultant effectiveness, or insurance claim trends.
  + **Predictive Analytics**: Use AI to predict student drop-out rates, consultant performance, or insurance fraud detection.
  + **KPI Dashboards**: Develop dashboards for admins to track key performance indicators (KPIs) related to appointments, course registrations, and insurance policies.

##### Mobile App Development

* + **Mobile App**: Develop a mobile version of the application to allow students, consultants, and administrators to access features on the go.
  + **Push Notifications**: Integrate push notifications for reminders (appointments, courses, insurance renewals, etc.).

##### Security and Compliance

* + **Data Privacy and Compliance**: Ensure compliance with data protection regulations like GDPR and HIPAA, especially if handling sensitive student or insurance data.
  + **Two-Factor Authentication (2FA)**: Add 2FA for secure login to protect sensitive student and insurance data.
  + **Audit Logs**: Implement audit logs to track user actions and changes made to records, enhancing security and accountability.

## REFERENCES

1. Universal Health Coverage, World Health Organization, Geneva, Switzerland, 2022.
2. V. P. Aggelidis and P. D. Chatzoglou, ‘‘Using a modified technology acceptance model in hospitals,’’ Int. J. Med. Informat., vol. 78, no. 2, pp. 115–126, 2009.
3. A. Roehrs, C. A. da Costa, and R. da Rosa Righi, ‘‘OmniPHR: A distributed architecture model to integrate personal health records,’’ J. Biomed. Inform., vol. 71, pp. 70–81, Jul. 2017.
4. N. Spence, M. N. Bhardwaj, and D. Paul, ‘‘Ransomware in healthcare facilities: A harbinger of the future?’’ Perspect. Health Inf. Manage., vol. 10, pp. 1–22, Jul. 2018.
5. N. Thamer and R. Alubady, ‘‘A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,’’ in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), Apr. 2021, pp. 210–216.
6. T. Benson, Principles of Health Interoperability HL7 and SNOMED, 2nd ed. New York, NY, USA: Springer, 2012, pp. 1–316.
7. L. Coventry and D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 48–52, Jul. 2018.
8. S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decentralized Bus. Rev., vol. 5, p. 21260, Oct. 2008.
9. C. Burniske, E. Vaughn, J. Shelton, and A. Cahana, How Blockchain Technology Can Enhance EHR Operability. St. Petersburg, FL, USA: Ark Invest, 2016.
10. A. M.-H. Kuo, ‘‘Opportunities and challenges of cloud computing to improve health care services,’’ J. Med. Internet Res., vol. 13, no. 3, p. e67, Sep. 2011.
11. L. Bass, P. Clements, and R. Kazman, Software Architecture in Practice. London, U.K.: Pearson, 2012.
12. B. Kitchenham and P. Brereton, ‘‘A systematic review of systematic review process research in software engineering,’’ Inf. Softw. Technol., vol. 55, no. 12, pp. 2049–2075, 2013.
13. K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, ‘‘Systematic mapping studies in software engineering,’’ in Proc. 12th Int. Conf. Eval. Assessment Softw. Eng., 2008, pp. 68–77.
14. I. Kurtev, J. Bézivin, F. Jouault, and P. Valduriez, ‘‘Model-based DSL frameworks,’’ in Proc. Companion 21st ACM SIGPLAN Symp. Object-Oriented Program. Syst., Lang., Appl., 2006, pp. 602–616.
15. M. Brambilla, J. Cabot, M. Wimmer, and L. Baresi, Model-Driven Software Engineering in Practice, 2nd ed. San Rafael, CA, USA: Morgan & Claypool, 2017.
16. C. Agbo, Q. Mahmoud, and J. Eklund, ‘‘Blockchain technology in healthcare: A systematic review,’’ Healthcare, vol. 7, no. 2, p. 56, 2019.
17. E. Dulce and J. Hurtado, ‘‘The role of the blockchain technology in the elderly care solutions: A systematic mapping study,’’ in Proc. Int. Workshop Gerontechnol. Cham, Switzerland: Springer, 2021, pp. 23–34.
18. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ‘‘MedRec: Using blockchain for medical data access and permission management,’’ in Proc. 2nd Int. Conf. Open Big Data (OBD), Aug. 2016, pp. 25–30.
19. H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, ‘‘Blockchain technology in the healthcare industry: Trends and opportunities,’’ J. Ind. Inf. Integr., vol. 22, Jun. 2021, Art. no. 100217.
20. A. I. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, ‘‘Combination of hiding and encryption for data security,’’ Int. J. Interact. Mobile Technol., vol. 14, pp. 34–47, Jan. 2020.
21. L. Ismail and H. Materwala, ‘‘BlockHR: A blockchain-based framework for health records management,’’ in Proc. 12th Int. Conf. Comput. Modeling Simulation, Jun. 2020, pp. 164– 168.
22. V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, ‘‘A hierarchical multi blockchain for fine grained access to medical data,’’ IEEE Access, vol. 8, pp. 134393– 134412, 2020.
23. O. O’Donoghue, A. A. Vazirani, D. Brindley, and E. Meinert, ‘‘Design choices and trade- offs in health care blockchain implementations: Systematic review,’’ J. Med. Internet Res., vol. 21, no. 5, May 2019, Art. no. e12426.
24. A. R. Bartolomé, J. M. Moral Ferrer, D. Tapscott, A. Tapscott, A. I. D. Santos, V. Koulaidis, J. P. Schmidt, M. Sharples, J. Domingue, and N. Smolenski, ‘‘Blockchain en educación: Cadenas rompiendo moldes,’’ Learn., Media Social Interact., vol. 3, no. 2, pp. 95–97, 2018.
25. J. Martinez-Gil, M. Pichler, T. Beranic, L. Brezocnik, M. Turkanovic, G. Lentini, F. Polettini, A. Lué, A. C. Vitale, G. Doukhan, and C. Belet, ‘‘Framework for assessing the smartness maturity level of villages,’’ in Proc. Eur. Conf. Adv. Databases Inf. Syst. Cham, Switzerland: Springer, 2019, pp. 501–512.

**Healthcare Consultancy using Blockchain**

Dr.G.Vasavi Associate professor

Department of Cyber security Malla Reddy University, Hyderabad, Telangana, India

K. Akhil Department of Cybersecurity

Malla Reddy University, Hyderabad, Telangana, India

D. Jathin Department of Cybersecurity

Malla Reddy University, Hyderabad, Telangana, India

Mohamad Reyaz Department of Cybersecurity Malla Reddy University, Hyderabad, Telangana, India

**Descriptions: The combination of machine learning and blockchain technology offers transformative opportunities in a variety of areas of great importance in medicine, promising to revolutionize healthcare, clinical research and data management. The platform provides solutions to critical problems such as increasing privacy and confidentiality through secure storage and preventive storage, while allowing machine learning algorithms to gain insights from patient data without compromising privacy. Patient empowerment is facilitated through the use of health information management systems that enable personalized medicine through machine-assisted analysis of individual patient records.**

**REFERENCES: Machine Learning, Data Analytics, Blockchain Technology, Information Security, Healthcare, Healthcare Information Management, Interoperability.**

1. INTRODUCTION

The convergence of machine learning and blockchain technology represents a pivotal frontier in addressing critical challenges across diverse sectors, particularly within the healthcare domain. Both technologies individually have demonstrated profound impacts on data analysis, decision- making, and security. Machine learning, with its capacity to discern intricate patterns within data, has become indispensable across various industries, including healthcare, transportation, e-commerce, and marketing. Meanwhile, blockchain technology, originating from the groundbreaking Bitcoin cryptocurrency, has garnered recognition for its decentralized database architecture, ensuring data integrity and security through cryptographic mechanisms and consensus protocols. In healthcare, where data reliability and privacy are paramount, the fusion of these two technologies holds immense potential to revolutionize patient care, medical research, and data management practices.

However, despite the advancements, challenges persist, particularly concerning data acquisition, model efficiency, and scalability. This paper delves into exploring the intersection of machine learning and blockchain technology within the healthcare sector, aiming to elucidate the transformative applications, benefits, and challenges encountered in leveraging this synergistic approach to enhance healthcare outcomes and drive innovation**.**

1. LITERATURE REVIEW

[3] Advances in information and communications technology (ICT) have brought many benefits to healthcare, especially in the digital storage of patient health records. However, achieving a common understanding of patients' health histories remains challenging because health information is often distributed across different healthcare settings. Additionally, there are many standards for these documents, some open, some proprietary. Medical records are typically stored in databases within healthcare organizations and are rarely accessible from outside. This issue is especially true when patient information is stored by healthcare providers, known as EHRs (Electronic Health Records). In the case of PHRs (Private Health Records), where by definition patients can manage their own medical records, patients generally have no control over the information stored in healthcare providers' databases. Therefore, we address two important questions regarding PHR: first, how patients can get a single view of their health in a granular way, and second, how healthcare providers can get the most up-to-date information about their patients. Even if the changes took place elsewhere. To solve these problems, this initiative offers a model called OmniPHR, a proposed model for integrating PHRs that patients and healthcare providers can use. The scientific contribution is to provide an architectural model to support a distributed PHR that allows patients to track their health history in a single way from any device, from anywhere. Healthcare

providers can also ensure that patient data is linked to healthcare organizations. An overview of the health recordkeeping model's approach is provided in a database supporting a single-view PHR with a simple and easy-to-use interface. [4] Cybercriminals are beginning to target the healthcare industry using ransomware, malware, and any connected device or hard drive (). Once discovered, cybercriminals demand a ransom before releasing the device's code. Without adequate disaster recovery and recovery plans, many companies are forced to pay ransom. We have recently examined the prevalence of life- threatening diseases, the burden of risks and costs associated with these diseases, and ways to reduce the risk. The methodology of this study was literature review. The research was limited to sources published in English between 2005 and 2017. 74 of the 118 sources found were used in the results section. We also conducted two semi- structured interviews, one with a health law expert and the other with an IT officer at a local teaching hospital who was also a health technology expert. The financial costs of restoring business operations following ransomware attacks on healthcare companies are significant and growing in both size and scope. Other consequences include loss of future business and damage to reputation. Research has shown that the best plan of action is to have a good business continuity and contingency plan, as well as being vigilant in storing adequate data to prevent potential attacks and educating employees on ransomware sources. [5] Health is one of the sectors most affected by cyber-attacks. As cybercriminals continue to expand and offer more digital healthcare services, they seek to exploit the vulnerabilities and uncertainties that come with these changes. Due to technological advancement, many serious threats such as Ransomware are threatened. Ransomware is an attack that targets businesses and home users, and its number has recently increased to due to its prolific results. The conflict has evolved significantly in recent years. The research provides a comprehensive survey of ransomware attacks and solutions to these attacks. The main purpose of this study is to solve many problems in medicine, such as Blockchain technology, software that explains network technology, Machine Learning and other tools used to prevent Ransomware, to apply strategies to solve Ransomware attacks and to reveal what researchers will do. We are faced with. Onto explore ways to deal with ransomware attacks in healthcare systems. In addition, the research provides scientific benefits to researchers working in the field of information security, healthcare institutions and security companies. [7] Electronic health technology dominates the world and offers many opportunities to increase clinical productivity and transform service delivery. But there are growing concerns about the security of health information and devices. The addition of to standard computer networks

has exposed medical devices to new security challenges. Healthcare is an attractive target for cybercrime for two main reasons: it is a rich source of valuable information and it is difficult to defend. Cybersecurity breaches include the theft of health information and ransomware attacks on hospitals, but can also include attacks on compromised medical equipment. Exceeding this can reduce the patient's confidence, harm their health and threaten people's lives. After all, cybersecurity is critical to patient safety but has historically been weak. New rules and regulations are in place to ease the transition. This requires cybersecurity to be an integral part of patient safety. Changes in human behaviour, technology and processes are needed as a comprehensive solution. [8] Peer-to-peer electronic money allows online payments to be sent directly from one party to another without the intervention of financial institutions. Digital signatures provide part of the solution, but significant benefits are lost if a trusted third party is still needed to prevent double spending. We propose a solution to the dual-use problem using peer-to-peer networking. Real-time network processing by accelerating a continuous chain of hash-based workflows, creating an immutable record without shortening the decision-making process. A longer chain serves not only as evidence of the sequence, but also as evidence that it comes from a larger amount of CPU power. As long as the majority of CPU power is controlled by nodes that do not cooperate in the network attack, it will create a long chain of remote attackers. The network itself requires very little configuration. Messages are broadcast on a positive basis and nodes can move and re-enter the network at will, allowing long-distance viewing such as event tokens in transit. [10] Cloud computing is a new way of delivering tools and services. Many leaders and experts believe it could improve healthcare, benefit health research, and change the face of health information technology. However, like all innovations, cloud computing needs to be carefully evaluated before adoption. This article discusses the concept and its place in medicine, using four factors (governance, technology, security, and law) to explore the opportunities and challenges of this computational approach. Planning can be used by a healthcare organization to determine its vision, strategy, and resource allocation when deciding to move from traditional healthcare to cloud-based healthcare. [14] More than five years ago, OMG proposed the Model Driven Architecture (MDA™) to address the distinction between dependent and independent processes in information systems. Since then, the original concept of MDA has evolved and Model Driven Engineering (MDE) has been developed to solve various problems in software or information architecture. MDE is more general than OMDA's recommended standards and practices for MDA. In MDE, the concept model includes not only the OMG

model but also XML documents, Java programs, RDBMS data, etc. It also represents many other structures such as Today we are looking at a new step in evolution. The connection between MDE and DSL (Diagnostic Language) engineering is clear. Since MDE is specific to MDA, the DSL architecture can be viewed as a generalization of MDE. One of the aims of this article is to investigate the potential for significant change in technological performance. To take the discussion to a practical level, we provide a list of common problems that can be solved with classic (displayed on objects, etc.), MDE or DSL technology. The answers to these questions will depend on the available forums (EMF, AMMA, GME, etc.). This article presents a robust, process- based approach that allows the use and creation of a variety of DSLs that can help solve complex problems efficiently.

1. METHODOLOGY

The methodology for exploring the integration of machine learning and blockchain technology in healthcare involves a multi-faceted approach aimed at understanding the synergistic potential and addressing the challenges inherent in this convergence. Firstly, comprehensive literature review and analysis are conducted to understand the current state-of-the-art in both machine learning and

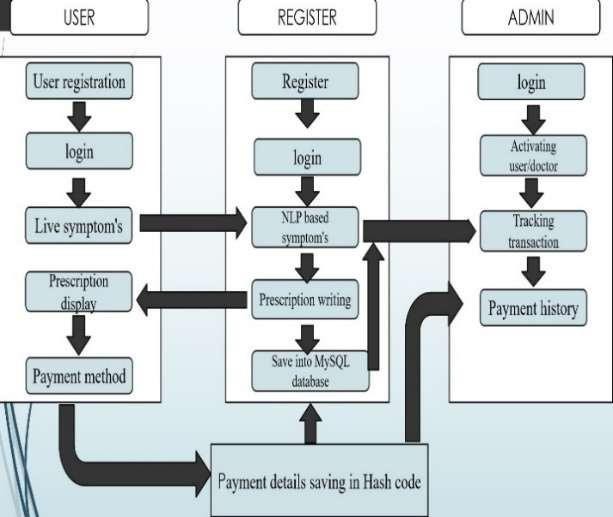


Fig1: System Architecture

blockchain technology, particularly within the healthcare sector. This involves examining relevant research papers, academic journals, industry reports, and case studies to identify key trends, applications, and challenges. Subsequently, empirical studies and experiments are conducted to evaluate the efficacy and feasibility of integrating machine learning algorithms with blockchain technology for various healthcare applications. This includes designing and implementing proof-of-concept projects or prototypes to demonstrate the practical utility and benefits of this convergence.

Additionally, qualitative research methods such as interviews and surveys may be employed to gather insights from healthcare professionals, researchers, and stakeholders regarding their perspectives, requirements, and concerns related to adopting machine learning and blockchain solutions in healthcare. Furthermore, collaboration with industry partners or healthcare institutions may be established to access real-world datasets and validate the performance of machine learning models integrated with blockchain technology. Overall, this methodology combines theoretical analysis, empirical studies, and stakeholder engagement to provide a holistic understanding of the integration of machine learning and blockchain technology in healthcare and to identify pathways for its successful implementation and adoption.

*A. Benefits*

The integration of machine learning with blockchain technology offers numerous benefits to the healthcare sector. Firstly, machine learning algorithms can be leveraged for the identification of treatments and personalized suggestions to patients based on their medical history and current condition. By analysing vast amounts of patient data, machine learning models can provide tailored recommendations that improve treatment efficacy and patient outcomes.

Additionally, machine learning techniques such as SVM classifier, Naive Bayes, and Decision Trees enable accurate disease prediction and outbreak detection, with results showing impressive accuracy rates such as 98.51%. The consensus mechanism in blockchain technology further enhances data integrity and trustworthiness, thereby providing a robust foundation for machine learning applications in healthcare. Overall, the convergence of machine learning and blockchain technology holds tremendous potential to revolutionize healthcare by delivering highly accurate and secure solutions that improve practices.

**System framework**

System level with the advancement of Machine Learning and Machine Learning tools becoming popular, people are starting to get used to the new era. Blocks are marked with the previous hash and timestamp and added to the current block. people (patients) can submit their information and share this information with the doctors (physicians) they want to deal with. Doctors can be trained to predict outcomes. data files are simple, doctors are allowed to select

patient data and individuals (patients). Clearly, disclosure of personal information is a critical issue managed by the data controller. We provide an overview of how combining these two technologies can help in the healthcare industry. (1) Doctor (2) Patient (3) Operations Manager (4) Block (5) Machine Learning.

1. IMPLEMENTATION
2. **Blockchain**: Blockchain technology ensures secure and transparent transactions in the healthcare sector. It provides a decentralized and immutable ledger where data transactions, such as sharing medical records between patients and doctors, can be recorded securely. The use of cryptographic hashing and consensus mechanisms ensures data integrity and prevents unauthorized access or tampering.
3. **Machine Learning**: Machine learning algorithms play a crucial role in healthcare by analysing large datasets to make predictions, identify patterns, and provide personalized recommendations. In this framework, machine learning models can be trained on medical data stored on the blockchain to predict outbreaks, suggest treatments, and offer lifestyle recommendations to patients based on their medical history and symptoms.
4. **Doctors**: Doctors benefit from machine learning models that can predict outbreaks, suggest treatments, and provide insights into patient health based on data stored on the blockchain. They can access patient records securely, make informed decisions, and offer personalized care. Additionally, machine learning models can assist doctors in analysing medical tests, predicting equipment maintenance needs, and offering lifestyle recommendations to patients.
5. **Patients**: Patients can securely upload and share their medical records with doctors of their choice using blockchain technology. Machine learning models can analyse patient data to provide personalized recommendations, lifestyle advice, and clinical suggestions to both patients and doctors. Patients can also benefit from the collective knowledge stored on the blockchain by accessing insights and recommendations based on similar cases.
6. **Transaction Manager**: The transaction manager ensures the integrity and security of transactions on the blockchain network. It authenticates users, manages digital certificates,

and ensures that users have the appropriate permissions to access and transact with data on the blockchain. By providing identity verification and access control, the transaction manager enhances data privacy and security in the healthcare sector.

By combining blockchain technology with machine learning, this framework addresses key challenges in healthcare, including data privacy, secure transactions, and efficient data acquisition. It empowers doctors and patients with valuable insights and recommendations while ensuring the integrity and security of medical data transactions.

1. EXPERIMENTAL RESULTS
   1. *Login*

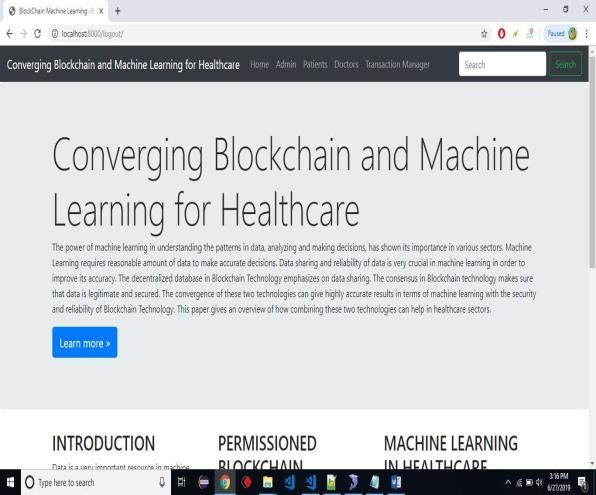


Fig 2: Home page

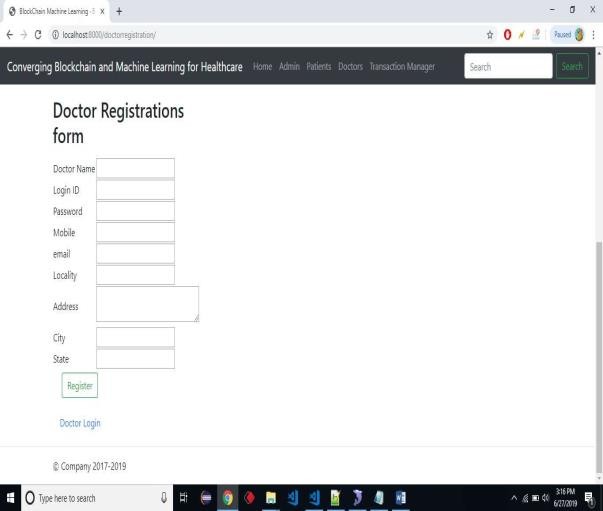


Fig 3: Doctor Registration

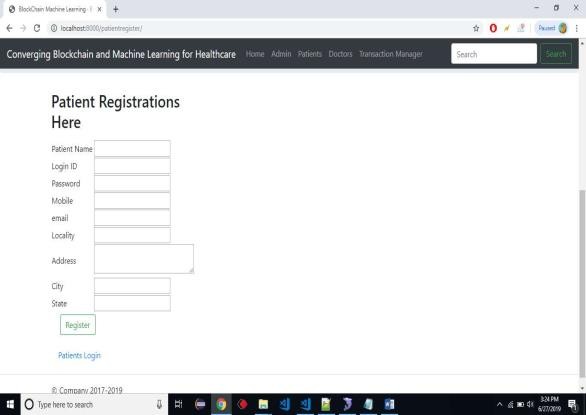
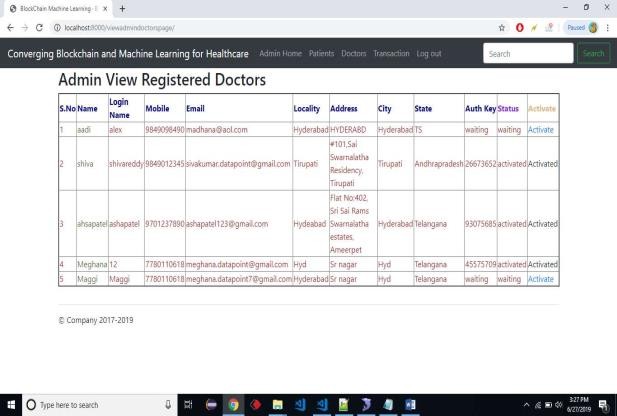
 

Fig 4: Patient Registration

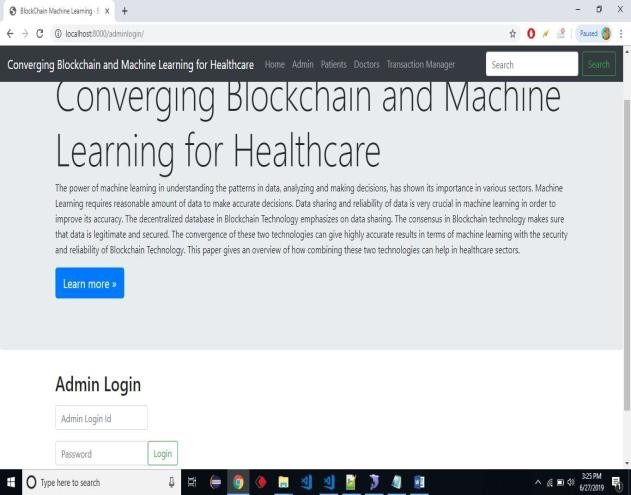


Fig 5: Admin Login

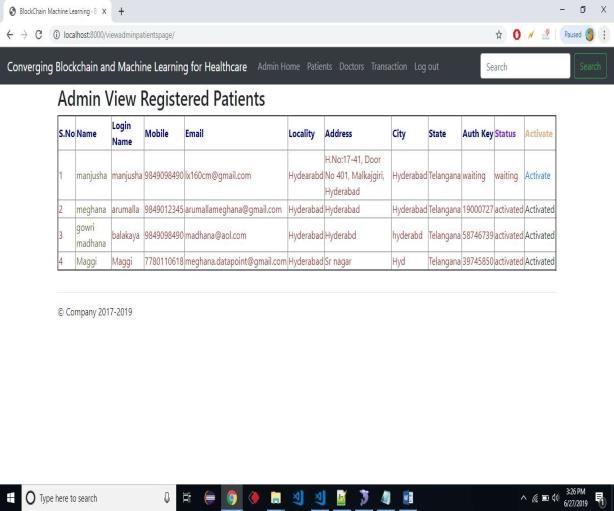


Fig 5: Patient Activation

Fig 6: Doctor Activation

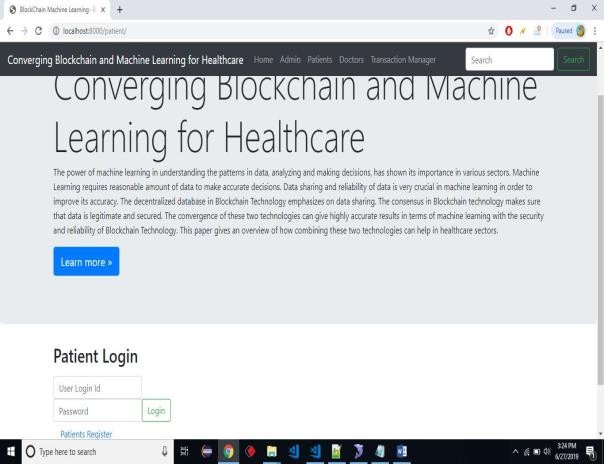


Fig 7: Patient Login

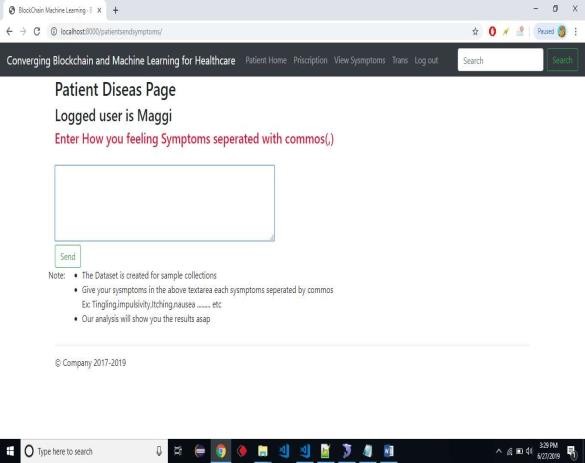


Fig 8: Prescription

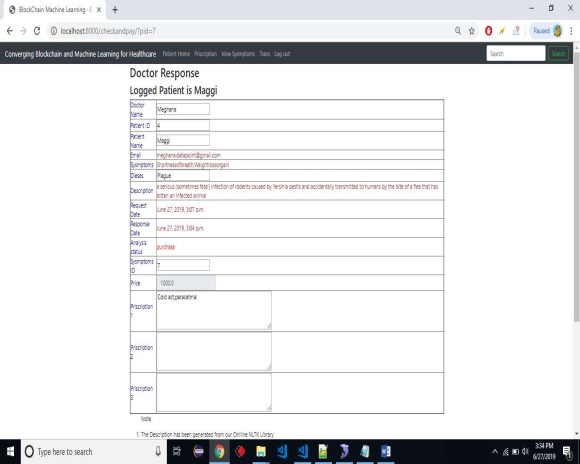
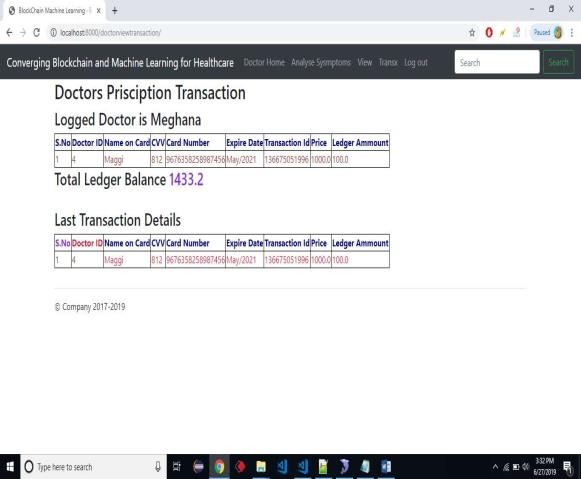
 

Fig 9: Doctor Response

* 1. *Analyse Symptoms*

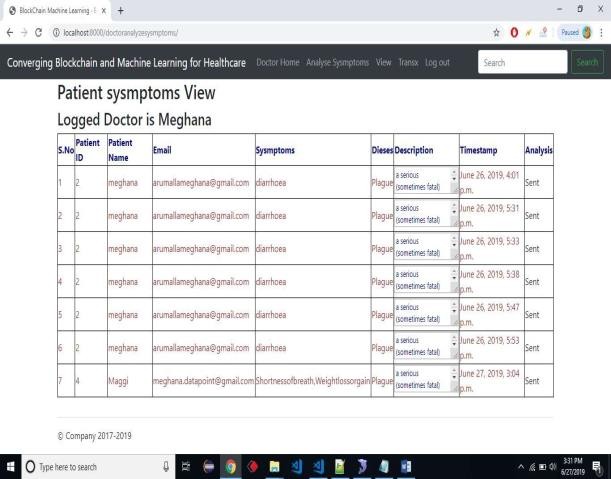


Fig 10: Analyse Symptoms

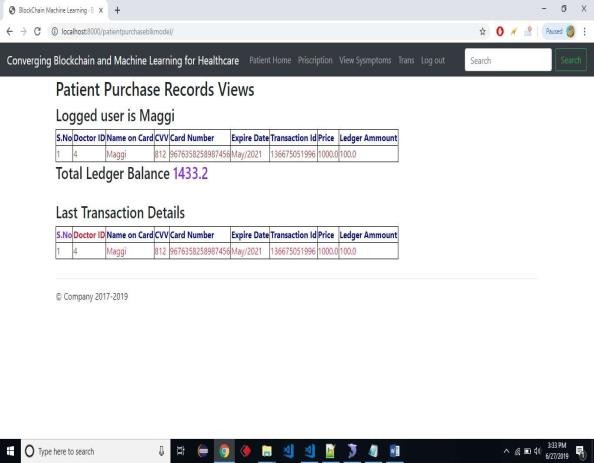


Fig 11: Patient Transactions

Fig 12: Doctor view

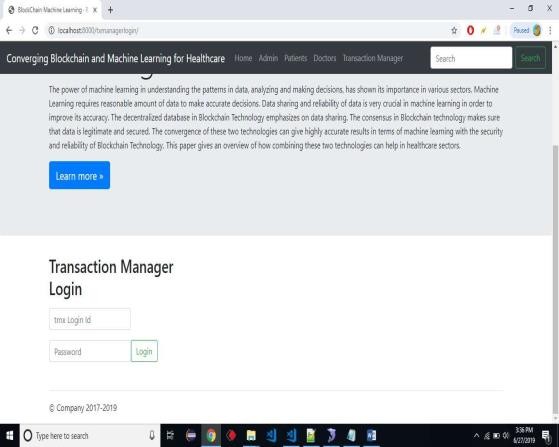


Fig 13: Transaction Manager

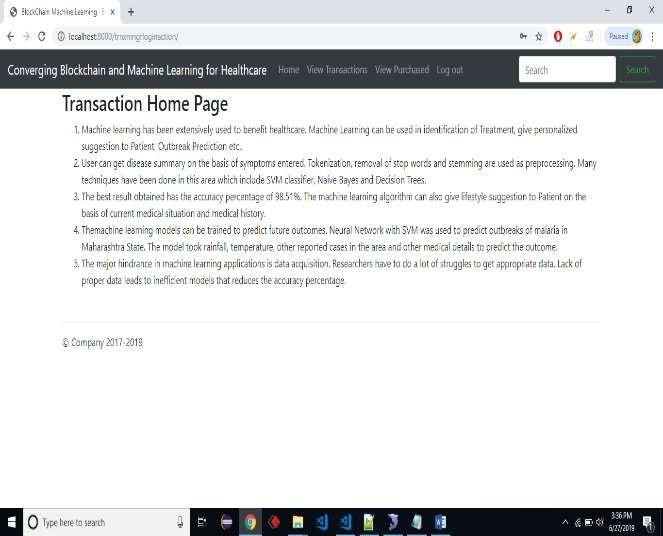


Fig 14: Transactions Home page

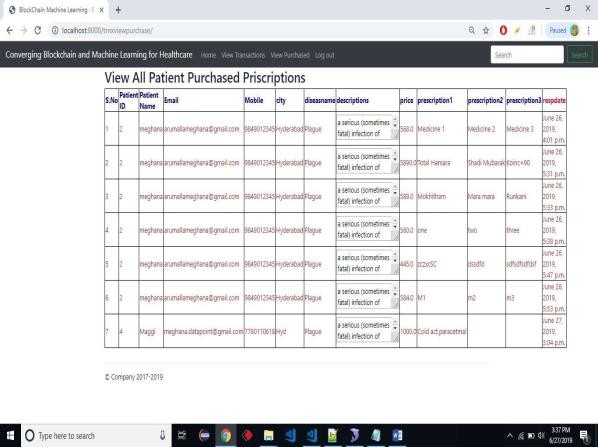
underscores its importance in shaping the future of industries across the globe.

Fig 15: View Purchased

1. CONCLUSION

Blockchain technology presents a vast array of opportunities beyond its initial association with cryptocurrencies like Bitcoin. It has the potential to revolutionize various industries by fundamentally altering traditional structures and processes. One of its most compelling features is its capacity to decentralize authority, thereby reducing reliance on centralized entities and eliminating associated commissions.

The healthcare industry stands to benefit immensely from this synergy. Given the critical nature of healthcare decisions, the utilization of blockchain-powered machine learning models can lead to more precise diagnoses and treatment plans. Patients receive better care, while healthcare providers can make more informed decisions, ultimately enhancing overall outcomes.

Looking ahead, the practical implementation of this model holds significant promise. As blockchain technology matures and becomes more widely adopted, its application in various sectors will continue to expand. In particular, the extension of this model to inventory management can serve as a potent tool in preventing fraud and optimizing supply chain operations.

In essence, the convergence of blockchain technology and machine learning represents a paradigm shift in how data is managed and utilized. Its potential to streamline processes, increase efficiency, and improve outcomes

FUTURE WORK

In the evolving landscape of blockchain technology integrated with machine learning, future work is poised to unlock transformative advancements across numerous domains.

Researchers and practitioners are likely to delve deeper into enhancing interoperability between disparate blockchain networks and machine learning systems, fostering seamless data exchange and collaboration. Moreover, the focus will be on developing privacy- preserving techniques to safeguard sensitive data in applications such as healthcare, while also exploring scalable solutions to accommodate the growing volume and complexity of data.

Additionally, efforts will be directed towards integrating federated learning techniques with blockchain technology, enabling secure and collaborative model training across decentralized networks. Alongside technological innovations, the establishment of regulatory frameworks and industry standards will be pivotal in ensuring ethical and responsible deployment of these technologies, fostering trust and adoption in real-world applications across diverse sectors.

ACKNOWLEDGMENT

In healthcare, blockchain networks can help store and share patient data. Blockchain applications can accurately identify critical and even dangerous errors in the medical field. Blockchain can play a key role in combating deception in clinical trials to improve health outcomes.

REFERENCE

1. N. Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. Matthias Mettler, “Blockchain Technology in Healthcare”, 2016

IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)

1. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy
2. Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct,2008
3. Pinyaphat Tasatanattakool and Chian Techapanupreeda, “Blockchain: Challenges and Applications”
4. Francisca Adoma Acheampong, Big Data Machine Learning and the BlockChain Technology: An Overview, International Journal of Computer Applications (0975 - 8887) Volume 180 - No.20, March 2018.
5. G. Dwyer. “The economics of Bitcoin and similar private digital currencies,” Journal of Financial Stability, vol. 17, pp. 81-91, April 2015.
6. G. Irving, H. John (2016, May), How blockchain- timestamped protocols could improve the trustworthiness of medical science. [Online].
7. Keerrthega.M.C, Ms.D.Thenmozhi “Identifying Disease Treatment Relations using Machine Learning Approach”, 2016 International Conference on Computational Science.
8. Bharti E. Nerkar and Sanjay S. Gharde, “Best Treatment Identification for Disease Using Machine Learning Approach in Relation to Short Text”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 22788727Volume 16, Issue 3, Ver. VII (May-Jun. 2014), PP 05-12.
9. https:/[/www.lanner-america.com/blog/10-applications-](http://www.lanner-america.com/blog/10-applications-) machinelearning-within-healthcare/

pharmaceuticals/applying blockchain-technology to medicine trace ability/s40/a2766/#.V5mxL\_m

1. G. Prisco (2016, April), The Blockchain for Healthcare: Gem Launches Gem Health Network with Philips Blockchain Lab, [Online]. Available: https://bitcoinmagazine.com/articles/theblockchain-for- heathcare-gemlaunches-gem-health-networkwith-philips- blockchain-lab-1461674938
2. S. Som, R. Roy Som, R. Mahajan (2016) “Survey of e- Health Status and Services in Eastern India”, Far East Journal of Electronics and Communication (International Journal), Vol. 3, Scopus Indexed, ISSN: 0973-7006, November 2016, Pages 723739.
3. O. Williams-Grut (2016, March), Estonia is using the technology behind bitcoin to secure 1 million health records, [Online].Available: <http://www.businessinsider.com/guardtime-estonian-> healthrecordsindustrial-blockchain-bitcoin-2016- 3?r=UK&IR=T.
4. P. Taylor (2016, April), Applying blockchain technology to medicine traceability, [Online]. Available: https:/[/www.securingindustry.com/](http://www.securingindustry.com/)

**HealthCare System Using Blockchain**

**Result**

**Introduction**

The healthcare industry faces a critical challenge in achieving seamless data exchange across its ecosystem due to diverse systems and formats. Hospitals, clinics, and labs frequently operate on different Electronic Health Record (EHR) systems that lack compatibility, resulting in fragmented patient information and disrupted care coordination. This fragmentation not only hinders the timely and comprehensive delivery of care but also increases the risk of treatment errors. Without smooth data integration, healthcare providers struggle to make informed decisions, leading to compromised patient outcomes and elevated operational costs. Ensuring interoperability is essential to improving healthcare quality, efficiency, and security.

**Objectives**

This study explores blockchain-based health management systems with a focus on interoperability and security. Through a systematic literature review, we examine architectural mechanisms that enhance these systems. Building on these insights, we propose a high-level architecture for a "Health Chain" system, validated through an experiment using Domain Specific Language (DSL) and Model Driven Engineering to create tailored smart contracts. Lastly, we address secure payment transactions between doctors and patients, leveraging blockchain technology to safeguard financial exchanges in healthcare.

**Methodology**

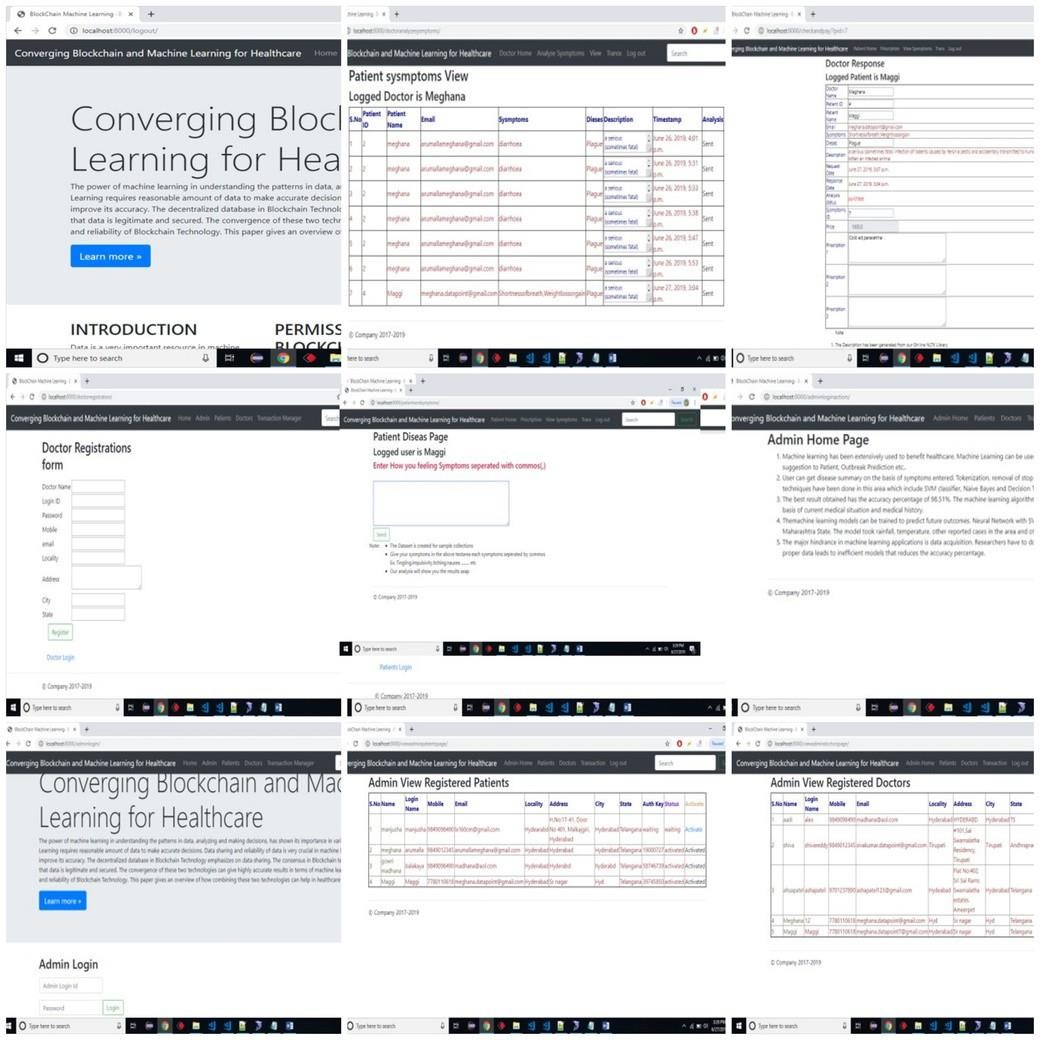
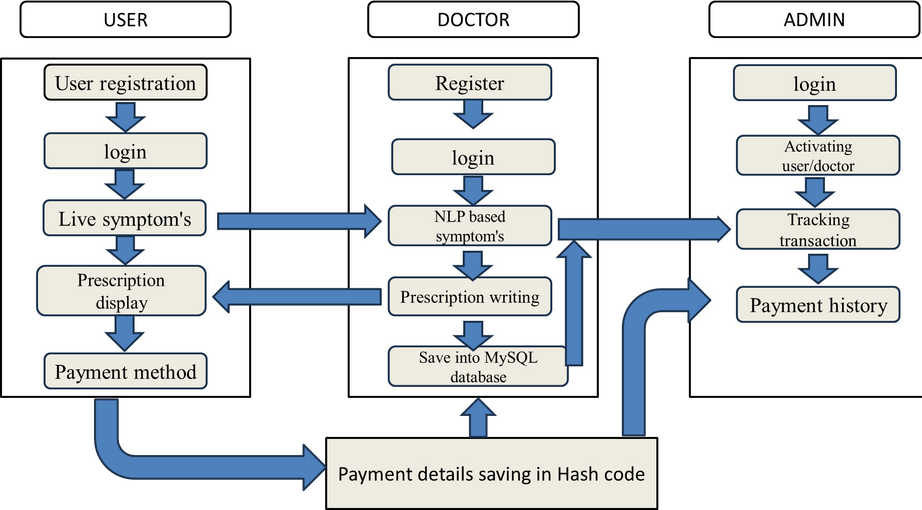
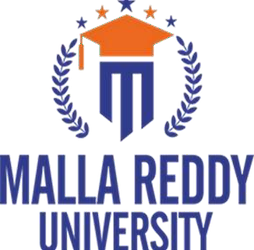
#### This methodology involves using blockchain technology to enable secure payment transactions between doctors and patients. The system supports interoperability by allowing the exchange of patients' medical information across healthcare systems. Patients will pay fees to access prescriptions, with blockchain ensuring transaction security and transparency.

Blockchain technology offers vast potential beyond cryptocurrency, eliminating central authorities and related fees. By enabling Machine Learning models to access data directly with managed rights, accuracy and usability are improved. This advancement benefits healthcare significantly, positively impacting both patients and doctors. Future work includes implementing this model practically and expanding it for fraud prevention in inventory management.

**Architecture**

**Conclusion**

**Future work**



**Authors:**

Dr.G.Vasavi(Associate professor) K.Akhil

D.Jathin Md.Reyaz

#### The next steps involve implementing the proposed blockchain and ML model in healthcare settings to evaluate its effectiveness in real- world scenarios. Expanding the model for secure data exchange across various healthcare systems is a key objective. Additional enhancements include integrating advanced fraud detection techniques, particularly for managing inventory and resources in hospitals. Improving scalability to accommodate larger datasets is also crucial. Further research will optimize blockchain-based payment solutions and refine ML-driven access rights management, supporting broader adoption and impact in healthcare.