**APPENDIX 1**

**DEVELOPMENT OF A SECURE HEALTHCARE MANAGEMENT SYSTEM UTILIZING BLOCKCHAIN TECHNOLOGY FOR ENCRYPTED PATIENT DATA TRANSMISSION**

**A PROJECT REPORT**

***Submitted By***

**DHANUSH BALAJI. G**

**SRIRAM. A**

**DARSHAN. R**

**VASANTH. V**

***in partial fulfillment for the award of the degree***

***of***

***BACHELOR OF ENGINEERING***

***IN***

COMPUTER SCIENCE AND ENGINEERING

**KARPAGA VINAYAGA COLLEGE OF ENGINEERING AND TECHNOLOGY**

**ANNA UNIVERSITY:: CHENNAI 600 025**

MAY 2025

**APPENDIX 2**

**ANNA UNIVERSITY: CHENNAI 600 025**

**BONAFIDE CERTIFICATE**

Certified that this project report **“DEVELOPMENT OF A SECURE HEALTHCARE MANAGEMENT SYSTEM UTILIZING BLOCKCHAIN TECHNOLOGY FOR ENCRYPTED PATIENT DATA TRANSMISSION”** is the Bonafide work of **“DHANUSH BALAJI. G, SRIRAM. A, DARSHAN. R, VASANTH. V”** who carried out the project work under my supervision.

**SIGNATURE**

(Dr. Jayapradha)

**HEAD OF THE DEPARTMENT**

Computer Science and Engineering

GST Road, Chinna Kolambakkam,

Palayanoor PO, Madurantagam Taluk,

Chengalpattu, Tamil Nadu 603 308.

**SIGNATURE**

(xxxxxxxxxxx)

**SUPERVISOR**

Assistant Professor

Computer Science and Engineering

GST Road, Chinna Kolambakkam,

Palayanoor PO, Madurantagam Taluk,

Chengalpattu, Tamil Nadu 603 308.

**DEVELOPMENT OF A SECURE HEALTHCARE MANAGEMENT SYSTEM UTILIZING BLOCKCHAIN TECHNOLOGY FOR ENCRYPTED PATIENT DATA TRANSMISSION**

**Abstract**:

In this project, patients visiting a hospital first consult a general doctor, who updates a prescription with the patient’s ID and medical notes. This prescription is securely shared with other departments—such as surgery, radiology, and pharmacy—where only authorized staff can access it using a department-specific secret key. To ensure security, the prescription is encrypted using the AES algorithm before being sent to each department. Once accessed, department staff can view and proceed with the necessary treatment, updating the patient’s details in the database. For added security, all patient data in the database is encrypted using the SHA-256 algorithm. This system ensures secure, authorized sharing and storage of sensitive medical information across departments.

**APPENDIX 3**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT**  **LIST OF FIGURES**  **LIST OF SYMBOLS**  **LIST OF ABBREVATIONS** |  |
| **1.** | **INTRODUCTION**   * 1. INTRODUCTION   2. EXISTING SYSTEM   3. PROPOSED SYSETM   1.3.1 OBJECTIVES  1.3.2 SCOPE   * 1. LITERATURE SURVEY   2. MERITS   3. DEMERITS |  |
| **2.** | **PROJECT DESCRIPTION**  2.1 GENERAL  2.2 METHEDOLOGIES  2.2.1 MODULES NAME  2.2.2 MODULES EXPLANATION  2.2.3 MODULE DIAGRAM  2.3 TECHNIQUE OR ALGORITHM |  |
| **3.** | **REQUIREMENTS**  3.1 GENERAL  3.2 HARDWARE REQUIREMENTS  3.3 SOFTWARE REQUIREMENTS |  |
| **4.** | **SYSTEM DESIGN**  4.1 GENERAL  4.1.1 USECASE DIAGRAM  4.1.2 STATE DIAGRAM  4.1.3 ACTIVITY DIAGRAM  4.1.4 CLASS DIAGRAM  4.1.5 SEQUENCE DIAGRAM  4.1.6 DATAFLOW DIAGRAM  4.1.7 ER – DIAGRAM  4.1.8 SYSTEM ARCHITECTURE |  |
| **5.** | **SOFTWARE SPECIFICATION**  5.1 GENERAL  5.1.1 FRONT END  5.2 JAVA  5.2.1 THE JAVA FRAMEWORK  5.2.2 OBJECTIVES OF JAVA  5.2.3 JAVA SERVER PAGES  5.2.4 EVOLUTION OF ANDROID APPLICATION  5.2.5 BENEFITS OF JSP  5.3 ANDROID XML  5.4 LAYOUTS  5.5 CONCLUSION |  |
| **6.** | **IMPLEMENTATION**  6.1 GENERAL  6.2 IMPLEMENTATION |  |
| **7.** | **SNAPSHOTS**  7.1 GENERAL  7.2 VARIOUS SNAPSHOTS |  |
| **8.** | **SOFTWARE TESTING**  8.1 FEASIBILITY STUDY  8.1.1 ECONOMICAL FEASIBILITY  8.1.2 TECHNICAL FEASIBILITY  8.1.3 OPERATIONAL FEASIBILITY  8.2 SYSTEM TESTING  8.2.1 VARIOUS LEVEL OF TESTING  8.2.1.1 WHITE BOX TESTING  8.2.1.2 BLACK BOX TESTING  8.2.1.3 UNIT TESTING  8.2.1.4 FUNCTIONAL TESTING  8.2.1.5 PERFORMANCE TESTING  8.2.1.6 INTEGRATION TESTING  8.2.1.7 VALIDATION TESTING  8.2.1.8 SYSTEM TESTING  8.2.1.9 OUTPUT TESTING  8.2.1.10 USER ACCEPTANCE TESTING |  |
| **9.** | **APPLICATION AND FUTURE ENHANCEMENT**  9.1 GENERAL  9.2 APPLICATIONS  9.3 FUTURE ENHANCEMENTS |  |
| **10.** | **CONCLUSION**  10.1 CONCLUSION  10.2 REFERNCES |  |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO** | **NAME OF THE FIGURE** | **PAGE NO.** |
| 2.3.2 | Module Diagram |  |
| 4.2 | Activity Diagram for Anonymous database Management |  |
| 4.3 | Use case Diagram for Anonymous database Management |  |
| 4.4 | Data flow diagram for Anonymous database Management |  |
| 4.5 | Sequence diagram for Anonymous database Management |  |
| 4.6 | Collaboration diagram for Anonymous database Management. |  |
| 4.7 | Class diagram for Anonymous database Management. |  |
| 4.8 | Architecture Diagram for Anonymous database Management |  |
| 4.9 | Object Diagram |  |
| 4.10 | State Diagram |  |
| 4.11 | Component Diagram |  |
| 4.12 | E-R Diagram |  |

**LIST OF SYMBOLS**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **NOTATION NAME** | **NOTATION** | **DESCRIPTION** |
| 1. | Class | *+ public*  *-private*  *# protected*  *Class Name*  *-attribute*  *-attribute*  *+operation*  *+operation*  *+operation* | Represents a collection of similar entities grouped together. |
| 2. | Association | Class B  Class A  name | Associations represents static relationships between classes. Roles representsthe way the two classes see each other. |
| 3. | Actor |  | It aggregates several classes into a single class. |
| 4. | Aggregation | Class B  Class A  Class B  Class A | Interaction between the system and external environment. |
| 5. | Relation  (uses) | **uses** | Used for additional process communication. |
| 6. | Relation  (extends) | extends | Extends relationship is used when one use case is similar to another use case but does a bit more. |
| 7. | Communication |  | Communication between various use cases. |
| 8. | State | State State | State of the processs. |
| 9. | Initial State |  | Initial state of the object |
| 10. | Final State |  | Final state of the object |
| 11. | Control Flow |  | Represents various control flow between the states. |
| 12. | Decision Box |  | Represents decision making process from a constraint |
| 13. | Usecase |  | Interaction between the system and external environment. |
| 14. | Component |  | Represents physical modules which is a collection of components. |
| 15. | Node |  | Represents physical modules which are a collection of components. |
| 16. | Data Process / Sate |  | A circle in DFD represents a state or process which has been triggered due to some event or action. |
| 17. | External entity |  | Represents external entities such as keyboard, sensors, etc. |
| 18. | Transition |  | Represents communication that occurs between processes. |
| 19. | Object Lifeline |  | Represents the vertical dimensions that the object communications. |
| 20. | Message |  | Represents the message exchanged. |

**LIST OF ABBREVATIONS**

|  |  |  |
| --- | --- | --- |
| **S.NO** | **ABBREVATION** | **EXPANSION** |
| 1**.** | DB | Data Base |
| 2. | SMC | Secure Multiparty Computation |
| 3. | SC | Service Center |
| 4. | DBC | Data Base Confidentiality |
| 5. | JVM | Java Virtual Machine |
| 6. | JSP | Java Server Page |

**CHAPTER 1:**

* 1. **INTRODUCTION:**

Patients who come to a hospital are first referred to a general doctor. A doctor updates the prescription with the patient's ID and medical notes. Such a prescription is safely shared with other departments: surgery, radiology, and pharmacy, among others. Only by authorized staff, a department-specific secret key can enable access to the prescription. For the purpose of security, a prescription is encrypted using the AES algorithm before sending it to each department. Such information, accessed only by staff in the department, can be viewed as helping to continue the required treatment. Then, patient details are updated in the database. All patient data in the database is encrypted with the SHA-256 algorithm for extra security. Thus, sensitive medical information is shared and stored across departments securely, accessible only to authorized personnel.

* 1. **EXISTING SYSTEM:**

The emergence of cloud computing enables various healthcare institutions to outsource pre-diagnostic models and provide timely and convenient services for patients. However, healthcare institutions and patients have serious concerns about potential privacy leakage as cloud servers cannot be fully trusted.

**Techniques**:

MAFRL method, kNN-based pre-diagnosis with linear complexity

k-Nearest Neighbor (kNN), and Mahalanobis Distance (MD)

* 1. **PROPOSED SYSTEM:**

In response to privacy concerns in healthcare, the proposed system adopts edge computing and blockchain technology. Edge devices process patient data locally, ensuring confidentiality, while blockchain establishes a secure ledger for data access. Patients retain control over their encrypted medical data, granting access only to authorized healthcare professionals. This decentralized approach enhances trust and transparency, safeguarding patient privacy without reliance on cloud computing.

**Techniques:**

AES Algorithm, OPEN SOURCE Blockchain, sha256.

**1.3.1 OBJECTIVES:**

**Enhance Data Security and Integrity**: Utilize blockchain technology to create a secure and immutable ledger for recording patient data, ensuring that information remains accurate and protected from unauthorized alterations or tampering.

**Streamline Specialist and Department Integration**: Develop a system where various healthcare professionals, including client specialists, radiologists, surgeons, and pharmacists, can efficiently register, log in, and access patient data through a structured endorsement process by administrators.

**Maintain Confidentiality**: Implement a unique encrypted identifier system for patient data to prevent misuse and ensure that sensitive information is only accessible by authorized personnel within different departments.

**Facilitate Efficient Data Handling**: Enable seamless communication between healthcare departments by forwarding unique encrypted identifiers, ensuring that patient information is correctly and securely processed across different stages of care.

**Ensure Compliance and Reliability**: Create a reliable and compliant system that adheres to healthcare data protection standards, fostering trust among patients and healthcare providers by ensuring the confidentiality and integrity of patient information.

**1.3.2 SCOPE:**

**User Registration and Login**:

**Client Specialist**: Register and log in, with endorsement by administrator support specialists.

**Radiologists, Surgeons, and Pharmacists**: Register and log in, with endorsement by administrators.

**Administrators**: Manage the registration and endorsement process for all specialists.

**Patient Interaction**:

**Patient Registration and Login**: Patients will register and log in to the web application.

**Specialist Interaction**: Specialists will provide patients with a unique encrypted identifier after consultation.

**Data Forwarding and Processing**:

**Unique Encrypted Identifier**: Specialists will issue a unique encrypted number to patients, which is then forwarded to relevant departments (surgery, radiology, pharmacy).

**Data Confidentiality**: Ensure that the unique identifier prevents any misuse of patient details.

**Blockchain Integration**:

**Immutable Ledger**: Use blockchain to record and verify patient data, enhancing data integrity and security.

**Encryption and Access Control**: Employ encryption techniques to secure patient data and control access based on role and endorsement.

**System Management**:

**Administrator Oversight**: Administrators will oversee the registration, endorsement, and login processes for all users, ensuring compliance and security within the system.

* 1. **LITERATURE SURVEY:**

# **TITLE:** Achieving Secure, Verifiable, and Efficient Boolean Keyword Searchable Encryption for Cloud Data Warehouse

**AUTHOR**: Thanaruk Theeramunkong, Somchart Fugkeaw

**YEAR:** · January 2024

**DESCRIPTION:**

Cloud data warehouse (CDW) platforms have been offered by many cloud service providers to provide abundant storage and unlimited accessibility service to business users. Sensitive data warehouse (DW) data consisting of dimension and fact data is typically encrypted before it is outsourced to the cloud. However, the query over encrypted DW is not practically supported by any analytical query tools. The Searchable Encryption (SE) technique is palpable for supporting the keyword searches over the encrypted data. Although many SE schemes have introduced their own unique searching methods based on indexing structure on top of searchable encryption techniques, there are no schemes that support Boolean expression queries essential for the search conditions over the DW schema. In this paper, we propose a secure and verifiable searchable encryption scheme with the support of Boolean expressions for CDW. The technical construct of the proposed scheme is based on the combination of Partial Homomorphic Encryption (PHE), B+Tree and Inverted Index, and bitmapping functions to enable privacy-preserving SE with efficient search performance suitable for encrypted DW. To enhance the scalability without requiring a third party to support the verification of search results, we employed blockchain and smart contracts to automate authentication, search index retention, and trapdoor generation. For the evaluation, we conducted comparative experiments to show that our scheme is more proficient and effective than related works.

# **TITLE:** MaxD K-means: A clustering algorithm for Auto-generation of centroids and distance of data points in clusters

**AUTHOR**: Tutut Herawan, Abul Beg

**YEAR:** · January 2012

**DESCRIPTION:**

K-Means is one of the unsupervised learning and partitioning clustering algorithms. It is very popular and widely used for its simplicity and fastness. The main drawback of this algorithm is that user should specify the number of cluster in advance. As an iterative clustering strategy, K-Means algorithm is very sensitive to the initial starting conditions. In this paper, we propose a clustering technique called MaxD K-Means clustering algorithm. MaxD K-Means algorithm auto generates initial k (the desired number of cluster) without asking for input from the user. MaxD K-means also used a novel strategy of setting the initial centroids. The experiment of the Max-D means has been conducted using synthetic data, which is taken from the Llyod’s K-Means experiments. The results from the new algorithm show that the number of iteration improves tremendously, and the number of iterations is reduced by confirming an improvement rate is up to 78%

# **TITLE:** Privacy-Preserving Patient-Centric Clinical Decision Support System on Naive Bayesian Classification

**AUTHOR:** Rongxing Lu, Ximeng Liu , Jianfeng Ma

**YEAR:**January 2015

**DESCRIPTION:**

Clinical decision support system (CDSS), which uses advanced data mining techniques to help clinician make proper decisions, has received considerable attention recently. The advantages of CDSS include not only improving diagnosis accuracy but also reducing diagnosis time. Specifically, with large amounts of clinical data generated everyday, na¨ ıve Bayesian classification can be utilized to excavate valuable information to improve CDSS. Although CDSS is quite promising, the flourish of CDSS still faces many challenges including information security and privacy concerns. In this paper, we propose a new privacy preserving patient-centric clinical decision support system, called PPCD, which helps clinician complementary to diagnose the risk of patients’ disease in a privacy-preserving way. In PPCD, the past patients’ historical data are stored in cloud and can be used to train the na¨ ıve Bayesian classifier without leaking any individual patient medical data, and then the trained classifier can be applied to compute the disease risk for new coming patients and also allow these patients to retrieve the top-k disease names according to their own preferences. Specifically, to protect the privacy of past patients’ historical data, a new cryptographic tool called additive homomorphic proxy aggregation scheme is designed. Moreover, to leverage the leakage of na¨ ıve Bayesian classifier, we introduce a privacy-preserving top-k disease names retrieval protocol in PPCD. Detailed privacy analysis ensures that patient’s information is private and will not be leaked out during the disease diagnosis phase. In addition, performance evaluation via extensive simulation also demonstrates that our PPCD can efficiently calculate patient’s disease risk with high accuracy in a privacy-preserving way.

* 1. **MERITS:**

**Merits:**

* **Privacy Protection**: Ensuring the confidentiality and security of sensitive patient information.
* **Edge Computing**: Processing data locally on devices within the healthcare institution rather than relying on centralized cloud servers.
* **Blockchain Technology**: A decentralized and secure ledger system for recording and managing data access and transactions.
* **Data Sovereignty**: Giving patients control over their medical data, allowing them to manage access permissions.
* **Security**: Measures taken to protect data from unauthorized access, modification, or disclosure.

**DEMERITS:**

It requires high energy utilization contrasted with other agreement conventions. Information exchange is unreliable.

**CHAPTER 2**

**2.1 GENERAL:**

**2.2 METHODOLOGIES:**

Methodologies is the process of analysing the principles or procedure of a Progressive Anonymous Database management system.

**2.2.1 MODULES NAME:**

* USER
* DOCTORS
* SURGEON
* RADIOLOGIST
* PHARMACIST
* ADMIN

**2.2.2 MODULE EXPLANATION:**

1. **USER REGISTER AND LOGIN:**

This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. They registered with datas and then login

1. **ADMIN LOGIN AND APPROVE:**

This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. The admin login in to the application, they verify the user application and approve to check it manually in these application.

1. **DOCTORS** **REGISTER AND LOGIN:**

This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. They registered with datas and then login.

1. **SURGEON** **REGISTER AND LOGIN:**

This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. They registered with datas and then login.

1. **RADIOLOGIST** **REGISTER AND LOGIN:**

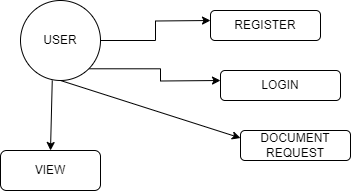
This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. They registered with datas and then login.

1. **PHARMACIST** **REGISTER AND LOGIN:**

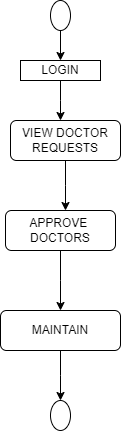
This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. They registered with datas and then login.

**2.2.3 MODULE DIAGRAM:**

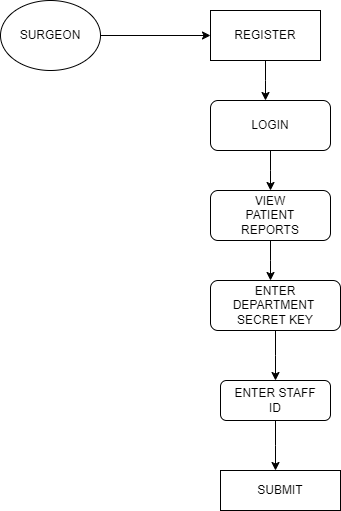
**USER:**

****

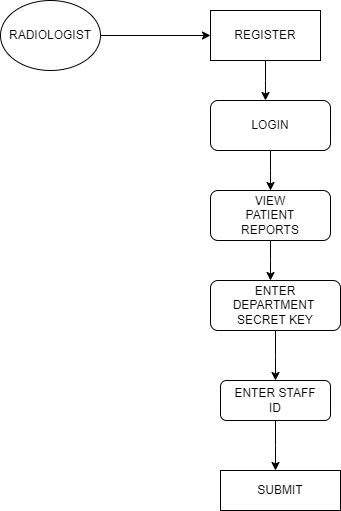
**ADMIN**

****

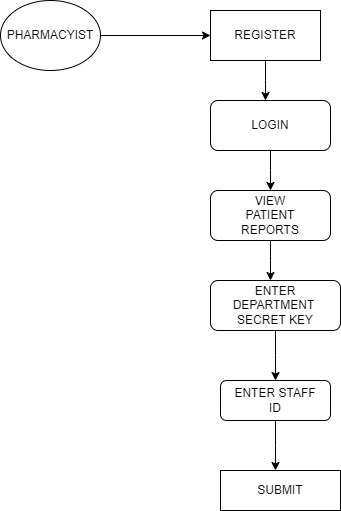
**SURGEON**

****

**RADIOLOGIST**

****

**PHARMACIST:**

****