# *Development and Validation of an Artificial Intelligence System to Optimize Clinician Review of Patient Records*

**Authors:** Ethan Andrew Chi, Gordon Chi, Cheuk To Tsui, et al.
**Published in:** *JAMA Network Open, 2021*

---

**Key Takeaways**

This research paper focuses on the use of **Artificial Intelligence (AI) to improve clinician efficiency in reviewing patient records** by organizing and optimizing data retrieval.

**What We Use**

🔷 **AI-Assisted Data Organization for Patient Records:**

- The research developed an **AI-powered system** that organizes **unstructured medical records** into structured formats.
- Your project can **apply a similar approach** to enhance **data accessibility for healthcare professionals in Sri Lanka**.

🔷 **Reduction in Time for Clinician Data Review:**

- The AI system **reduced review time by 18%** compared to non-AI record review while maintaining high accuracy.
- Your project can leverage **AI-driven searchability & indexing** to **reduce time spent by doctors and improve efficiency in Sri Lankan hospitals.**

🔷 **Challenges in Medical Data Extraction:**

- Issues in data extraction include **scanning errors, redundant information, and lack of structured formatting.**
- Your system should integrate **Natural Language Processing (NLP) and Optical Character Recognition (OCR)** to **improve data structuring and readability.**

🔷 **Cloud-Based Data Security Considerations:**

- The paper highlights concerns regarding **data security, encryption, and user authentication.**
- Your project must **ensure secure patient record handling** using **cloud-based encryption and access control mechanisms** (e.g., **AES encryption, secure login authentication**).

---

**What We Gained**

**✓ Understanding AI's Role in Healthcare Record Management:**

- The study proves that **AI can significantly improve the efficiency of medical data review**, reducing clinician workload.
- This validates your **project's goal to digitize healthcare records** for Sri Lankan hospitals.

✓ **Inspiration for System Design:**

- The research used **a web-based interface to present structured patient data.**
- Your system can **adopt a similar design** with an **interactive dashboard for medical professionals.**

✓ **Validation of AI Accuracy in Medical Record Review:**

- AI **did not compromise accuracy** while improving efficiency.
- This supports your approach of **integrating AI models for data analysis while maintaining medical accuracy.**

✓ **Empirical Evidence for AI Adoption in Healthcare:**

- 92% of clinicians preferred AI-assisted record review over traditional methods.
- This shows that **healthcare professionals are willing to adopt AI-driven solutions**, reinforcing your project's feasibility.

# *Patient Health Record Systems Scope and Functionalities: Literature Review and Future Directions*

**Authors:** Lina Bouayad, Anna Ialynytchev, Balaji Padmanabhan

**Published in:** *Journal of Medical Internet Research, 2017*

**Key Takeaways**

This paper presents a **literature review of Personal Health Records (PHRs)** and their evolution, functionality, and challenges. It provides insights into **how PHRs contribute to patient engagement, healthcare digitization, and AI-based analytics**.

**What We Use**

🔷 **Evolution of Personal Health Records (PHRs):**

- PHRs have evolved from simple **data storage systems** to **interactive platforms** that allow data sharing, automation, and predictive analytics.
- Your project can **incorporate AI-driven automation and predictive analytics** for better **patient-centric healthcare management.**

🔷 **Integration of AI & Data Analytics in Healthcare:**

- The study highlights **how AI-based analytics in PHRs can help with disease prediction, patient risk assessment, and treatment recommendations.**
- Your system can **apply machine learning models** to predict patient conditions based on stored health records.

🔷 **Security & Privacy Challenges in PHRs:**

- The research emphasizes **data security concerns** in handling **patient-generated data.**
- Your project should **prioritize strong encryption, role-based access control, and compliance with healthcare regulations (e.g., GDPR, HIPAA).**

🔷 **Impact of PHRs on Patient-Centric Healthcare:**

- PHRs **empower patients** by providing them access to their medical records, appointment scheduling, and treatment plans.
- Your system can **include a patient dashboard** where users can track their health progress, receive automated alerts, and communicate with doctors.

🔷 **Emerging Trends: Remote Monitoring & IoT in Healthcare:**

- The paper highlights **real-time health tracking using IoT devices** such as smartwatches and biosensors.

- Your project can explore **integrating wearable health data** into the system for **real-time patient monitoring and AI-based health predictions.**

---

**What We Gained**

**✓ Understanding How PHRs Enhance Healthcare Efficiency:**

- AI-driven **electronic health record (EHR) management** reduces **doctor workload** and **improves decision-making.**

**✓ Validating the Role of AI & Predictive Analytics in Healthcare:**

- AI-powered **patient risk assessment and health prediction models** can enhance the **quality of medical care.**

**✓ Inspiration for System Architecture:**

- A **secure cloud-based platform** with **patient-provider communication, automated reminders, and data-driven decision support.**

**✓ Recognizing Data Security as a Core Concern:**

- Need for **encrypted storage, multi-factor authentication, and compliance with healthcare regulations.**

## *Performance Evaluation of AWS and IBM Cloud Platforms for Security Mechanism*

**Authors:** Avneet Kaur, Sachin Yadav, Gaurav Raj, Tanupriya Choudhury
**Published in:** *International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), 2018*

---

**Key Takeaways**

This research compares **AWS and IBM Cloud** based on security mechanisms, **performance benchmarking**, and **cost efficiency** using the **Phoronix Test Suite**.

**What We Use**

🔷 **Cloud-Based Security Mechanisms:**

- AWS uses **RSA security** techniques, while IBM lacks this feature.
- Your project should **implement strong encryption (e.g., RSA, AES) for patient record security** in the cloud.

🔷 **Performance Benchmarks for Healthcare AI Systems:**

- AWS outperforms IBM in **disk performance and RAM speed.**
- For AI-driven healthcare solutions, AWS might be **more suitable for high-speed data processing** in **Sri Lankan hospitals**.

🔷 **Cost Analysis for Cloud-Based Healthcare AI:**

- AWS is **more cost-effective** compared to IBM.
- Your system can **optimize cost efficiency by leveraging AWS Elastic Compute Cloud (EC2) and S3 storage** for medical records.

🔷 **Cloud Scalability & Flexibility for Hospitals:**

- AWS allows **on-demand scaling**, making it easier to **handle large hospital datasets**.
- Your project should integrate **cloud-based auto-scaling** to **manage patient records efficiently** as hospital demands fluctuate.

---

**What We Gained**

✓ **Understanding the Best Cloud Platform for Your Project:**

- AWS is **more secure, cost-effective, and scalable** than IBM for **AI-based patient record management**.

✓ **Guidelines for Implementing Secure Cloud Storage:**

- The research emphasizes **security layers (IAM policies, RSA encryption, and firewall protection)**, which you should incorporate.

✓ **Cloud Computing in AI-Driven Healthcare:**

- AWS services like **EC2, S3, CloudFront, and Route 53** can improve **data storage, access speed, and reliability**.

✓ **Data Processing Speed for AI Models:**

- Since AWS provides **better performance metrics** for **RAM, storage, and processing**, it is ideal for **training AI models on patient health records**.

# *Data Security in Cloud Computing*

**Authors:** Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills
**Published in:** *University of Southampton, IEEE, 2016*

---

**Key Takeaways**

This research paper provides an in-depth **analysis of data security concerns in cloud computing**, including **encryption mechanisms, virtualization risks, public cloud threats, and security challenges**.

**What We Use**

🔷 **Cloud Security for Healthcare Data Protection**

- The study discusses **the importance of encrypting both Data-at-Rest and Data-in-Transit**.
- Your project can **implement strong encryption techniques (AES, RSA) to secure patient records** stored in the cloud.

🔷 **Challenges in Public Cloud Storage for Medical Records**

- Public cloud solutions expose **sensitive patient data to risks like unauthorized access, breaches, and cyber-attacks**.
- Your project should consider **a hybrid cloud model** (using both **private and public clouds**) for balancing **security and accessibility**.

🔷 **Virtualization Security Risks in Healthcare AI Systems**

- The paper highlights how **hypervisor vulnerabilities** can expose patient data in **multi-tenant cloud environments**.
- Your project should include **isolation mechanisms and strong user authentication protocols** to **prevent unauthorized access**.

🔷 **Encryption Techniques for Securing Cloud Data**

- The study explains **three cryptographic methods** used in cloud security:
  ✅ **Block Ciphers** – Encrypts data in **fixed-size blocks** (e.g., AES-256).
  ✅ **Stream Ciphers** – Encrypts data **bit-by-bit** (used for **real-time data transmission**).
  ✅ **Hash Functions** – Converts patient data into **unique digital signatures** for **integrity verification**.
- Your system should **use a combination of AES (for storage) and Hashing (for integrity verification)**.

🔷 **Authentication & Access Control in Cloud-Based Healthcare Systems**

- The research highlights **multi-factor authentication (MFA) and role-based access control (RBAC)** as critical security measures.

- Your project should **restrict access based on user roles** (e.g., **Doctors, Nurses, Admins**) to **prevent unauthorized modifications**.

---

**What We Gained**

**✓ Understanding Cloud-Based Data Protection Strategies**

- The study emphasizes **data confidentiality, integrity, and availability (CIA)**, which are critical for **securing patient records**.

**✓ Justification for Using Hybrid Cloud in Healthcare AI**

- Public cloud **reduces costs but poses security risks**, while private cloud **ensures stronger control over patient data**.

**✓ Guidelines for Implementing AI Security in Medical Data Handling**

- Ensures **compliance with healthcare security standards (HIPAA, GDPR)** for handling **sensitive patient data**.

**✓ Validation of Security Mechanisms for Your AI System**

- You can **apply best practices** from this study to **secure AI-driven medical analytics and patient monitoring**.

## *Clinical Data Analysis for Prediction of Cardiovascular Disease Using Machine Learning Techniques*

**Authors:** Rajkumar Gangappa Nadakinamani, A. Reyana, Sandeep Kautish, et al.
**Published in:** *Computational Intelligence and Neuroscience, 2022*

---

**Key Takeaways**

Despite its retraction, this research explores **machine learning (ML) techniques for cardiovascular disease prediction**, which is **relevant to AI-based patient health management** in your project.

**What We Use**

🔷 **Application of ML in Clinical Data Analysis**

- The study used **various ML models (Random Tree, Naïve Bayes, J48, Linear Regression, JRIP) to classify cardiovascular disease data.**
- Your project can **apply similar ML models** for **predictive analytics in patient health monitoring.**

🔷 **Best Performing ML Model for Disease Prediction**

- The study found **Random Tree achieved 100% accuracy** in cardiovascular disease prediction.
- Your system could **benchmark its own ML model's performance** against these reported accuracy levels.

🔷 **Importance of Data Preprocessing in Healthcare AI**

- The research emphasized **handling missing and noisy values using filtering techniques** to improve prediction accuracy.
- Your project must **include robust data preprocessing techniques** to ensure **clean and structured patient data.**

🔷 **Feature Selection for ML-Based Disease Prediction**

- The study highlights **key health record features** used in prediction models:
    - **Age, Blood Pressure, Cholesterol, ECG Readings, Heart Rate, etc.**
- Your project can **incorporate a similar feature set** while **validating their impact on prediction accuracy.**

🔷 **Evaluation Metrics for ML Models**

- The study used **Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and Accuracy** to assess model performance.
- Your project should **apply these metrics** to **evaluate AI-driven medical insights.**

---

**What We Gained**

✓ **Understanding ML's Role in Disease Prediction**

- Reinforces the idea that **ML can effectively analyze medical data** to predict diseases.

✓ **Guidance on Model Selection for Healthcare AI**

- Confirms that **Random Tree, Naïve Bayes, and J48** perform well in **classifying patient health data.**

✓ **Data Preprocessing as a Key Factor in AI-Driven Healthcare**

- Highlights the need for **handling missing values, feature selection, and data standardization.**

✓ **Performance Benchmark for Your Project's ML Model**

- Your AI system can be **compared against the reported 100% accuracy of Random Tree** to **validate improvements.**

## *Electronic Patient Records – The Reality*

**Authors:** Dr. Kumara Mendis, Prof. Ian Purves
**Published in:** *University of Kelaniya, Sri Lanka (2019)*

---

**Key Takeaways**

This paper provides an in-depth **analysis of Electronic Patient Records (EPRs)** and their role in improving **healthcare efficiency, data management, and decision-making**. It also examines **Sri Lanka's healthcare context** and discusses the **challenges and benefits of digitizing patient records**.

**What We Use from This Research**

🔷 **Challenges of Paper-Based Medical Records**

- Paper records are **inefficient, error-prone, and difficult to manage** in modern healthcare.
- Your project supports **digital transformation by replacing manual records with AI-driven EPRs** for **better efficiency and accuracy**.

🔷 **Electronic Patient Records (EPRs) as Essential Tools**

- The **Institute of Medicine (USA)** considers EPRs an *"essential tool for modern medicine."*
- Your system aligns with this vision by **creating a cloud-based patient record system** integrated with **AI-driven analytics**.

🔷 **EPRs in Developed vs. Developing Countries**

- Developed countries have **successfully implemented EPRs** for improved healthcare.
- In Sri Lanka, **EPR adoption is still in its early stages**, providing an **opportunity for AI-driven transformation** in **local hospitals**.

🔷 **Impact of EPRs on Clinical Efficiency**

- Doctors spend **one-third of consultation time retrieving medical records**.
- Your project **reduces this workload** by offering **AI-powered data retrieval and analysis**, improving **decision-making efficiency**.

🔷 **EPR Features & Functionalities for Sri Lankan Healthcare**

- The paper highlights key **EPR functionalities** required for **Sri Lankan hospitals**, including:
  ✅ **Cloud storage for medical records**
  ✅ **Clinical decision support systems (CDSS)**
  ✅ **AI-based diagnostic assistance**
  ✅ **Secure patient data handling with access control**
- Your system can **incorporate these features** to enhance **patient care quality and hospital efficiency**.

### 🔷 Security & Privacy Challenges in EPRs

- **Data breaches, unauthorized access, and cyber risks** are major concerns in EPR adoption.
- Your project must integrate **AES encryption, multi-factor authentication, and role-based access controls** to **ensure patient data privacy**.

### 🔷 Adoption Barriers & Implementation Strategies

- The research identifies **barriers to EPR adoption** in Sri Lanka, such as:
    - **Lack of funding and IT infrastructure**
    - **Limited digital literacy among healthcare staff**
    - **Resistance to change from manual to digital records**
- Your project should include **training programs and user-friendly interfaces** to **ease the transition to AI-driven EPRs**.

---

## What We Gained

### ✓ Validation of EPR Importance in Healthcare

- Reinforces the idea that **digitizing patient records improves efficiency, decision-making, and data security**.

### ✓ Understanding Local Healthcare Challenges

- Provides insights into **Sri Lanka's healthcare digitalization gaps**, helping your project **tailor solutions to local needs**.

### ✓ Guidance for System Features & Design

- Confirms the need for **cloud-based AI-driven patient management systems** in Sri Lankan hospitals.

### ✓ Security Measures for Cloud-Based EPRs

- Recommends **data encryption, access control, and secure authentication methods** to protect **patient records**.

## *Implementation Challenges and Research Gaps of Electronic Medical Records (EMR) in Public Sector Hospitals of Sri Lanka*

**Authors:** Kumudini Sarathchandra, Shriyananda Rathnayake
**Published in:** *International Journal of Scientific and Research Publications, July 2019*

---

**Key Takeaways**

This research focuses on **the challenges, progress, and research gaps in implementing Electronic Medical Records (EMR) in Sri Lanka's public hospitals**. It provides a **valuable local perspective** on the **barriers to adopting digital health solutions**, which aligns with your project's goals.

**What We Use from This Research**

🔷 **Challenges in Implementing EMRs in Sri Lanka**

- The study identifies **barriers to EMR adoption**, including:
  ✅ **Resistance to change** among healthcare professionals.
  ✅ **Limited IT infrastructure** in public hospitals.
  ✅ **Lack of a national policy** for full-scale EMR implementation.
  ✅ **Security and privacy concerns** related to patient data protection.
- Your project should **address these challenges by incorporating user-friendly designs, secure cloud storage, and training programs** for medical staff.

🔷 **Gaps in EMR Research in Sri Lanka**

- **Few scientific studies exist** on the effectiveness of EMRs in Sri Lanka.
- Most research focuses on **user acceptance** rather than **technical and economic feasibility**.
- Your thesis can help **fill this gap by analyzing the performance and cost-effectiveness of AI-driven EMRs in local hospitals.**

🔷 **Current Status of EMR Adoption in Sri Lankan Hospitals**

- The government planned to implement EMRs in **300 hospitals by 2018**, but by mid-2019, only **50 hospitals (15%) had adopted the system**.
- Lack of **interoperability between different healthcare institutions** prevents full integration.
- Your project should **design an AI-based EMR solution that integrates seamlessly across different hospitals** to enhance **data-sharing and accessibility.**

🔷 **Security & Privacy Concerns in EMR Implementation**

- Over **3 million patient records** exist in digital form, but **data security measures are weak.**
- Your project should include **AES encryption, multi-factor authentication, and routine security audits** to **ensure data integrity and confidentiality.**

### 🔷 Role of AI & Data Analytics in EMR Adoption

- The study recommends integrating **data mining and AI-driven decision support tools** to enhance **patient care**.
- Your project aligns with this **by using AI analytics for predictive healthcare insights**.

---

### What We Gained

**✓ Understanding the Barriers to EMR Implementation in Sri Lanka**

- Helps you **identify potential challenges** and plan **solutions** for successful system deployment.

**✓ Guidance on Policy & Standardization for EMRs**

- Confirms the need for a **national policy and government involvement** to scale up **AI-powered EMR systems.**

**✓ Security & Privacy Best Practices for Your System**

- Reinforces the importance of **strong data protection mechanisms** in **cloud-based healthcare solutions.**

**✓ Benchmark for EMR Adoption in Sri Lanka**

- Provides **local implementation statistics** you can **compare with your project's expected impact.**

## *Enhancing the Security of Cloud Data Using Hybrid Encryption Algorithm*

**Authors:** K. R. Sajay, Suvanam Sasidhar Babu, Yellepeddi Vijayalakshmi
**Published in:** *Journal of Ambient Intelligence and Humanized Computing, 2024*

---

### Key Takeaways

This research focuses on **hybrid encryption techniques for securing cloud data**, which is **relevant to protecting patient health records in cloud-based Electronic Medical Record (EMR) systems**. Despite its retraction, **some of its concepts remain valuable** for understanding **cloud security strategies**.

### What We Use from This Research

🔷 **Hybrid Encryption for Cloud-Based EMR Security**

- The study proposed a **hybrid encryption model** combining:
  ✅ **AES (Advanced Encryption Standard)** for **fast encryption of large medical datasets**.
  ✅ **RSA (Rivest-Shamir-Adleman)** for **secure key exchange between users and cloud servers**.
- Your project can **adopt a similar hybrid encryption approach** to ensure **high-security standards for patient records stored in the cloud**.

🔷 **Cloud Data Security Vulnerabilities**

- The paper highlights **common security threats** in cloud storage:
  ✅ **Data breaches due to weak encryption mechanisms.**
  ✅ **Man-in-the-middle (MITM) attacks on unprotected communication channels.**
  ✅ **Unauthorized access due to improper authentication protocols.**
- Your project should integrate **multi-layer encryption** and **secure authentication mechanisms (e.g., Multi-Factor Authentication - MFA)** to mitigate these threats.

🔷 **Comparative Performance of Encryption Algorithms**

- The study compared encryption techniques in terms of **speed, security level, and resource consumption**:
  ✅ **AES was the fastest but less secure for key exchange.**
  ✅ **RSA was highly secure but computationally expensive.**
  ✅ **A hybrid model (AES + RSA) provided the best balance between speed and security.**
- Your project should consider **benchmarking encryption techniques** for **optimal performance in securing patient records.**

🔷 **Key Exchange Mechanism for Secure Data Access**

- The research suggested **a hybrid key exchange system** using:
  ✅ **Public-key cryptography (RSA) for initial authentication.**
  ✅ **Session-based AES encryption for fast data retrieval.**

- Your project can **adopt this hybrid key exchange model** to enhance **secure access control for hospital data storage.**

---

**What We Gained**

**✓ Understanding Hybrid Encryption for Cloud-Based Healthcare Systems**

- Confirms that **a combination of AES + RSA provides a robust encryption solution for securing medical records.**

**✓ Guidelines for Data Security in Cloud-Based EMRs**

- Reinforces the importance of **secure key exchange mechanisms, end-to-end encryption, and secure authentication layers.**

**✓ Validation of Secure Data Transmission Approaches**

- Supports the need for **TLS/SSL encryption** in **cloud-based patient record management systems.**

**✓ Performance Benchmarking of Encryption Algorithms**

- Helps **evaluate trade-offs between encryption speed, security, and computational efficiency** in your project.

# *Encryption as a Service for Data Healthcare Cloud Security*

**Authors:** Abdelali El Bouchti, Samir Bahsani, Tarik Nahhal
**Published in:** *IEEE, 2016*

---

**Key Takeaways**

This research focuses on **Encryption as a Service (EaaS)** for securing **cloud-based healthcare data**, which directly relates to the **security model of your AI-driven patient record management system**.

**What We Use**

🔷 **Encryption as a Service (EaaS) for Healthcare Cloud Security**

- The study introduces **EaaS as a cloud security model** that allows **healthcare organizations to manage their encryption keys independently from cloud providers**.
- Your project can **incorporate EaaS** by enabling **end-to-end encryption for patient records**, ensuring that hospitals retain control over **data privacy and compliance**.

🔷 **Hybrid Encryption Model Using Cryptography-as-a-Service (CaaS)**

- The paper proposes a **hybrid cloud security model** based on:
  ✅ **Homomorphic Encryption** – Allows computations on encrypted data without decryption.
  ✅ **RSA Algorithm** – Provides **strong asymmetric encryption** for securing patient data.
- Your system can **use a similar hybrid encryption strategy** to ensure **secure medical data storage and processing**.

🔷 **Benefits of Cloud-Based Encryption for Healthcare**

- Cloud encryption enhances:
  ✅ **Data confidentiality** – Prevents unauthorized access to sensitive patient data.
  ✅ **Data integrity** – Ensures that **medical records remain unchanged and verifiable**.
  ✅ **Secure patient-doctor communication** – Protects **EHR access** using **end-to-end encryption**.
- Your project should **incorporate these security measures** to **enhance cloud-based patient record management.**

🔷 **Challenges in Implementing Cloud-Based Encryption in Healthcare**

- The paper identifies **three major barriers**:
  ✅ **Latency issues** – Complex encryption can **slow down hospital data retrieval**.
  ✅ **Data availability concerns** – Hospitals must ensure **secure data backup & redundancy**.
  ✅ **Regulatory compliance** – Cloud-based EHR systems must **comply with HIPAA & GDPR**.
- Your system should **optimize encryption for speed, integrate backup solutions, and comply with healthcare data regulations**.

**What We Gained**

✓ **Understanding the Role of EaaS in Securing Healthcare Data**

- Confirms that **hospitals can maintain control over their encryption keys** using **cloud security models like EaaS**.

✓ **Guidance for Implementing Hybrid Encryption in Patient Record Management**

- Reinforces the **use of RSA & Homomorphic Encryption** for **secure healthcare cloud storage**.

✓ **Validation of Security Challenges in Cloud-Based Healthcare AI**

- Identifies **latency, data availability, and compliance risks**, which your project must **address**.

✓ **Inspiration for AI-Based Secure Medical Data Processing**

- Suggests that **hospitals can process encrypted data using AI without compromising security** (e.g., **secure AI-driven patient analytics**).

# *Database Security Management for Healthcare SaaS in the Amazon AWS Cloud*

**Authors:** Fabio Bracci, Antonio Corradi, Luca Foschini

**Published in:** *University of Bologna, IEEE, 2012*

---

### Key Takeaways

This research explores **data security management in cloud-based healthcare Software as a Service (SaaS) applications**, focusing on Amazon AWS. It highlights **security risks, encryption gaps, and solutions** to ensure **safe medical data storage and transmission**.

### What We Use

#### 🔷 Security Challenges in Cloud-Based Healthcare SaaS

- SaaS applications provide **ubiquitous access to healthcare data**, improving **patient monitoring and remote care**.
- However, **data privacy risks** arise due to:
  ✅ **Unauthorized access** to patient data.
  ✅ **Insufficient encryption mechanisms** in AWS databases.
  ✅ **Limited security key management** in AWS cloud services.
- Your project should **address these gaps by implementing strong encryption and role-based access controls (RBAC)**.

#### 🔷 AWS Security Deficiencies & Required Enhancements

- The research highlights that **AWS does not provide built-in at-rest encryption** for databases.
- **Solution:**
  ✅ Use **MySQL native encryption** for **storing patient data securely**.
  ✅ Implement **third-party key management services** to **protect encryption keys**.
- Your project should **incorporate an advanced encryption model** for **securing cloud-hosted patient records**.

#### 🔷 Encryption Models for Healthcare SaaS Security

- The study evaluates **three encryption approaches**:
  ✅ **Transparent Data Encryption (TDE):** Encrypts **entire databases automatically**.
  ✅ **Column-Level Encryption:** Encrypts **specific sensitive fields** (e.g., patient names, diagnoses).
  ✅ **Application-Level Encryption:** Encrypts data **before storing it in the cloud**.
- Your project can **combine TDE with column-level encryption** to **enhance security without sacrificing performance**.

🔷 **Role-Based Access Control (RBAC) for Secure Data Access**

- The research suggests **RBAC for multi-user environments**, where:
  ✅ **Doctors access medical records but cannot modify billing data**.
  ✅ **Nurses access prescriptions but not patient financial information**.
  ✅ **Administrators manage system settings without seeing patient details**.
- Your project should **implement RBAC to control access to patient data based on roles**.

🔷 **Performance Testing of Encrypted Healthcare Databases**

- The study benchmarked **database performance with and without encryption**, finding:
  ✅ **Minimal performance impact (1-2% overhead) for column-level encryption**.
  ✅ **Significant slowdown (5-10% latency) when encrypting entire databases**.
- Your project should **test encryption speed and optimize database queries to maintain real-time access**.

---

**What We Gained**

**✓ Understanding the Security Challenges in AWS-Based Healthcare SaaS**

- Confirms that **AWS lacks built-in at-rest encryption for healthcare data**, requiring **custom encryption implementations**.

**✓ Guidance on Choosing the Right Encryption Model**

- Suggests using **a hybrid encryption approach (TDE + column-level encryption)** for **securing patient data**.

**✓ Validation of Role-Based Access Control (RBAC) for Healthcare Security**

- Confirms the **importance of limiting access to sensitive patient records based on user roles**.

**✓ Performance Benchmark for Cloud-Based EMRs**

- Helps **compare encryption techniques** and **evaluate their impact on system performance**.