

Project Report on

Implementing Data Security on EHR Using Hybrid Cryptography.

Submitted in partial fulfilment of the requirements
of the degree of

BACHELOR OF ENGINEERING

In

INFORMATION TECHNOLOGY

by

Dipak AvtarSingh Bisht (213143)

Deepak Indrajeet Sharma (213185)

Meet Santosh Todankar (213190)

Under the guidance of

Prof. Sneha Sankhe



Department of Information Technology

Theem College of Engineering, Boisar.

Boisar Chilhar Road, Boisar (E), Palghar

University of Mumbai

2023-2024

CERTIFICATE

This is to certify that the project entitled “**Implementing Data Security On EHR Using Hybrid Cryptography**” is a bonafide work of “**Dipak Bisht (213143), Deepak Sharma (213185), Meet Todankar (213190)**” submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of “**Bachelor of Engineering**” in “**Information Technology**”.

Prof. Sneha Sankhe
Guide

Prof. Sonali Karthik
Project Coordinator

Prof. Sneha Sankhe
Head of Department

Dr. Riyazoddin Siddiqui
Principal

Project Report Approval for B. E.

This project report entitled *Implementing Data Security on EHR Using Hybrid Cryptography* by *Dipak Bisht(213143)*, *Deepak Sharma(213185)*, *Meet Todankar(213190)* is approved for the “**Bachelor of Engineering**” in “**Information Technology**”.

INTERNAL EXAMINER

EXTERNAL EXAMINER

Date:

Place:

Declaration

We declare that this written submission represents our ideas in own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Dipak AvtarSingh Bisht (203105)

Deepak Indrajeet Sharma (203111)

Meet Santosh Todankar (203112)

Date:

Acknowledgement

We would like to take this opportunity to express our gratitude towards all the people who have in various ways, helped in the successful completion of our project. We would like to express our deepest gratitude to our honourable director sir **Dr. N. K. Rana** for their invaluable guidance, support, and mentorship throughout the duration of this project. Their expertise, encouragement, and insightful feedback have been instrumental in shaping the direction and outcome of this endeavor. We extend our gratitude to our respected principal sir **Dr. S. Riyazoddin Siddhiqui** for their continuous support and dedication to the holistic development of students, providing invaluable resources and opportunities for growth. We convey our gratitude to our HOD and project guide **Prof. Sneha Sankhe** and our major project Coordinator **Prof. Sonali Karthik** for giving us the constant source of inspiration and help in preparing the project, personally correcting our work and providing encouragement throughout the project. Additionally, we extend our appreciation to all the teaching staff, whose profound knowledge, passion for teaching, and dedication to students' learning have been a constant source of inspiration and motivation. We are also thankful to all the non-teaching staff, for their behind-the-scenes efforts in maintaining the infrastructure, administrative support, and logistical assistance that contributed to the project's success. We would also like to thank our parents, whose unwavering love, encouragement, and sacrifices have been the cornerstone of our journey. Their belief in our abilities and endless support have been a constant source of strength and motivation. Finally, we are grateful to our family and friends, for their understanding, encouragement, and unwavering support throughout this endeavor. We extend our heartfelt gratitude to each and every individual mentioned above, as well as to all those who have contributed in various ways, directly or indirectly, to this project's completion."

Dipak AvtarSingh Bisht (213143)

Deepak Indrajeet Sharma (213185)

Meet Santosh Todankar (213190)

Abstract

The development of electronic health records (EHR's) for patient monitoring is a concept widely adopted in the field of healthcare industry. Through this considerable web app patients can communicate with respective doctors and consult them for their disease diagnosis. This helps them to keep a track of their medical records in a digital and electronic form. However, the data uploaded on the EHR is huge in terms of volume, as multiple patients might try to access them. In such a scenario the data so collected might undergo certain attacks and breaches due to the vulnerability of the system model which might even lead to power failure of data stored on the respective EHR. Therefore, in this report, we propose the implementation of two encryption algorithms that would help to secure the data being transferred on the EHR. For this purpose, a Hybrid Cryptographic Technique (HCT) is used that includes the execution of AES, RSA and Serpent Algorithm. Using the mentioned HCT, the informational exchange is expected to be secured on cloud. The Advanced Encryption Standard (AES) is lauded for its efficiency in protecting data through its symmetric encryption approach. RSA, an asymmetric encryption scheme, enhances security by leveraging complex mathematical relationships. This innovative amalgamation safeguards medical records from unauthorized access, cyber-attacks, and potential power-related incidents, reinforcing the confidentiality and integrity of sensitive healthcare data. The marriage of encryption methodologies thus presents a significant stride toward ensuring the safety and privacy of patient information in the evolving landscape of healthcare technology.

The organization of this report is as follows.

Chapter 1: Introduction

This chapter gives a brief introduction about Electronic health Record using hybrid Cryptography Furthermore includes Motivation, Problem definition, Aim and Scope of the project.

Chapter 2: Literature survey

This Chapter divided in two sections; first one is background of the project which includes background study for the literature review prepared for building the EHR system and understanding the methodology

Chapter 3: System Architecture and Design

This chapter provides implementation details of the project in system design which gives information about the necessary things required for project implementation. It also provides information regarding the proposed system architecture to understand the project.

Chapter 4: System Design

This chapter presents different diagrams like Use-Case diagram, Data Flow diagram, Activity diagram, Sequence diagram, etc. to understand connectivity and flow of various activities.

Chapter 5: Results and Discussion

This chapter contains the screenshots of the project output and the results of the project.

Chapter 6: Conclusion and Future scope

This chapter presents the lessons learned represented with the conclusion and the area where work can be further carried out in further represented with future scope.

Sr. No	Contents	Pg. No
	List of contents.....	i
	List of Figures.....	iii
	List of Tables.....	v
	Acronyms.....	vi
Chapter -1	Introduction.....	1
1.1	An overview.....	1
1.2	Motivation.....	2
1.3	Problem Definition.	2
1.4	Aim	3
1.5	Scope	3
Chapter -2	Literature survey	4
2.1	Background.....	4
2.2	Analysis Table.....	7
Chapter -3	System Architecture	9
3.1	Introduction.....	9
3.2	Design.....	10
3.2.1	Requirement Analysis.....	10
3.3	System Architecture (Model Design)	11
3.4	Proposed System.....	12
3.5	Algorithms	13

Chapter -4	System design.....	15
4.1	Introduction.....	15
4.2	Uml Diagrams.....	16
4.2.1	Use Case Diagram.....	16
4.2.2	Class Diagram	17
4.2.3	Activity Diagram.....	18
4.2.4	Sequence diagram.....	17
4.3	Data Flow diagram.....	21
4.4	Gantt Chart.....	22
4.5	Work Breakdown Structure.....	23
Chapter-5	Result and Discussion.....	24
Chapter-6	Conclusion and Future Scope.....	35
	References.....	37

List of Figures

Sr. No	Figures	Pg. No
Fig. 3.1	System Architecture.	11
Fig. 3.2	Proposed System.....	12
Fig. 4.1	Use Case Diagram.....	16
Fig. 4.2	Class Diagram.....	17
Fig. 4.3	Activity Diagram.....	18
Fig. 4.4	Sequence Diagram.....	20
Fig. 4.5	Data Flow Diagram.....	21
Fig. 4.6	Gantt Chart.....	22
Fig. 4.7	Work Breakdown Structure.....	23
Fig. 5.1	Signup Page for EHR system.....	25
Fig. 5.2	Login Page for Doctor.....	26
Fig. 5.3	Doctor Side for Managing Patient Data.....	27
Fig. 5.4	Doctor Side for Adding Patient Data for registration.....	28
Fig. 5.5	Doctor Side for Managing File of Patient.....	29
Fig. 5.6	Doctor Side to Download Patient uploaded Report	30
Fig. 5.7	Downloading and Viewing the report matching with Shared Key	31

Fig. 5.8	Patient Side for Logging into Patient Panel.....	32
Fig. 5.9	Patient Side for Sharing their medical Report	33
Fig. 5.10	Patient Side for Viewing their medical Report updated via..... Doctor Side	34

List of Table

Sr. No	Figures	Pg. No
Table. 2.1	Table Analysis.	7
Table. 3.1	Requirements Table.....	10

Acronyms

EHR: ELECTRONIC HEALTH RECORD

HCT: HYBRID CRYPTOGRAPHY TECHNOLOGIES

AES: ADVANCED ENCRYPTION STANDARD

RSA: RIVEST, SHAMIR, ADLEMANS

Chapter 1

Introduction

1.1 An overview

Implementing data security for Electronic Health Record (EHR) data is of vital importance to ensure patient privacy, and the integrity of sensitive medical information. Hybrid cryptography is a robust approach that combines the strengths of both symmetric and asymmetric encryption methods to achieve a high level of data security. Integrating hybrid cryptography for Electronic Health Record (EHR) data safeguards patient information, and upholds data integrity. This method employs symmetric encryption for efficient data protection and asymmetric encryption for secure key exchange. By uniting these techniques, healthcare providers can establish a comprehensive and adaptable security framework for safeguarding sensitive medical records.

1.2 Motivation

In the domain of healthcare, safeguarding Electronic Health Record (EHR) data is vital to preserve patient privacy, and maintain the integrity of critical medical information. The motivation behind employing hybrid cryptography lies in its innovative fusion of symmetric and asymmetric encryption methods. By integrating the efficiency of symmetric encryption with the robustness of asymmetric encryption, healthcare institutions can construct a formidable security shield. This ensures that patient records remain confidential, unaltered, and accessible only to authorized personnel. This approach not only secures data protection but also demonstrates a proactive commitment to ethical medical practices. By mitigating the risks associated with data breaches and unauthorized access, hybrid cryptography empowers healthcare providers to advance patient care while upholding the highest standards of data security.

1.3 Problem Definition

The problem addressed by implementing data security on Electronic Health Record (EHR) using hybrid cryptography centres around the vulnerability of sensitive medical information. Traditional security measures often fall short in ensuring patient privacy, data integrity, and regulatory compliance. The challenge lies in developing an effective method that prevents unauthorized access, data breaches, and tampering while accommodating the complexities of healthcare data management. This requires overcoming the limitations of single encryption methods and establishing a solution that balances the efficiency of symmetric encryption with the secure key exchange of asymmetric encryption. The problem definition involves creating a robust security framework that safeguards EHR data from diverse threats while facilitating seamless access for authorized entities in accordance with healthcare regulations

1.4 Aim of Project

The primary objective of implementing data security on Electronic Health Record (EHR) data using hybrid cryptography is to ensure the utmost confidentiality, integrity, and availability of sensitive medical information. By seamlessly integrating both symmetric and asymmetric encryption techniques, this approach aims to establish a robust and efficient security framework that not only aligns with regulatory standards addresses the unique challenges of healthcare data management. Through the strategic use of symmetric encryption for data protection and asymmetric encryption for secure key distribution, the goal is to create a comprehensive security infrastructure that safeguards patient privacy, prevents unauthorized access, and maintains the trustworthiness of EHR systems.

1.5 Scope of Project

The scope of implementing data security on Electronic Health Record (EHR) using hybrid cryptography encompasses a comprehensive approach to reinforce healthcare data systems. By integration of symmetric and asymmetric encryption, this strategy ensures the confidentiality, integrity, and availability of sensitive patient information. It extends to secure key generation, efficient data encryption, and seamless decryption processes. This approach accommodates the scalability demands of modern healthcare while addressing the evolving threat framework. Ultimately, the scope of implementing hybrid cryptography in EHR data security spans across technological, regulatory, and ethical dimensions to establish a robust and adaptable safeguarding.

Chapter 2

Literature Survey

2.1 Background

Within the setting of healthcare, Electronic Health Record (EHR) information security has risen as a basic concern due to the expanding digitization of understanding records and the potential dangers related with unauthorized get to, information breaches, and security violation. Conventional encryption strategies frequently confront challenges in productively securing tremendous volumes of protect health information whereas assuring authorized get to. This foundation sets the organize for the selection of half-breed cryptography, which combines the qualities of symmetric and varied encryption. Symmetric encryption gives speed and proficiency, whereas deviated encryption addresses secure key trade.

2.2 Paper Reviewed

[1] Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud.

Authors: R. Manoj , Abeer AL Sadoon , P.W.C. Prasad , Nectar Costadopoulos , Salih

In this paper, a Hybrid Secure and Scalable Electronic Health Record Sharing (HSS-EHRS) system, whereby two cryptographic methods are utilized for providing a flexible, secure and fine grained access to EHR files in hybrid cloud. The proposed framework divides the system into two security domains and utilizes an ABE encryption scheme to encrypt the EHR files. The proposed system proved its efficiency based on encryption time and concurrent recipient data access and sharing. The enhanced MA-ABE encryption scheme is capable of handling on demand recipient data access and providing high levels of security.

[2] Attribute Based Encryption For Secure Access to Cloud Based EHR System

Authors: Maithilee Joshi, Karuna P Joshi, Tim Finin

In this paper we developed an attribute based, field level, document encryption for managing the access and data security of cloud-based EHRs. In our approach we designed and developed a complex knowledge graph that details the roles and attributes of different stakeholders of the medical organization along with the various relationships between them. We also developed an open-source, easy to use user interface

[3] A Systematic Review of the Security in Cloud Computing, Data Integrity, Confidentiality and Availability

Authors: Rajikumar, M P.S Bhatia

The existing method in cloud security to evaluate the three main parameters such as integrity, authentication and confidentiality. To improve each aspect various methods is need to incorporate that are different from traditional security system on data transfer or file storage system. The summarized the existing method progress up to data and provides future scope of the method. The cloud storage security system requires the effective method to overcome the issues such as data leakage, insecure transmission and access credentials.

[4] Design of Secure storage For Cloud Using Hybrid Cryptography

Authors: P.Chinnasamy, P.Deepa Laxmi

For storing health-related data in cloud storage, data is encrypted by Blowfish and keys are managed using the enhanced RSA algorithm. This hybrid method offered the benefits like fast encryption, large prime numbers for key generation and efficient key management. The simulation results clearly show that encryption and decryption time of proposed hybrid technique is better than other methods considered for comparison.

[5] Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment

Authors: Wang Xiaoyu, Gao Zhengming

To solve the problem of cloud computing security, this paper presents the data security protection system based on the data security technology and infrastructure security of personnel, network and cloud, and puts forward the corresponding security technology and strategy. Aiming at the security problems of the internal personnel of cloud service providers that are easy to be ignored, this paper puts forward the identity authentication and role-based access control strategies based on account and certificate, analyzes and studies the cloud security standards and legal maintenance, and puts forward the cloud security assessment system and relevant legal suggestions and measures to provide a strong guarantee for data security protection.

2.3 Analysis Table

Table 2.1: Analysis Table

Sr. no	Paper Title [Reference]	Author	Advantages	Drawbacks
1.	Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud	R. Manoj , Abeer AL Sadoon , P.W.C. Prasad , Nectar Costadopoulos , Salih Ali	Advantage of the strengths of both methods. Symmetric encryption provides fast and efficient encryption for data, while asymmetric encryption ensures secure key exchange and protects against unauthorized access.	Implementing hybrid cryptography requires careful integration of symmetric and asymmetric encryption mechanisms. This complexity could introduce potential vulnerabilities if not implemented correctly
2.	Attribute Based Encryption for Secure Access to Cloud Based EHR Systems	Maithilee Joshi, Karuna P. Joshi and Tim Finin	ABE encrypts data based on attributes, ensuring only authorized users with matching attributes can access it, even in less secure cloud settings.	Handling keys and attributes, especially for many users, requires careful management to prevent leaks
3.	A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability	Rajeev Kumar,M P S Bhatia	The systematic review provides an in-depth analysis of security aspects (data integrity, confidentiality, availability) in cloud computing. It covers a wide range of research, enabling a holistic view of security challenges and solutions	Cloud security varies across providers, services, and deployment models. The review might struggle to capture the nuances of different cloud environments

Sr.no	Paper Title [Reference]	Author	Advantages	Drawbacks
4.	Design of Secure Storage for Cloud using Hybrid Cryptography	P.Chinnasamy, P. Deepa Lakshmi	Achieves fast data encryption using symmetric encryption for large datasets .	Requires effective management of both symmetric and asymmetric keys.
5.	Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment	Wang Xiaoyu, Gao Zhengming	With a cloud-based security system, organizations can centrally manage and monitor their data security measures	A data security multidimensional protection system in a cloud computing environment may still be vulnerable to sophisticated cyber-attacks or insider threats, requiring continuous monitoring and proactive threat detection.

Chapter 3

System Architecture

3.1 Introduction

The aim of the proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss.

For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

3.2 Design

After the requirements have been determined, the necessary specification for the hardware, software, people, data resources, and the information products that will satisfy the functional requirements of the proposed system can be determined. The design will serve as a blue print for the systems and helps to detect these problems before these errors or problems are built into the final system.

3.2.1 Requirement Analysis

Below mentioned names of hardware and software is used for making and creating the report and presentation of the project.

3.1 Requirement Table

Hardware Requirement	Software Requirement
1 GB RAM.	Operating System: Microsoft Windows 7,8,10
200 GB HDD	Microsoft .Net Framework
Intel 1.66 GHz Processor Pentium	Visual Studio2022
	MS Sql2018

3.3 System Architecture

The aim of the proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so.

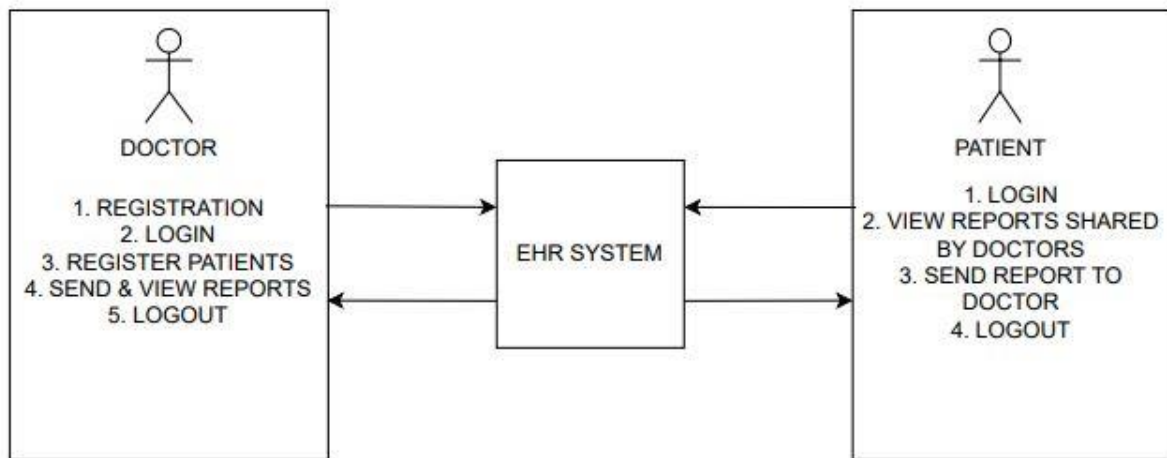


Fig 3.1: System Architecture of EHR system using HCT

To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss. For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

3.4 Proposed System

The primary aim of the research methodology is to develop a patient health care system wherein the patient and doctor could communicate with each other over cloud using MS Azure. This communication between both the parties thus involved, comprises of sharing of patient information such as his disease and necessary parameters.

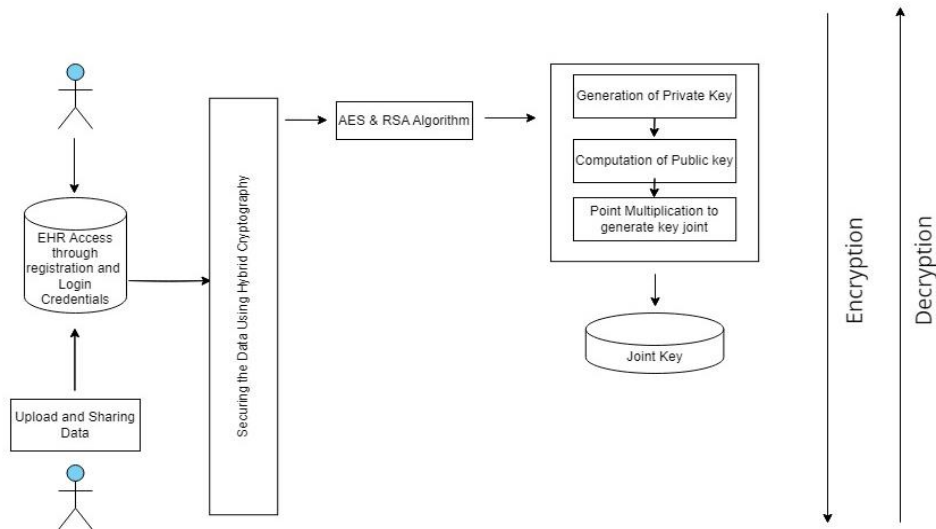


Fig 3.2: Proposed System of EHR system using HCT

The information also includes sugar levels, blood pressure, oxygen saturation etc. The doctor and the patient can login on the portal using their credentials which were initially used during their registration process. The overall implementation of the research is executed on two ends and thereby can be accessed by two separate individuals thus involved. In the proposed thesis; the two communicating parties is the doctor and the patient. They can thus individually login using their ID and passwords. Apart from the exchange of information between the communicating parties; securing, storing and retrieving the shared information on cloud is mandatory. For this reason, the authors have implemented the conceptual theories of cryptography that makes use of symmetric and asymmetric encryption techniques. The upload of data that takes place on the doctor's end is where the process of encryption takes place, the download of data on the patient's end is where the process of decryption takes place. For the purpose of encryption, we have used RSA algorithm whereas for the purpose of decryption, we

have used the AES algorithm. It is worthy to note here that once the keys are generated; they are communicated using a secure channel through Gmail ID of the registered user.

In addition to the execution of the thesis; it is simultaneously important to assess and evaluate the system model so that the levels of security could be maintained. This ensures that the time and phase complexities are eventually balances and thereby generated in conjunction so that the model can accomplish higher levels of security. For this to occur; the length and sizes of the keys thus generated must match with the system model so that parsing of keys could be performed. The workflow of the same can be depicted from the schematic diagram illustrated above Figure 3.2

3.5 Algorithm

RSA- (Rivest, Shamir, Aldmen)

Step 1. Key Generation: Choose two large prime numbers, p and q .

Step 2. Compute n : Multiply p and q to get n ($n = p * q$).

Step 3. Calculate $\phi(n)$: Compute Euler's totient function $\phi(n) = (p-1) * (q-1)$.

Step 4. Choose an e : Select a public exponent e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

Step 5. Calculate d : Find the modular multiplicative inverse of e ($d * e \equiv 1 \pmod{\phi(n)}$).

Step 6. Public Key: The public key is (n, e) .

Step 7. Private Key: The private key is (n, d) .

Encryption:

Step 8. To encrypt a message M , compute $C = M^e \pmod{n}$.

Decryption:

Step 9. To decrypt the ciphertext C , compute $M = C^d \pmod{n}$.

Step 10. Message Recovery: You've decrypted the ciphertext to recover the original message.

These steps illustrate the core process of the RSA encryption and decryption algorithm.

AES- (Advanced Encryption Standard.)

Step 1. Key Expansion: Generate round keys from the initial encryption key.

Step 2. Initial Round (AddRoundKey): XOR the input data with the first round key.

Step 3. Main Rounds (SubBytes, ShiftRows, MixColumns, AddRoundKey): Apply a series of transformations to the data for multiple rounds.

Step 4. SubBytes: Replace each byte with a corresponding value from an S-box.

Step 5. ShiftRows: Shift bytes within each row.

Step 6. MixColumns: Combine data in each column using matrix multiplication.

Step 7. AddRoundKey: XOR the data with the round key for the current round.

Step 8. Final Round (SubBytes, ShiftRows, AddRoundKey): A final round without MixColumns.

Step 9. Decryption (Inverse Operations): Apply the inverse of the encryption operations using round keys in reverse order.

Step 10. Key Schedule for Decryption: Generate round keys for decryption.

Step 11. Inverse SubBytes, Inverse ShiftRows, Inverse MixColumns: Apply inverse transformations for decryption.

Step 12. Inverse AddRoundKey: XOR the data with the round key for decryption.

Step 13. Message Recovery: The decrypted data is the original message.

AES is a symmetric-key encryption algorithm, which means the same key is used for both encryption and decryption.

Chapter 4

System Design

4.1 Introduction

Electronic Health Records (EHR) are a vital component of modern healthcare systems, providing a digital repository for patient health information. Ensuring the security and privacy of this sensitive data is of vital importance to protect patient confidentiality, comply with regulatory requirements and maintain the integrity of healthcare operations. One of the most effective ways to achieve robust data security in EHR systems is through the use of hybrid cryptography. And the proposed system consist of PC/Laptop, VS code, and required tools for implementation.

4.2 UML diagrams

We use these diagrams for describing our system in a static and dynamic way that represents the modern approach to modelling and documenting software. It is based on dramatic representation of the software. UML diagrams are high level points, arguably the most important aspects of any design system and it is rapidly evolving and responsive software.

4.2.1 Use case Diagram

This Use Case diagram gives an idea about the behaviour of the system with respect to various actions performed by the proposed system. In this use case diagram, the focus is on the interactions between actors and the key functions that ensure data security in the EHR system using hybrid cryptography. It highlights the need for authentication, encryption, and decryption to protect sensitive patient data.

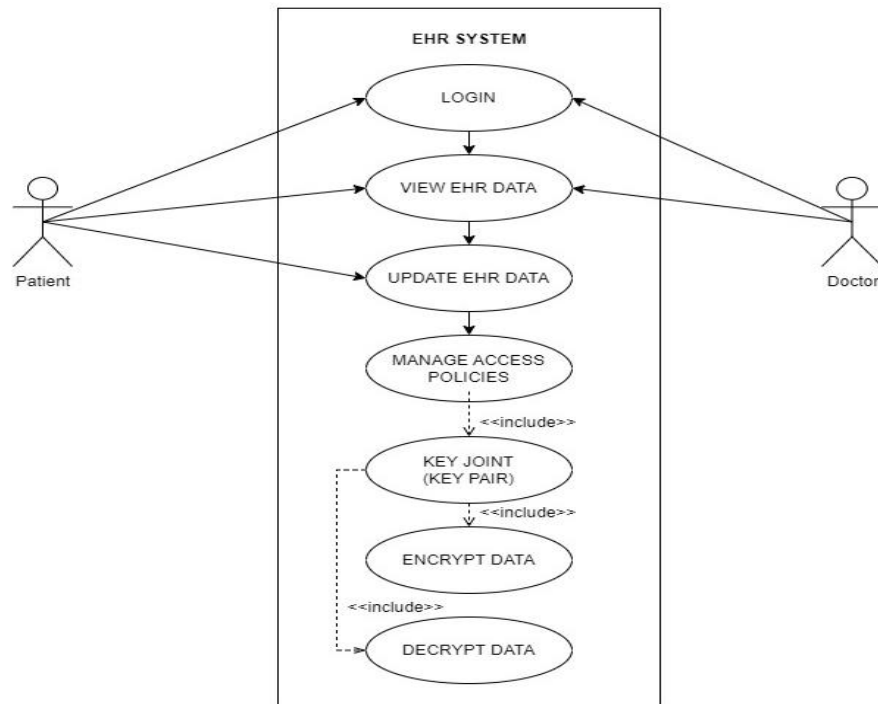


Fig 4.1: Use Case Diagram of EHR system using HCT

4.2.2 Class Diagram

A class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, The relationships between these classes would involve method calls and data flow, with the ultimate goal of ensuring data security within the EHR system by using hybrid cryptography techniques to protect patient data while allowing authorized users to access it securely.

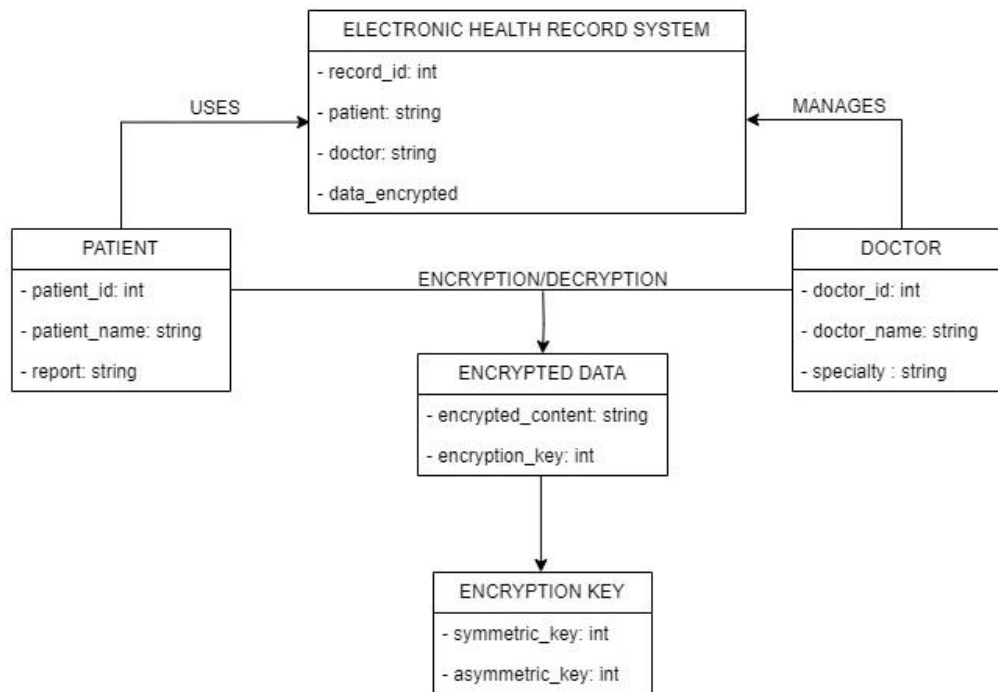


Fig 4.2: Class Diagram of EHR using HCT

Class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing, and documenting different aspects of a system but also for constructing executable code of the software application. The class diagrams are widely used in the modelling of object-oriented systems because they are the only UML diagrams, which can be mapped directly with object-oriented languages.

4.2.3 Activity Diagram

The activity diagram is another important behavioral diagram in the UML diagram to describe dynamic aspects of the system. activity diagram provides a visual representation of how data security is implemented in an EHR system using hybrid cryptography, highlighting the various steps involved in securing and managing electronic health records. It's a valuable tool for understanding the workflow and processes in such a security system.

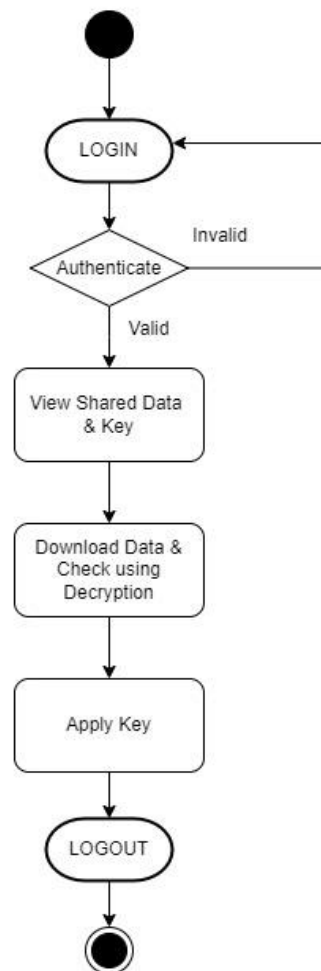


Fig 4.3.1: Activity Diagram for Doctor of EHR system using HCT

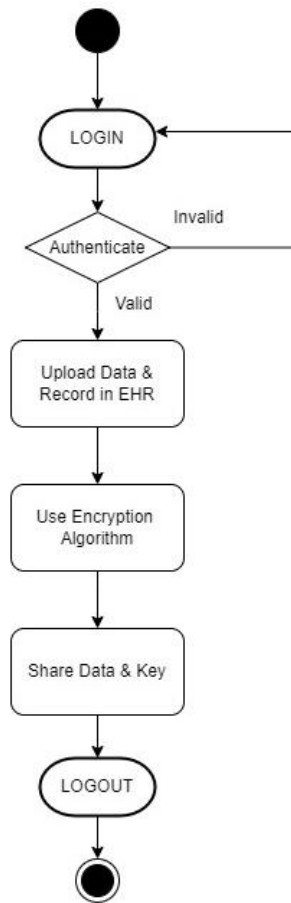


Fig 4.3.2: Activity Diagram for Patient of EHR system using HCT

The activity diagram is used to demonstrate the flow of control within the system rather than the implementation. It models the concurrent and sequential activities. The activity diagram helps in envisioning the workflow from one activity to another

4.2.4 Sequence Diagram

A sequence diagram is a type of interaction diagram in UML (Unified Modeling Language) that illustrates how objects or components in a system interact with each other over time. In the context of implementing data security in an Electronic Health Record (EHR) system and the Hybrid Cryptography Module when accessing patient data securely using a combination of symmetric and asymmetric cryptography. The use of a hybrid approach enhances data security in EHR systems by combining the efficiency of symmetric encryption with the security of asymmetric encryption.

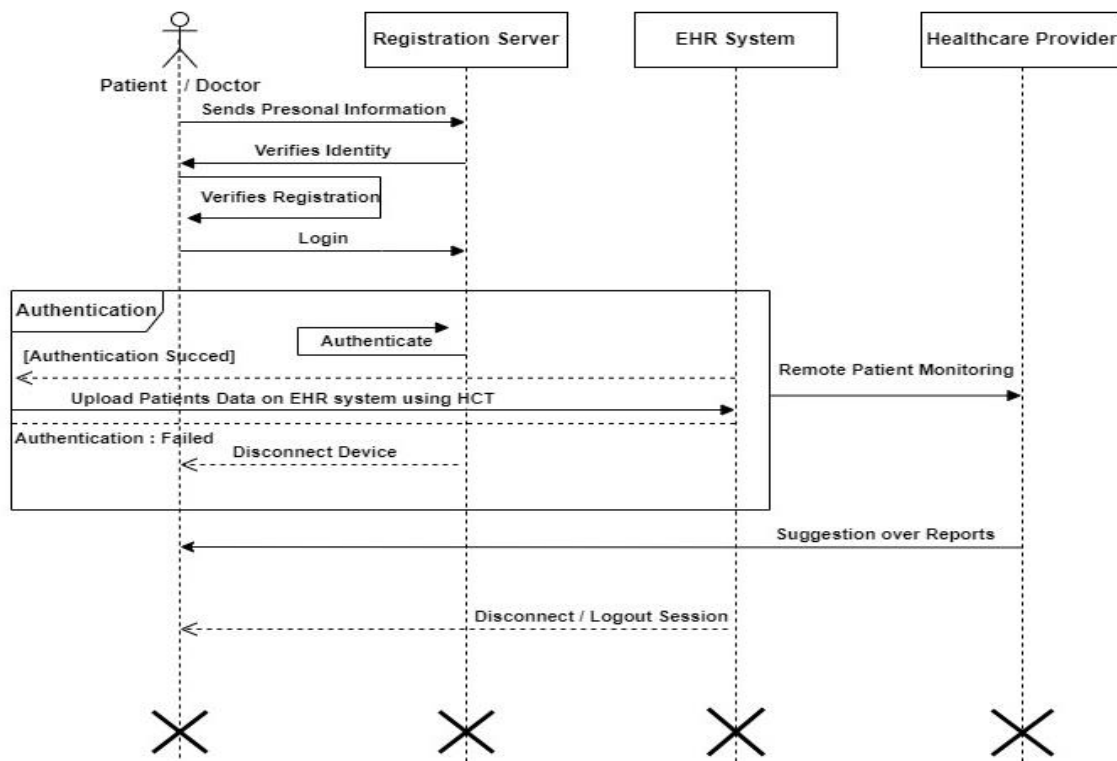


Fig 4.4: Sequence Diagram of EHR system using HCT

4.3 Data Flow Diagram

Data flow diagram is often used as an introductory step to create an overview. It consists of the overall application data flow and processes of the system. It contains all of the user flow and their entities such as sensor, Arduino.

Level 0 DFD

This is the level zero of the detection system, where we have involved the high-level process of this system, it's a basic overview of the whole system. In level zero we show the patient module

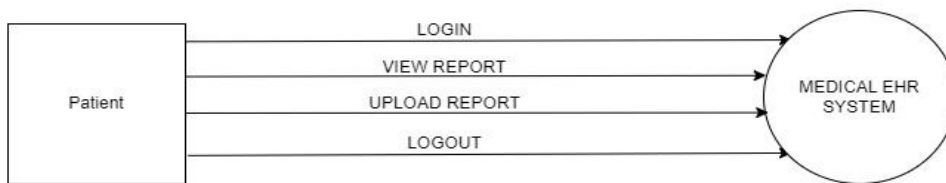


Fig 4.5: Level 0 DFD of HER using HCT

Level 1 DFD

Level one DFD shows how the system is divided into sub- systems (processes), each of which deals with one or more of the data flows to or from an external entity, which together provides all of the functionality of the DFD level 1 provides a more detailed breakout of piece of the Level 1 DFD. In level one we show the Doctor module

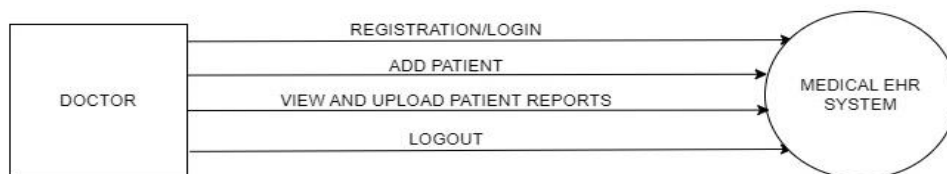


Fig 4.5.1: Level 1 DFD of EHR using HCT

4.5 Gantt Chart

A Gantt chart, commonly used in project management, is one of the most popular and useful ways of showing activities (tasks or events) displayed against time. On the left of the chart is a list of the activities and along the top is a suitable time scale. Each activity is represented by a bar; the position and length of the bar reflects the start date, duration and end date of the activity.

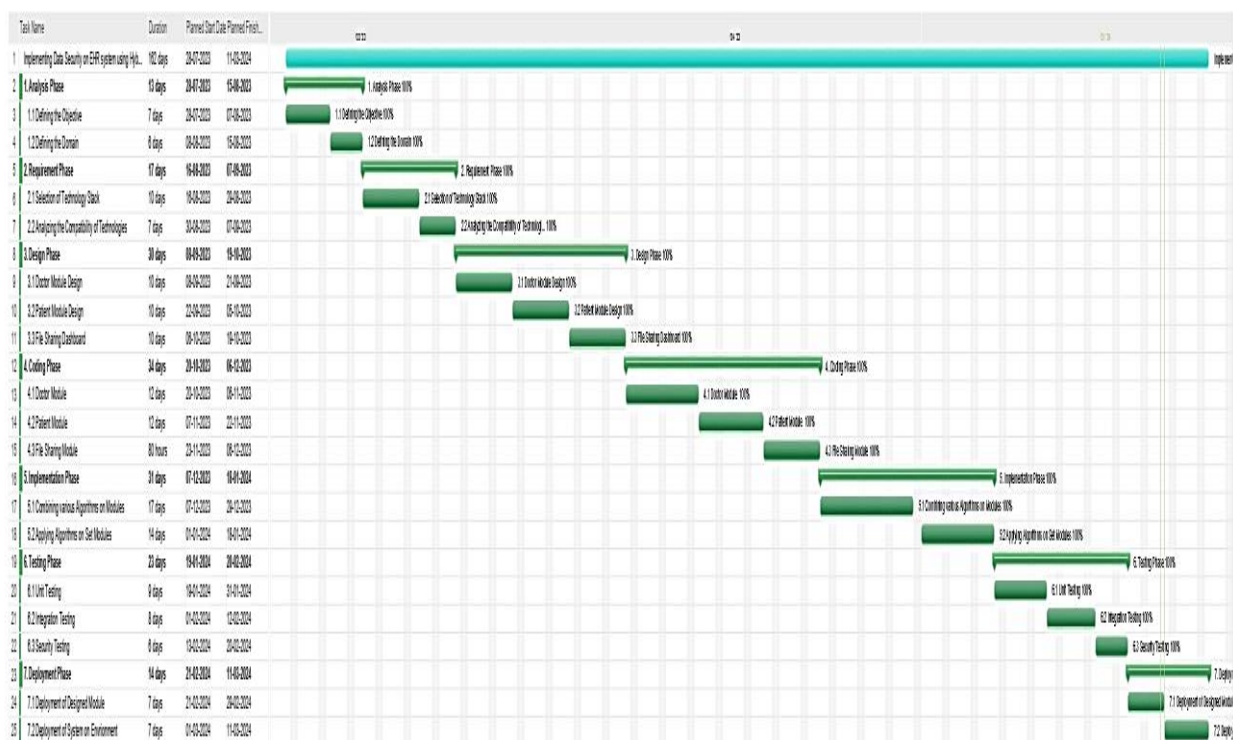


Fig 4.5: Gantt Chart of EHR using HCT

A Gantt chart is actually a project management tool or a bar chart that shows the schedule of a project. It also displays the work completed over a period of time. The above figure represents the Gantt chart of the project and which gives the schedule of our project.

4.6 Work Breakdown Structure Chart

A work breakdown structure (WBS) is a visual, hierarchical and deliverable-oriented deconstruction of a project. It is a helpful diagram for project managers because it allows them to break down their project scope and visualize all the tasks required to complete their projects. Making a WBS is the first step in developing a project schedule. It defines all the work that needs to be completed (and in what order) to achieve the project goals and objectives. By visualizing your project in this manner, you can understand your project scope, and allocate resources for all your project tasks.

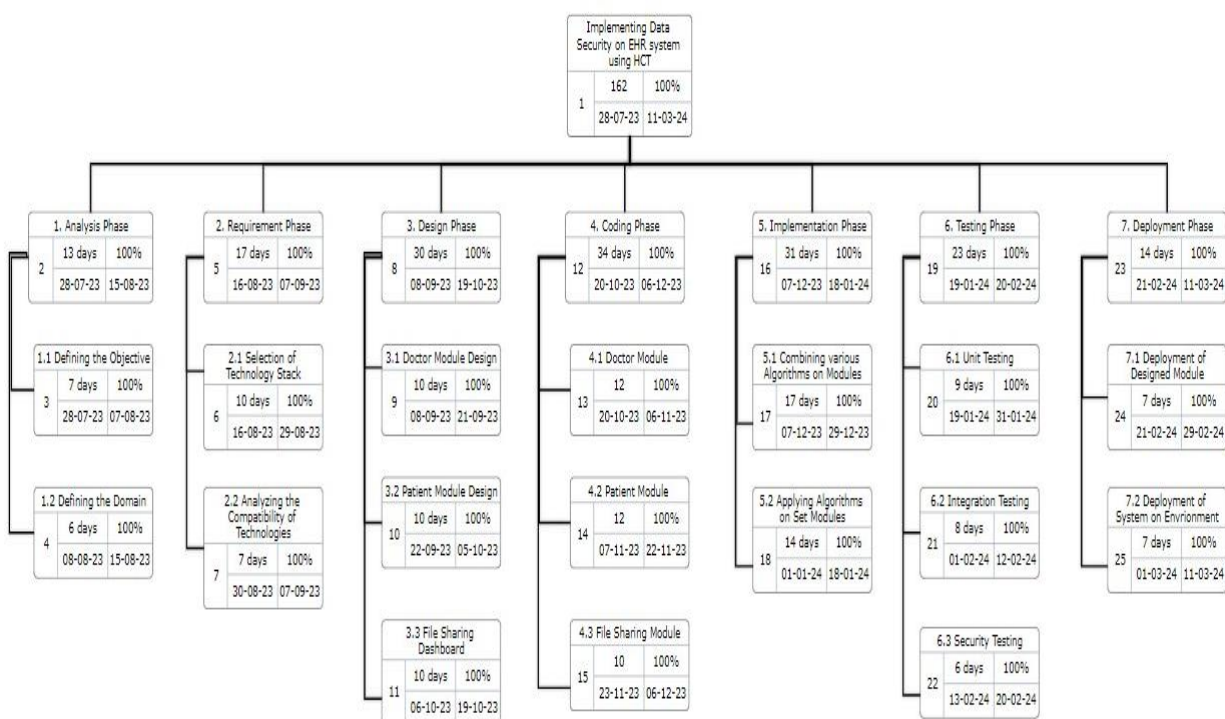


Fig 4.6: WBS Chart of EHR system using HCT

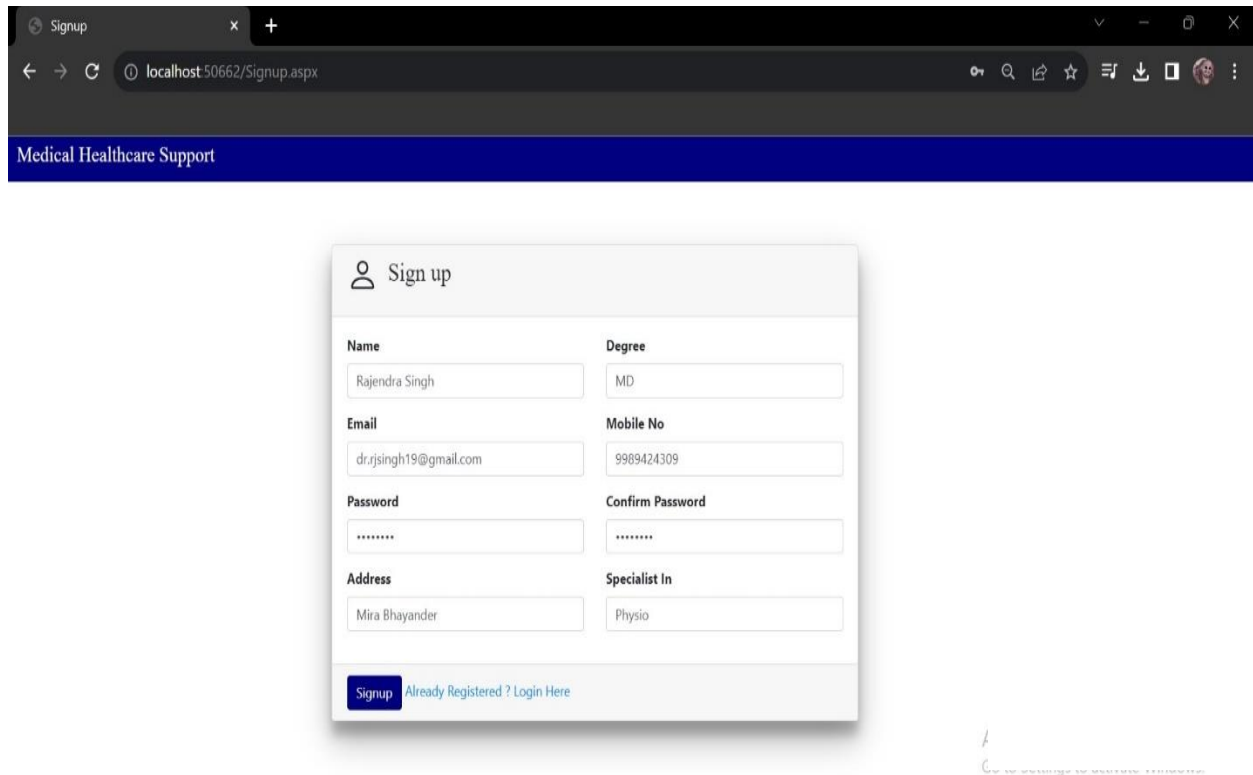
Chapter 5

Results and Discussion

Implementing hybrid cryptography in EHR systems has enhanced data security. This approach combines fast symmetric encryption with strong asymmetric encryption for encryption key protection, effectively reducing unauthorized access and data breaches. It ensures the confidentiality of patient records, facilitates secure data sharing, and enhances healthcare coordination while meeting regulatory compliance. Additionally, the use of digital signatures further strengthens data integrity and authentication, providing a comprehensive approach to safeguarding sensitive health information in EHR systems.

5.1 Signup Page for EHR system

The signup page for our EHR system provides a user-friendly interface for healthcare professionals to create accounts securely. Through a streamlined process, users can input their credentials, ensuring access to patient records while maintaining data security and regulatory compliance.



The image shows a web browser window with the address bar displaying 'localhost:50662/Signup.aspx'. The page title is 'Medical Healthcare Support'. Below the browser window, a modal form titled 'Sign up' is displayed. The form contains the following fields:

Name	Degree
Rajendra Singh	MD
Email	Mobile No
dr.rjsingh19@gmail.com	9989424309
Password	Confirm Password
*****	*****
Address	Specialist In
Mira Bhayander	Physio

At the bottom of the form, there is a blue 'Signup' button and a link that says 'Already Registered ? Login Here'.

Fig 5.1: Signup Page for EHR system

Fig 5.2, Illustrates the registration page for an Electronic Health Record (EHR) system, which serves both doctors and patients. Users provide their login credentials to establish accounts, which ensures safe access to sensitive medical information. The design promotes simplicity and efficiency, making the onboarding process easier for new users.

5.2 Login Page for Doctor

Our doctor login page offers a secure gateway for healthcare professionals to access patient data. Utilizing strong authentication measures, including username and password, it ensures confidentiality and regulatory compliance.

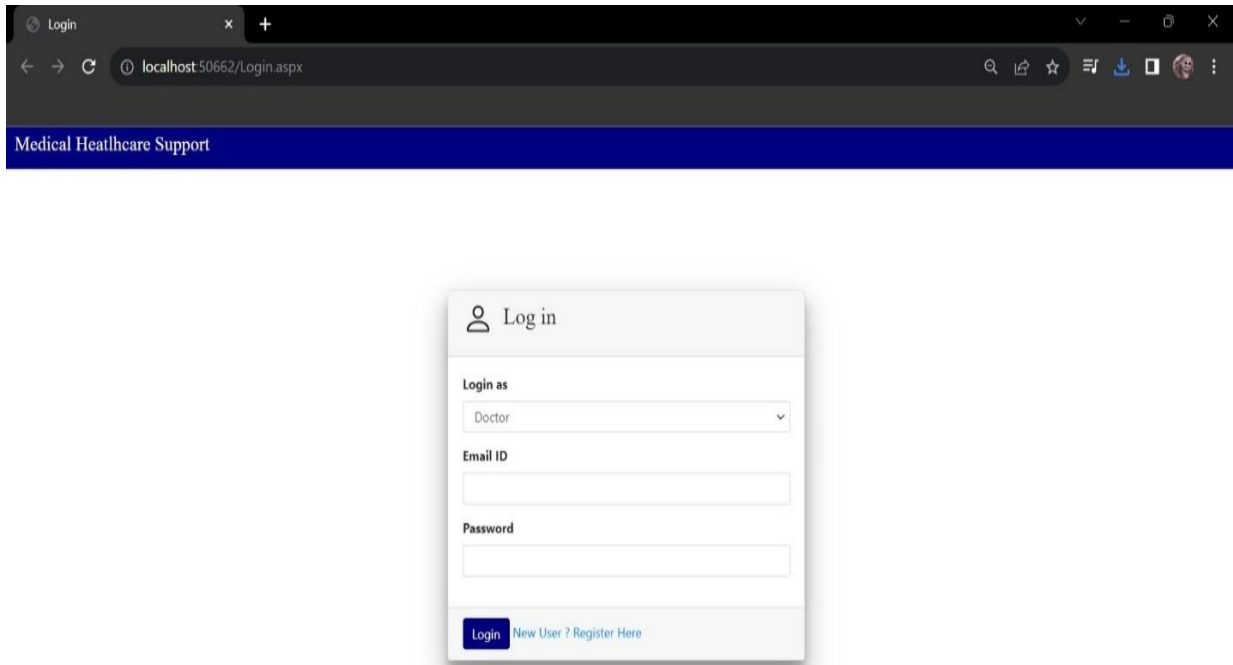


Fig 5.2: Login Page for Doctor and Patient

Fig 5.2, shows the login interface of an Electronic Health Record (EHR) system, which is particularly built for doctors to use the software. By entering their login credentials, doctors receive access to the specialized doctor panel. This simplified interface provides quick access to critical tools and patient information. It focuses on usability and functionality for medical professionals utilizing the EHR system.

5.3 Doctor Control panel

The module is anticipated to contain communication elements that will allow doctors to communicate directly with patients about their health issues. It gives clinicians the resources they need to provide tailored and effective patient care, encouraging a collaborative approach to healthcare management.

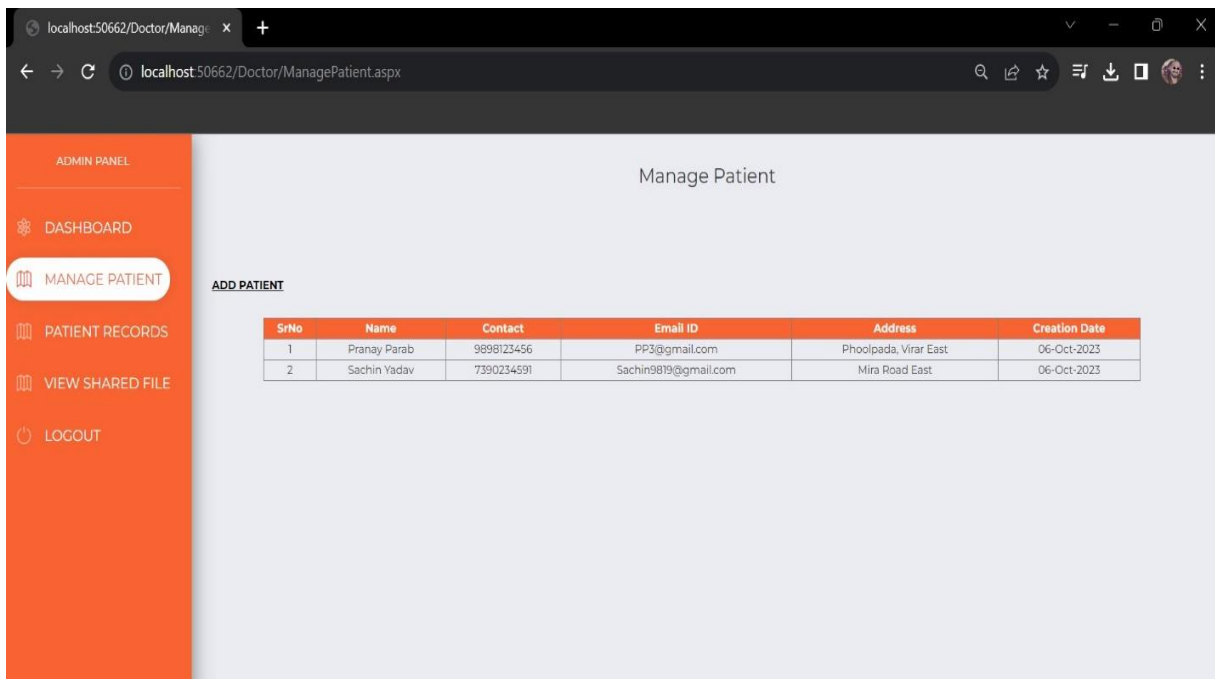
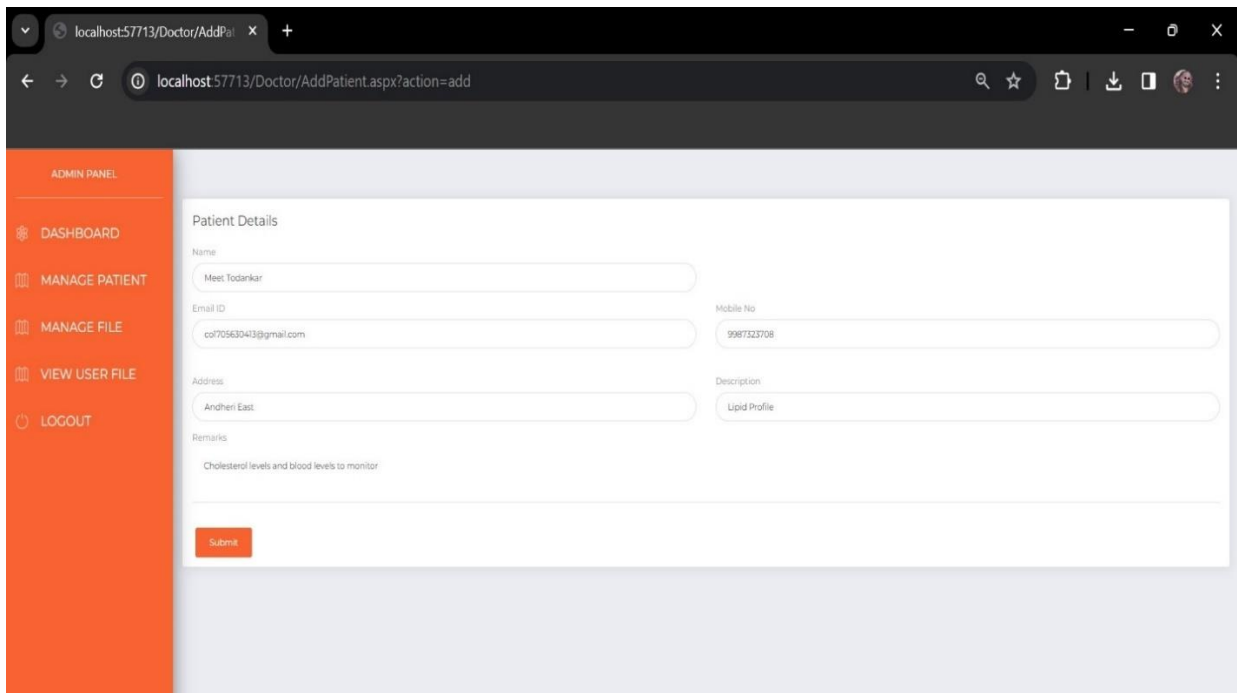


Fig 5.3: Doctor Side for Managing Patient Data

Fig 5.3, depicts the doctor-side module of the system, which provides clinicians with complete capabilities for monitoring and managing patient information. This interface allows clinicians to evaluate patient information, recommend drugs, and offer health advice. It provides a consolidated platform for clinicians to track patient development and make educated decisions about their treatment.

5.4 Adding Patient detail for registration

This ensures thorough patient information collection for effective healthcare management. Additionally, doctors can specify disease categories and note symptoms in the remarks section, facilitating precise diagnosis and treatment planning, thus optimizing healthcare delivery within the system.



The screenshot shows a web browser window with the URL `localhost57713/Doctor/AddPatient.aspx?action=add`. The interface features an orange sidebar on the left with the following menu items: ADMIN PANEL, DASHBOARD, MANAGE PATIENT, MANAGE FILE, VIEW USER FILE, and LOGOUT. The main content area is titled "Patient Details" and contains several input fields: Name (with the value "Meet Todankar"), Email ID (with the value "cd70563043@gmail.com"), Mobile No (with the value "9987323708"), Address (with the value "Andheri East"), and Description (with the value "Lipid Profile"). There is also a Remarks section with the text "Cholesterol levels and blood levels to monitor." and a red "Submit" button at the bottom.

Fig 5.4: Doctor Side for Adding Patient Data for registration

Illustrated in Figure 5.4, the doctor module facilitates the input of patient details, necessitating essential fields for registration. These include email address, mobile number, and address, ensuring comprehensive patient information. Furthermore, doctors can specify disease categories and note symptoms in the remarks section for precise diagnosis and treatment planning. This structured approach guarantees the inclusion of crucial patient data, enhancing the efficacy of healthcare management within the system.

5.5 Managing File of Patient

Managing patient files involves organizing, updating, and securely storing electronic health records. Through intuitive navigation and comprehensive features, our system ensures efficient access and management of patient information.

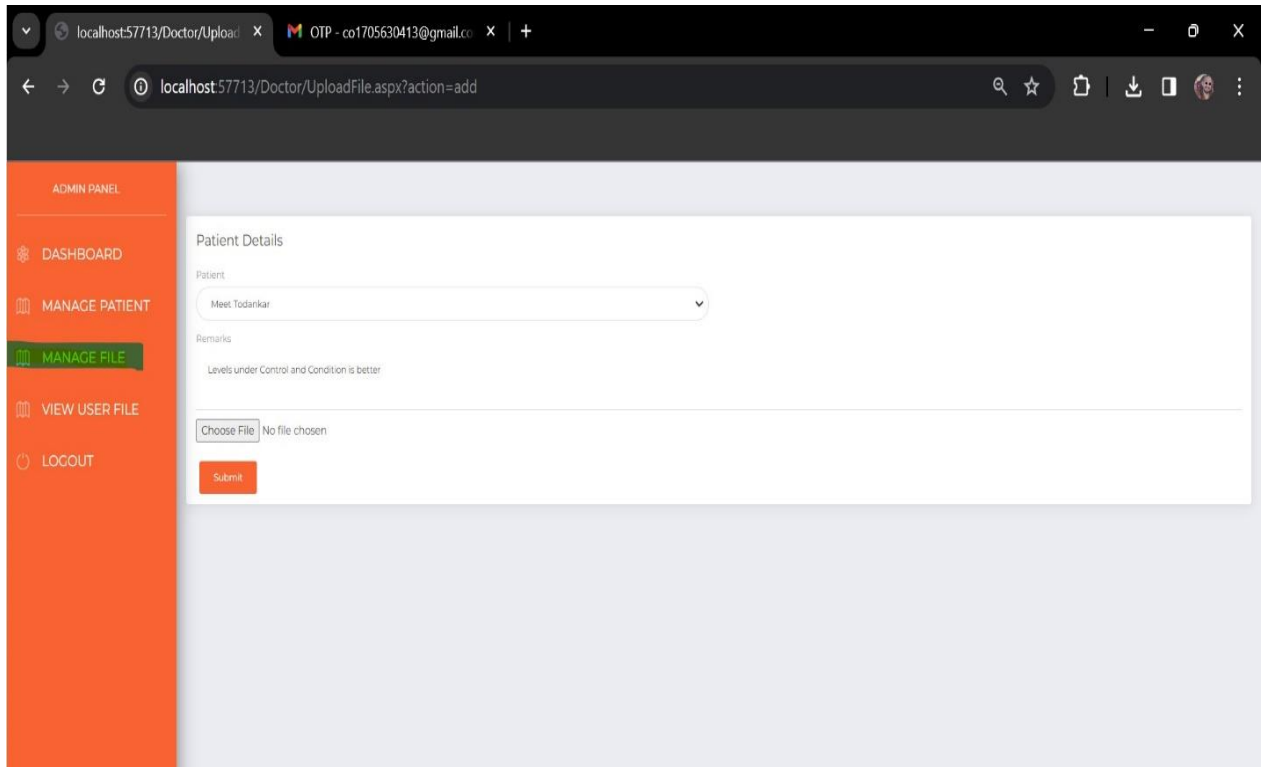


Fig 5.5: Doctor Side for Managing File of Patient

Referring to Figure 5.5, the doctor module allows seamless management of patient reports to be uploaded into the system. This functionality ensures that patients can access their historical reports on their side, contributing to data backup and the creation of comprehensive portfolios. The system facilitates a secure repository for past reports, enabling doctors to monitor patient health trends and make informed decisions. This feature enhances the overall efficiency of healthcare management by providing a centralized hub for organizing and accessing crucial patient data.

5.6 View User file and Download Report

The "View User File" feature allows authorized users to access patient records securely. With seamless functionality, users can review medical history, diagnoses, and treatment plans. Additionally, they can download comprehensive reports, promoting informed decision-making and collaborative healthcare efforts.

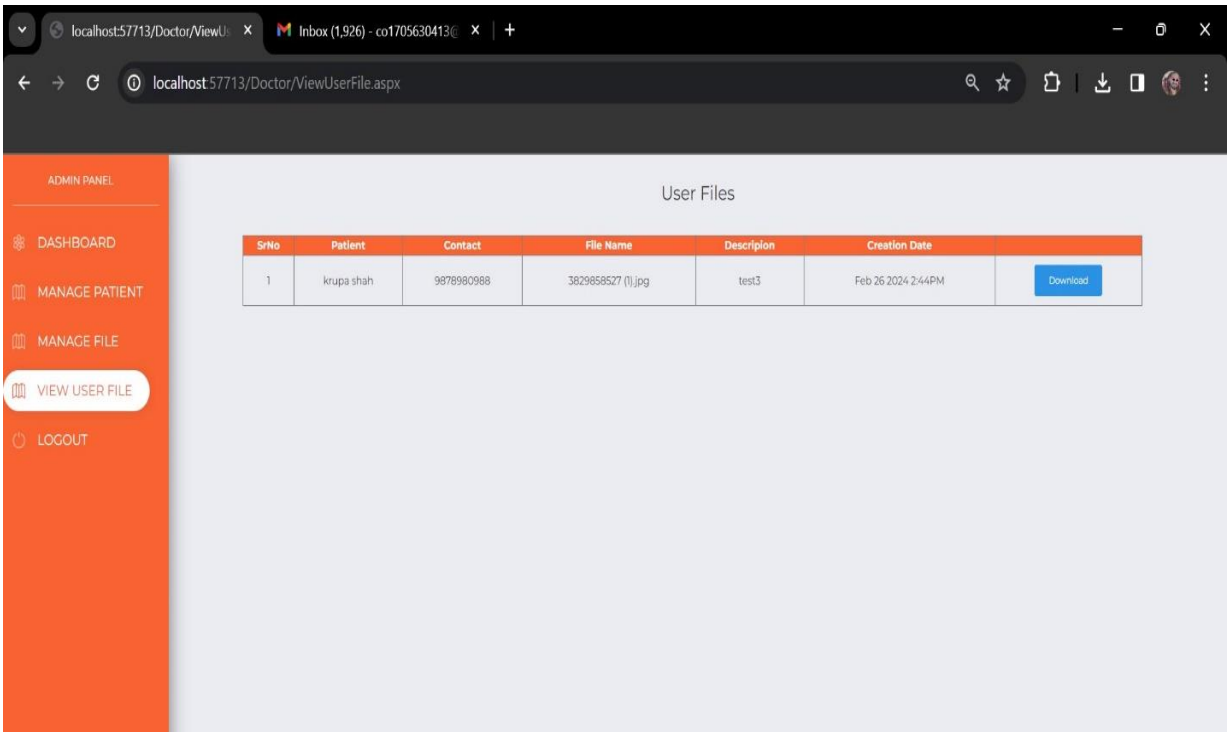


Fig 5.6: Doctor Side to Download Patient uploaded Report

Figure 5.6 is utilized in the doctor panel to download past medical reports uploaded by patients, showcasing their medical history. This allows doctors to review previous illnesses and treatments, aiding in comprehensive patient care. The process involves referencing a unique key provided via email for secure access to the reports, ensuring data privacy and integrity.

5.7 Doctor Side for Downloading and Viewing the report

Doctors can securely access patient reports for viewing and downloading through our platform's dedicated interface. This streamlined process ensures efficient retrieval of medical data, enabling informed decision-making and patient care planning.

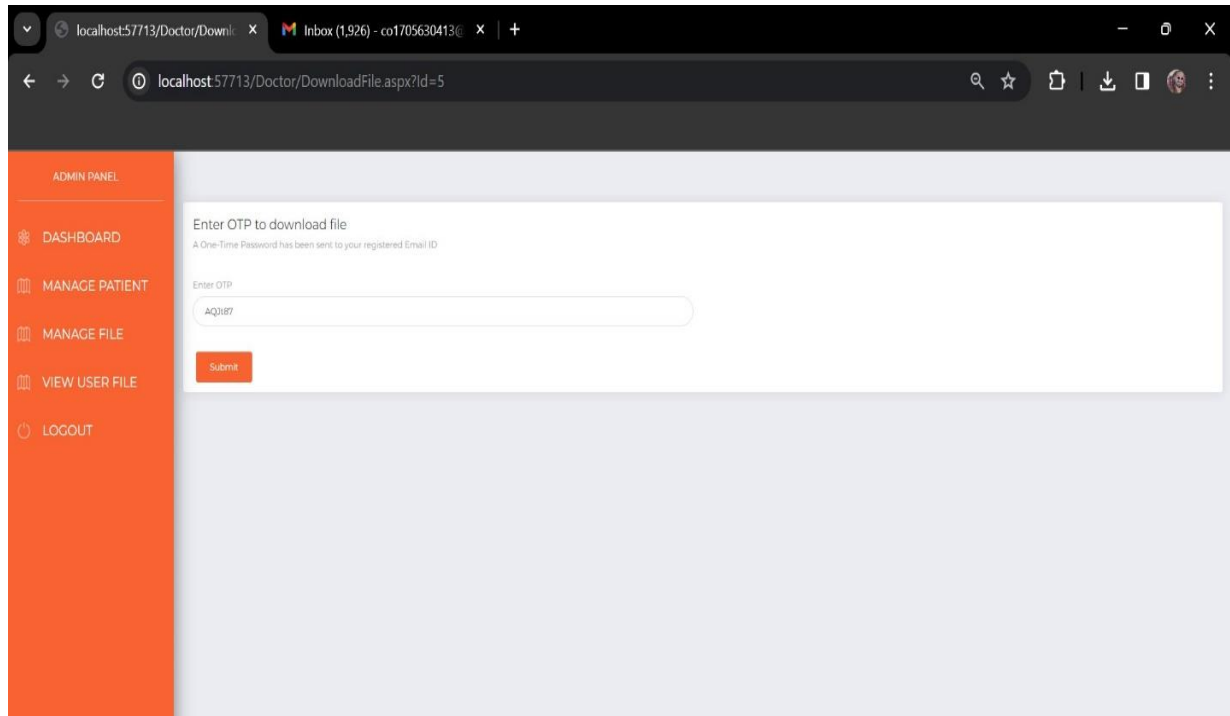
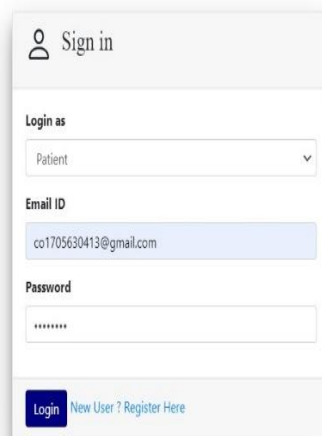


Fig 5.7: Doctor Side for Downloading and Viewing the report matching with Shared Key.

Figure 5.7 depicts the doctor panel designed for downloading patient reports uploaded into the system. Utilizing a shared key generated by the system and sent via email, doctors can securely access and download the files. This process ensures data confidentiality and integrity, facilitating efficient retrieval of patient information for comprehensive healthcare management.

5.8 Patient Panel

The Patient Panel provides a user-friendly interface for patients to access their medical records securely. Through this platform, patients can view their diagnoses, treatment plans, and medical history, informed participation in their healthcare journey.



Act
Go to

Fig 5.8: Patient Side for Logging into Patient Panel

Figure 5.8 showcases the login page of the EHR system tailored for patient access. Patients can securely log in using their email ID and a one-time password (OTP) generated by the system. This process grants them entry to the Patient Panel, ensuring streamlined access to their healthcare information. The utilization of email-based authentication enhances security and user experience within the system.

5.9 Patient side for sharing report

Patients can securely share their medical reports with healthcare providers through our platform's intuitive interface. This streamlined process ensures efficient communication of vital health information, facilitating collaborative care and treatment planning.

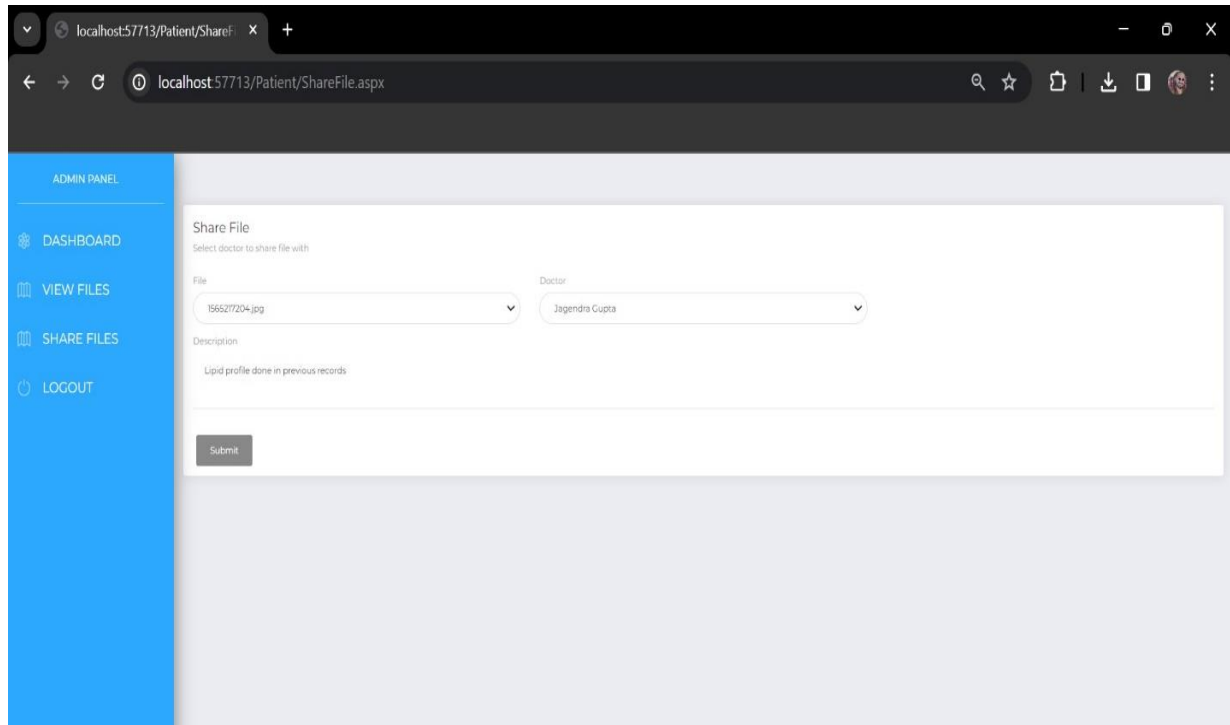
The image shows a web browser window with the address bar displaying 'localhost:57713/Patient/ShareFile.aspx'. The browser interface includes standard navigation buttons (back, forward, refresh) and a search bar. The web application has a blue sidebar on the left labeled 'ADMIN PANEL' with menu items: 'DASHBOARD', 'VIEW FILES', 'SHARE FILES', and 'LOGOUT'. The main content area is titled 'Share File' and contains a form with the following elements: a dropdown menu for 'File' with the value '156527204.jpg', a dropdown menu for 'Doctor' with the value 'Jagendra Gupta', a text input field for 'Description' containing the text 'Lipid profile done in previous records', and a 'Submit' button at the bottom.

Fig 5.9: Patient Side for Sharing their medical Report

Figure 5.9 pertains to the patient interface designed for uploading dedicated medical reports into the system. Patients can seamlessly share stored files with consulting doctors to provide comprehensive medical history. This functionality streamlines the consultation process, enabling efficient access to past medical records for informed decision-making. By utilizing the system's repository of medical data, patients ensure accurate and thorough communication with healthcare providers.

5.10 Patient side for sharing report

Patients can conveniently access and review their updated medical reports through our user-friendly interface. With seamless integration between doctor and patient modules, real-time updates ensure accurate and timely information retrieval. This enhances patient engagement and promotes informed decision-making regarding their healthcare journey.

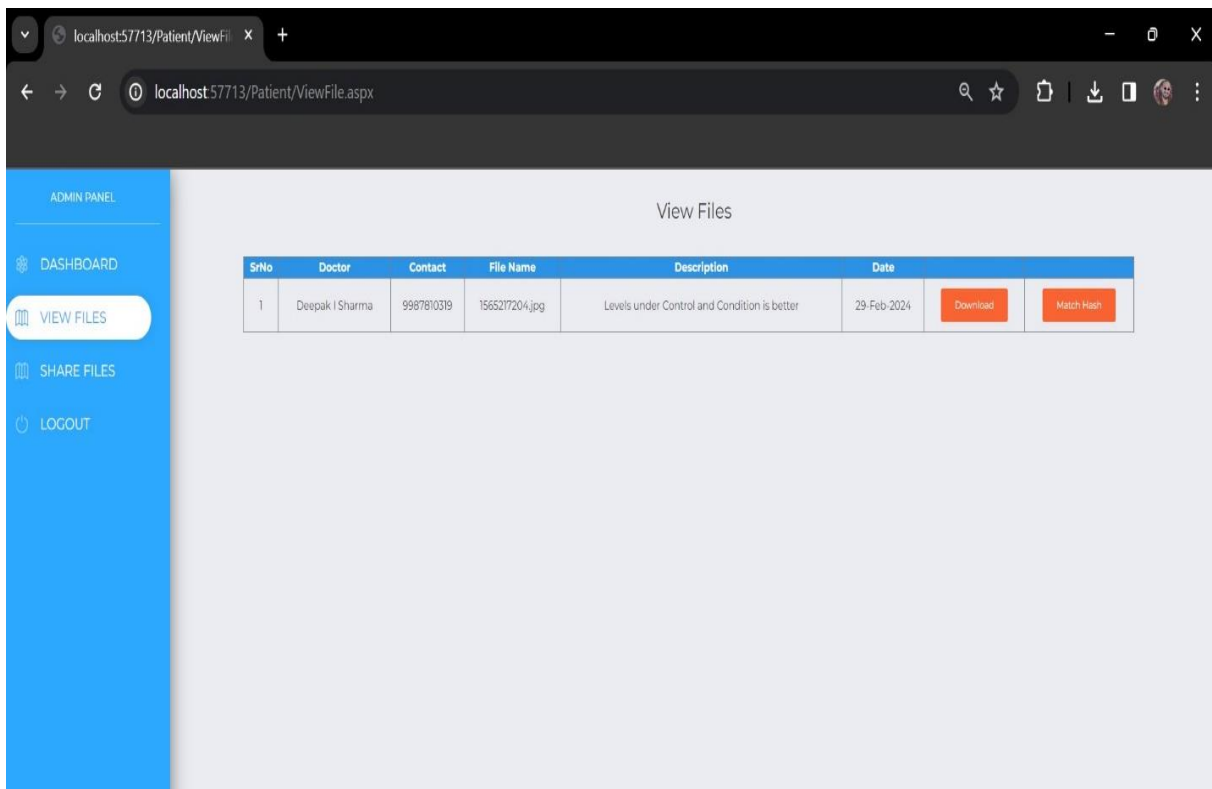


Fig 5.10: Patient Side for Viewing their medical Report updated via Doctor Side

Figure 5.11 grants patients access to view and download medical reports uploaded by the doctor panel. Utilizing an encryption key provided via email, patients can securely retrieve their reports from the system. This process ensures confidentiality and integrity of patient data, enhancing trust and security within the platform. It empowers patients to actively engage in their healthcare by accessing and managing their medical information conveniently.

Chapter 6

Conclusion and Future Scope

Conclusion

Patient healthcare systems operating on the cloud face significant security challenges due to the storage of sensitive data, emphasizing the need for robust measures to safeguard patient privacy. It is imperative to address security concerns comprehensively from the system's design phase onwards. Monitoring patient parameters like blood pressure and pulse using a healthcare server not only aids in treatment but also maintains comprehensive historical records. This study proposes the implementation of a Hybrid Cryptographic Technique (HCT), merging two encryption algorithms to bolster both security and system performance. The workflow involves deploying a healthcare server on MS Azure, enabling secure registration,

login, and management of patient data by healthcare professionals. Encryption utilizes RSA for uploading patient files, encrypting them into ciphertext with a random key sent to the patient for download, while AES decryption is employed for accessing these files. Consequently, the combined RSA-AES approach ensures robust data security within patient healthcare systems, enhancing overall patient confidentiality and system integrity.

Future Scope

The future of securing Electronic Health Records (EHR) through hybrid cryptography shows promise, holding significant potential for healthcare. As healthcare data digitization grows and cyber threats increase, robust security measures become imperative to safeguard sensitive patient information. Hybrid cryptography, merging symmetric and asymmetric encryption, offers a sophisticated solution, enhancing EHR data protection. Advancements in technology pave the way for improved security measures to counter evolving cyber threats, ensure compliance with regulations like HIPAA, and integrate with emerging technologies such as blockchain and artificial intelligence. By employing hybrid cryptography, healthcare organizations strengthen data security practices, ensuring patient information confidentiality and integrity in an interconnected digital healthcare environment.

References:

Journal Paper:

- [1] R. Manoj, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos and S. Ali, "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud," 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud), San Francisco, CA, USA, 2017, pp. 185-190, doi: 10.1109/MobileCloud.2017.38.
- [2] M. Joshi, K. P. Joshi and T. Finin, "Delegated Authorization Framework for EHR Services Using Attribute-Based Encryption," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 1612-1623, 1 Nov.-Dec. 2021
- [3] Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. i-cxviii
- [4] P. Chinnnasamy and P. Deepa Lakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.
- [5] W. Xiaoyu and G. Zhengming, "Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment," 2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI), Ottawa, ON, Canada, 2020, pp. 67-70, doi: 10.1109/ICAACI50733.2020.00019.
- [6] C. K. a. D. R. V. P. M. Aryan, "Enhanced Diffie Hellman algorithm for reliable key exchange," IOP Conference Series: Materials Science and Engineering, vol. 263(017) 042015, pp. 1-8, 2017
- [7] Kanna, G.P., Vasudevan, V.: A fully homomorphic-elliptic curve cryptography-based encryption algorithm for ensuring the privacy preservation of the cloud data. Clust. Comput. 22, 9561–9569 (2019)
- [8] Bhatt Agarwal, R.: A technological review on scheduling algorithm to improve performance of cloud computing environment. Int. J. Innov. Technol. Explor. Eng. (IJITEE) 8(6), 166–172 (2019)
- [9] Moudgil K, Maheshwari R, Parekh HB, Devadkar K. Cloud-based secure smartcard healthcare monitoring and tracking system. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). Coimbatore: IEEE; (2017). p. 1–8. 10.1109/ICECCT.2017.8117869
- [10] Yang Y, Li X, Qamar N, Liu P, Ke W, Shen B, et al. Medshare: a novel hybrid cloud for medical resource sharing among autonomus healthcare providers. IEEE Access. (2018) 6:46949-61. 10.1109/Access.2018.2865

Implementing Data Security on EHR Using Hybrid Cryptography

Mr. Dipak Bisht¹, Mr. Deepak Sharma², Mr. Meet Todankar³, Ms. Sneha Sankhe⁴

^{1,2,3} Student, Department of Information Technology, Theem College of Engineering, Boisar, Maharashtra, India

⁴Professor, Department of Information Technology, Theem College of Engineering, Boisar, Maharashtra, India

Abstract - The development of electronic health records (EHR's) for patient monitoring is a concept widely adopted in the field of healthcare industry. Through this considerable web app patients can communicate with respective doctors and consult them for their disease diagnosis. This helps them to keep a track of their medical records in a digital and electronic form. However, the data uploaded on the EHR is huge in terms of volume, as multiple patients might try to access them. In such a scenario the data so collected might undergo certain attacks and breaches due to the vulnerability of the system model which might even lead to power failure of data stored on the respective EHR. Therefore, in this report, we propose the implementation of two encryption algorithms that would help to secure the data being transferred on the EHR. For this purpose, a Hybrid Cryptographic Technique (HCT) is used that includes the execution of AES, RSA and Serpent Algorithm. Using the mentioned HCT, the informational exchange is expected to be secured on cloud. The Advanced Encryption Standard (AES) is lauded for its efficiency in protecting data through its symmetric encryption approach. RSA, an asymmetric encryption scheme, enhances security by leveraging complex mathematical relationships. This innovative amalgamation safeguards medical records from unauthorized access, cyberattacks, and potential power-related incidents, reinforcing the confidentiality and integrity of sensitive healthcare data. The marriage of encryption methodologies thus presents a significant stride toward ensuring the safety and privacy of patient information in the evolving landscape of healthcare technology.

Key Words: AES, cryptography, RSA, encryption, EHR

1. INTRODUCTION

The aim of the proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor.

Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss.

For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

2. LITERATURE REVIEW

A Hybrid Secure and Scalable Electronic Health Record Sharing (HSS-EHRS) system, whereby two cryptographic methods are utilized for providing a flexible, secure and fine-grained access to EHR files in hybrid cloud. The proposed framework divides the system into two security domains and utilizes an ABE encryption scheme to encrypt the EHR files. The proposed system proved its efficiency based on encryption time and concurrent recipient data access and sharing. The enhanced MA-ABE encryption scheme is capable of handling on demand recipient data access and providing high levels of security.^[1]

It has focus to developed an attribute based, field level, document encryption for managing the access and data security of cloud-based EHRs. In their approach they designed and developed a complex knowledge graph that details the roles and attributes of different stakeholders of the medical organization along with the various relationships between them. They also developed an open-source, easy to use user interface.^[2]

The existing strategy in cloud security to assess the three primary parameters such as judgment, verification and secrecy. To make strides each aspect various strategies is got to join that are distinctive from conventional security framework on information exchange or record capacity framework. The summarized the existing strategy advance up to information and gives future scope of the strategy. The cloud capacity security framework requires the compelling strategy to overcome the issues such as information spillage, unreliable transmission and get to qualifications.^[3]

It provides the health-related data is encrypted using Blowfish and keys are managed by the improved RSA technique when stored in cloud storage. Benefits of this

hybrid approach were quick encryption, a huge prime number pool for key production, and effective key management. The simulation results unequivocally demonstrate that the suggested hybrid technique's encryption and decryption times are faster than those of the other approaches taken into consideration.^[4]

This study proposes a data security protection system based on infrastructure security of human, network, and cloud, as well as the related security technology and strategy, to address the issue of cloud computing security. This paper addresses the easily overlooked security issues with cloud service provider internal staff by proposing identity authentication and role-based access control strategies based on account and certificate, analyzing and researching cloud security standards and legal maintenance, and presenting a cloud security assessment system along with pertinent legal recommendations and measures to offer a robust defense.^[5]

3. SYSTEM ARCHITECHURE

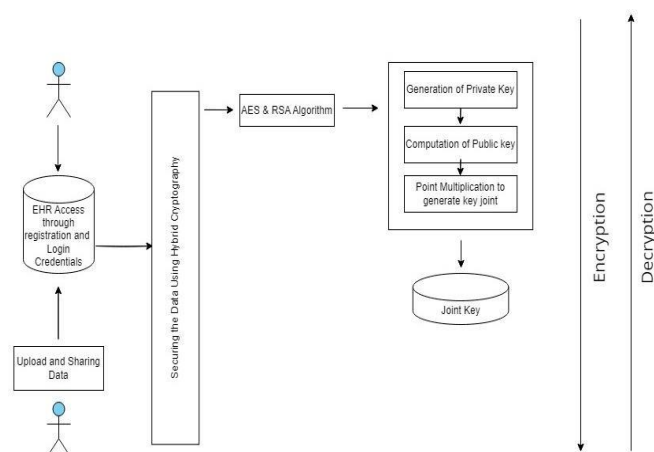


Fig 1. System Architecture of EHR system

Proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss. For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

4. RESULT AND ANALYSIS

Discover everything there is to know about electronic health records and the specific security threats they provide. Learn about the fundamentals of hybrid cryptography, such as the ways in which RSA and AES can work in tandem. When designing your system's architecture, take into account the safe storage, access, and transmission of EHR data. Determine the precise situations and use cases in which hybrid cryptography will be used. Select suitable encryption and decryption techniques for AES and RSA. Recognize both algorithms' key management procedures. Integrate the selected algorithms, making sure they are efficient and compatible with your EHR system. Provide techniques for combining RSA's asymmetric key encryption with AES's symmetric key encryption. To manage key generation, distribution, storage, and rotation securely, put in place a strong key management system. Carry out extensive testing to make sure the safety precautions work. Analyse your implementation's performance and make the required adjustments. Provide thorough justifications for the selected algorithms, important management procedures, and system architecture in your implementation documentation. Make sure that all of your work is unique and that any use of pre-existing methodology is appropriately cited.

```
.exe' 'c:\Users\Lenovo\.vscode\extensions\ms-pytho
py\launcher' '52631' '--' 'D:\Cyber Security M\EHR
AES algorithm is working correctly.
Accuracy: 100.00%
Encryption time: 0.003053 seconds
Decryption time: 0.000000 seconds
Transmission rate: 123.08%
PS D:\Cyber Security M\EHR Cloud\Acc>

.exe' 'c:\Users\Lenovo\.vscode\extensions\ms-pytho
py\launcher' '52647' '--' 'D:\Cyber Security M\EHR
RSA algorithm is working correctly.
Accuracy: 100.00%
Encryption time: 0.000000 seconds
Decryption time: 0.009667 seconds
Transmission rate: 1969.23%
PS D:\Cyber Security M\EHR Cloud\Acc>
```

Fig 2. System Architecture of EHR system

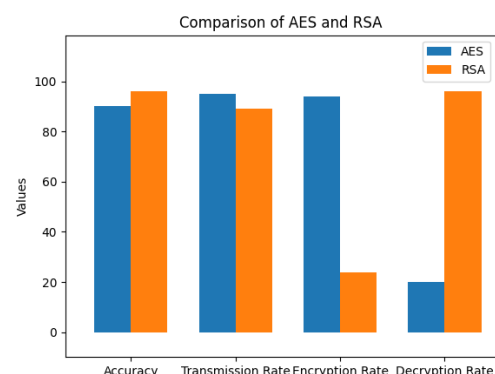


Fig 3. Testing of Encryption & Decryption using HCT

The above result shows the accuracy of encryption and decryption using hybrid cryptography technology based on two algorithms.

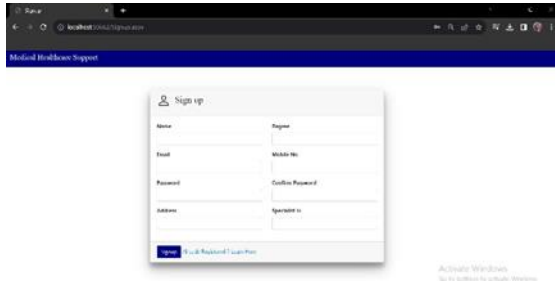


Fig 4. Signup Page for Doctors

Above fig 4. Shows the Signup page for the certified Doctors to get registered to manage the patient details.

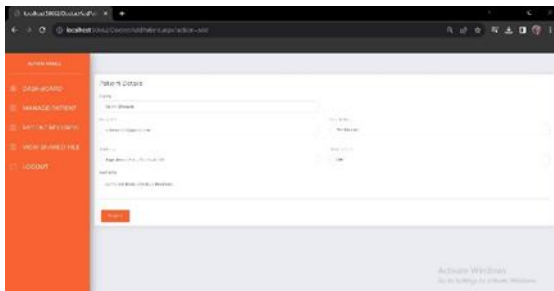


Fig 5. Doctor Dashboard panel to manage patient detail

From here Doctors can manage their Patient health report and can give medication remark according to the patient health condition.

5. CONCLUSIONS

The main steps we used in the project is to focused on establishing the foundational components for data security and user access control in the EHR system. The hybrid cryptography approach, along with the signup and login pages for doctors, will form the basis for a robust and secure EHR system. As the project progresses, further features and security enhancements will be implemented to ensure comprehensive data protection and a seamless user experience and Doctor can see the patient detail and go through the patient report and suggest medicine to the patient according to their report. Regular monitoring and updates are essential for maintaining the effectiveness of the security measures over time.

ACKNOWLEDGEMENT

We would like to take this opportunity to express our gratitude towards all the people who have in various ways, helped in the successful completion of our project. We must

convey our gratitude to our project guide Prof. Sneha Sankhe for giving us the constant source of inspiration and help in preparing the project, personally correcting our work and providing encouragement throughout the project. We also thank all my faculty members for steering me through the tough as well as easy phases of the project in a result-oriented manner with concern attention.

REFERENCES

- [1]. R. Manoj, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos and S. Ali, "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud," 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud), San Francisco, CA, USA, 2017, pp. 185-190, doi: 10.1109/MobileCloud.2017.38.
- [2]. M. Joshi, K. P. Joshi and T. Finin, "Delegated Authorization Framework for EHR Services Using Attribute-Based Encryption," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 1612-1623, 1 Nov.-Dec. 2021
- [3]. Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. i-cxviii
- [4]. P. Chinnasamy and P. Deepa Lakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.
- [5]. W. Xiaoyu and G. Zhengming, "Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment," 2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI), Ottawa, ON, Canada, 2020, pp. 67-70, doi: 10.1109/ICAACI50733.2020.00019.
- [6]. C. K. a. D. R. V. P. M. Aryan, "Enhanced Diffie Hellman algorithm for reliable key exchange," IOP Conference Series: Materials Science and Engineering, vol. 263(017) 042015, pp. 1-8, 2017
- [7]. Kanna, G.P., Vasudevan, V.: A fully homomorphic-elliptic curve cryptography-based encryption algorithm for ensuring the privacy preservation of the cloud data. Clust. Comput. 22, 9561-9569 (2019)

- [8]. Bhatt Agarwal, R.: A technological review on scheduling algorithm to improve performance of cloud computing environment. Int. J. Innov. Technol. Explor. Eng. (IJITEE) 8(6), 166–172 (2019)

- [9]. Moudgil K, Maheshwari R, Parekh HB, Devadkar K. Cloud-based secure smartcard healthcare monitoring and tracking system. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). Coimbatore: IEEE;(2017).10.1109/ICECCT.2017.8117869

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Mr. Dipak Bisht

In recognition the publication of the manuscript entitled

Implementing Data Security on EHR using Hybrid Cryptography

published in our Journal Volume 11 Issue 3 March 2024

Impact Factor : 8.226

www.irjet.net



Editor in Chief

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Mr. Deepak Sharma

In recognition the publication of the manuscript entitled

Implementing Data Security on EHR using Hybrid Cryptography

published in our Journal Volume 11 Issue 3 March 2024

Impact Factor : 8.226

www.irjet.net



Editor in Chief

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Mr. Meet Todankar

In recognition the publication of the manuscript entitled

Implementing Data Security on EHR using Hybrid Cryptography

published in our Journal Volume 11 Issue 3 March 2024

Impact Factor : 8.226

www.irjet.net



Editor in Chief

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Ms. Sneha Sankhe

In recognition the publication of the manuscript entitled

Implementing Data Security on EHR using Hybrid Cryptography

published in our Journal Volume 11 Issue 3 March 2024

Impact Factor : 8.226

www.irjet.net



Editor in Chief

E-mail : editor@irjet.net