A Secured Way Of Keeping Medical Data Efficiently Using Web Farm In The Perspective Of Bangladesh

by

Rakibul Hasan
18101709
Aditya Biswas
18101015
Md. Touhiduzzaman Touhid
17101030
Umme Nusrat Jahan
18101513

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
Brac University
January 2022

Declaration

Upon the completion of the thesis with necessary requirements, it is declared that,

1. The thesis paper is completed as our own work for the purpose of completion of our degree at BRAC University.

2. The thesis paper does not contain full, partial or intentional contents from any existing or previously completed works and therefore, it is free of any kind of direct imputation of any information from published sources. The materials which were investigated for the purpose of completing the thesis were cited with appropriate referencing.

3. The thesis is completely genuine and a new creation and therefore, it is only submitted to the authority of our supervisor only. It was never proposed, submitted or contacted to be used as a publishing material to any other stakeholder party.

Student's Full Name & Signature:

Rakibul Hasan

Rakibul Hasan
18101709

Aditya Biswas

Aditya Biswas
18101015

Touhid

Md. Touhiduzzaman Touhid
17101030

Umme Nusrat Jahan

Umme Nusrat Jahan
18101513

Approval

The thesis/project titled “A Secured Way Of Keeping Medical Data Efficiently Using Web Farm In The Perspective Of Bangladesh” submitted by

1. Rakibul Hasan (18101709)
2. Aditya Biswas (18101015)
3. Md. Touhiduzzaman Touhid (17101030)
4. Umme Nusrat Jahan (18101513)

Of Fall, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on January 20, 2022.

Examining Committee:

Supervisor:
(Member)

Iqbal

Dr. Muhammad Iqbal Hossain
Assistant Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Noor

Jannatun Noor
Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

____

Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Ethics Statement

The proposed here in this paper is a novel work. In addition, we the members, hereby and sincerely declare that this thesis has been done based on the findings of our extensive research. All the materials, which have been used are properly noted and cited in this report. This research work, neither in full nor in any part, has never been submitted by any other person to another university or any institution for the award of any degree or any other purpose.

Abstract

Bangladesh is a fast developing country and aims to enter the list of developed countries by 2030. With that aim, there are remarkable technological advancements taking place in all sectors, but information technology in the medical sector is really lagging behind. In this new era of technology, the healthcare system needs to keep up with the constantly changing world. Our existing medical sector is still keeping important and confidential medical records in hard copies, which sometimes is a big hassle for both doctors as well as patients. The people are still indifferent about the confidentiality of their personal data. So, we want to propose an efficient model of Electronic Health Records (EHR), especially for Bangladesh using the concept of a web farm consisting two separate private and public cloud servers, with secured authentication features like kerberos, OTP authorization system, AES encryption, user friendly UI, and cost effective measures. Already, a few models of EHR are implemented around the world, and some others are being proposed too. However, most of them are not applicable to the Bangladeshi scenario because of unfriendly environments such as lack of awareness, slow internet speed, lack of technical knowledge of the people, and the scope of corruption. The model proposed here is able to overcome those deficiencies to meet the requirements that accept the challenges and adapt to the environment of this country.

Keywords: Data Security, Authentication, EHR, AES, Encryption, Decryption, Cloud server, Authorization, Web Farm.

Dedication

This thesis is dedicated to our loving parents and our department's respectable faculties, who have encouraged and supported us during the entire thesis and motivated us to achieve excellence in every aspect.

Acknowledgement

Firstly, we are grateful to almighty Allah for giving us the opportunity to complete our thesis without any kind of significant interruption.

Secondly, we express our heartiest appraisals for our supervisor Dr Muhammad Iqbal Hossain sir And co supervisor Jannatun Noor ma'am for guiding us with all necessary support, advice and guidelines. And finally, we express our gratitude to our beloved parents, without their continuous care and support it would not be possible.

Special mention for our classmates during the undergraduate period who enormously contributed to our development and progress.

Table of Contents

List of Figures

List of Tables

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

AES	Advanced Encryption Standard
AWS	Amazon Web Services
CPU	Central Processing Unit
CT	Computed Tomography
DES	Data Encryption Standard
EHR	Electronic Health Records
ER	Entity Relationship
GDPR	General Data Protection Regulation
HIMSS	healthcare Information And Management System Society
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
ICT	Information And Communication Technology
IP	Internet Protocol
LAN	Local Area Network
MD5	Message-Digest algorithm 5
MFA	Multi Factor Authentication
MRI	Magnetic Resonance Imaging
NID	National Identity Card
OAuth	Open Authorization
OTP	One Time Password

PaaS	Platform as a Service
PC-CBEHR	Patient-Centric Cloud-Based EHR
PHR	Personal Health Record
PSD	Personal Domain
PUD	Public Domain
RC	Rivest Cipher
RSA	Rivest–Shamir–Adleman
SaaS	Software as a Service
SFA	Single Factor Authentication
SQL	Structured Query Language
U.K	United Kingdom
UNIM	Unified Network Interface Middleware
USG	Ultrasound Sonography Test
UTAUT	Unified Theory of Acceptance and Use of Technology
WHO	World Health Organization
XSS	Cross-site Scripting

Chapter 1

Introduction

We live in a fast-growing era of information technology which is keeping its effect on every aspect of our lives. It is changing the way we live or the way we do our jobs. Behind all these, the Internet is the backbone of this revolution. The world is already enjoying the 5G network, and projects like Starlink are a matter of time [1][2]. The efficiency and portability of digital data storage have already inspired people to keep data in soft copies rather than in hard copies. Nowadays cloud-based storage is becoming more popular due to its security features and availability of high-speed internet.

Developing Countries are also keeping pace with the evolving world of information technology. Bangladesh can be a good example of that. The government is already shifting many important and crucial official works into online platforms such as e-passport, voting registration, online admission, job application, official meetings, etc. However, the healthcare sector still follows the traditional way to keep data and is yet to be introduced with digital data-keeping. The people of this country still do not understand the importance of keeping their personal health information private. Whereas, healthcare data is a very lucrative target for cybercriminals nowadays. There were previous studies that showed strategies for e-health facilities in Bangladesh [3]. Health is a major key for development. To improve the quality and access to healthcare, developed countries have put together ICT-based systems like EHR, EMR, etc. for patients and healthcare professionals. The efficiency of EHR in the healthcare system has already been proven before in previous studies [4]. For example, no one will be able to access health records without patients' permission, patients will not need to carry or preserve their medical records on paper anymore, there will be no loss of data, in case of emergencies doctors can access patients' previous health records easily, etc.

EHR (Electronic Health Records) is a way to keep medical or health-related data in a secured digital data storage system privately. Every authorized user can keep their medical data on the system and can access it whenever and wherever needed. EHR can contain a patient's sensitive data such as treatment history, diagnoses report, important dates, list of medications, etc. The data in EHR can be stored in various ways, but a cloud server is the best possible way to keep data secured. Cloud storage is a cloud computing service where data can be kept and different operations can be done using the internet. With "anytime, anywhere" data access, agility, global scalability, and durability are achieved [5] in the cloud. The concept of a web farm with multiple cloud servers may increase these abilities to a further extent. To upload, download and manage the data in the EHR safely, concepts of information security are used. Information security is the set of practices applied to secure data from unauthorized access. To take the healthcare data to a secure state, encryption and decryption are used. With the help of authorization techniques, specified access control is also performed in an EHR.

Successful implementation of a relevant EHR model for Bangladesh will take the healthcare system of the country to another level while keeping all the healthcare data safe and private.

1.1 Motivation

Bangladesh has more than 163 million people at present [6]. This is a high density of population for Bangladesh. This higher density of population needs a higher need for medical attention. The right to personal privacy should be reserved too. Whenever people go to the doctor or hospital or any diagnosis center, they get a huge number of reports or prescriptions. This creates a long unorganized paper trail which is not always easy to keep track of. Moreover, we see representatives of different pharmaceutical companies standing near the hospitals who stop the patients and take snaps of their prescriptions [7]. This is a serious violation of privacy protection which the patients are not even aware of. An EHR can bring an end to this problem.

Currently, reports on healthcare data breaches are increasing at an alarming rate. There were almost 600 healthcare data breaches in 2020 which is a huge spike of almost 55% from 2019 [8]. A graphical figure of this is shown in figure 1.1.

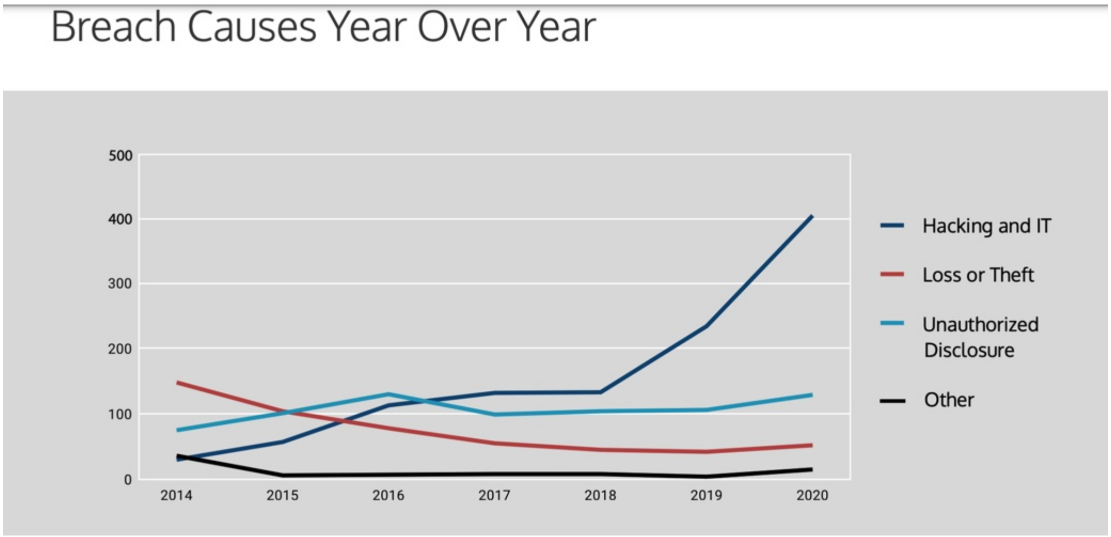


Figure 1.1: Reported data breaches over year

In other industries, data breaches may cost loss of money or personal information but in the healthcare sector, the impact can be far more devastating. Sensitive information should not be leaked or lost at any cost from a system. So, to protect the data from any illegal access, our model consists of proper authentication as well as an encryption and decryption system in the EHR.

As the health sector maintains many personal and sensitive data which is huge in size and also increases every day with the increasing number of patients, this sector needs easily scalable storage. It has to be a storage system that can be accessed anytime and from anywhere without compromising privacy. To prevent data redundancy, data should not be duplicated in the directory. Moreover, the storage system needs to be ready to accept plenty of traffic at the same time without any kind of interruptions. We will try to meet all these requirements with an easy and cost-effective solution.

1.2 Research Problem

For smooth healthcare services and proper security of patient data, Bangladesh must implement an EHR countrywide like the developed nations. However, the systems existing in developed countries are not very suitable for a developing country like Bangladesh. There are certain challenges in our country which the developed countries do not face usually. Also, the developed countries have some advantages over us. So, the existing system needs some modifications and add-ons to be implemented successfully in Bangladesh.

Bangladesh has a huge population and the healthcare providers have to deal with way more patients. The current doctor-patient ratio in Bangladesh is only 5.26 per 10,000 population and according to the WHO, Bangladesh ranks second last among the South Asian countries in this matter [9]. So the system must be able to cope up with this huge load. Every day the pathologists have to create plenty of patients' reports and doctors need to check them. Hence, the uploading and fetching of the reports should be as fast as possible.

Bangladesh has a literacy rate of 74.7% which is much lower than developed countries and the population is not well introduced to technologies [6]. As the EHR system is an advanced technological implementation, most of the people of this country will find it difficult and will be discouraged to use it. So, to take full advantage of this system we need an EHR that will be very user-friendly and the process must be easy to understand.

In our country, especially in rural areas, the internet speed is not so satisfactory, and there is also a huge problem of load shedding. These kinds of problems are seen only in developing countries. Any EHR system will be useless without the internet or electricity. That is why the EHR system must come up with some solutions to these problems.

There might be a tendency of manipulating or corrupting the data in EHR for personal benefits or wrongful acts. For this reason, the system must not be vulnerable to data manipulation and corruption. It has to be designed in such a way so that the users have specific and limited access according to their roles.

Bangladesh recently has acquired lower-middle-income status [10]. The government has already taken on a lot of megaprojects. As the country is still struggling with economical and financial problems, the implementation of EHR must be cost-efficient. So, all the unnecessary expenses should be trimmed from the model so that it becomes a feasible solution for Bangladesh.

Keeping all these in mind, we want to propose an EHR model which will address all these conditions and provide suitable solutions in terms of Bangladesh. Furthermore, we will also develop a system where we will implement our proposed system to some extent and observe the outcomes through multiple testing methods.

1.3 Research objective

This research aims to develop an initial full-fledged secured EHR platform for Bangladesh to develop its medical sector in information technology. A nationwide EHR will be used by several medical professionals, hospitals, patients, etc. Finding out what kind of data should be in the EHR is necessary. In addition, which data should be editable and which are not, who will have access to edit those data, and who will not should be defined. For how long access permission should be granted has to be decided. To make it available on all platforms, a suitable cloud type and service has to be selected. Then the cloud storage has to be unified with an authentication server which will be responsible for authentication and authorization of the users. Securing data over the cloud is quite important as there will be many personal data of the patient and doctor. So, the system will need a suitable encryption method to secure the data. In this case, deciding which data to be encrypted and which not to be is a crucial factor. There will be a huge amount of data going in and out of the cloud server at a time. During this data transaction, the system will run its encryption or decryption. Finding out an efficient way to do this is important so that the delay for data transactions is not noteworthy. Lastly, while deciding the mechanism and features, cost-effectiveness must be considered. Therefore, the objectives of this research are,

1. To deeply understand EHR, and what Bangladesh needs from this.
2. To analyze a patient and a doctor's needs from the EHR.
3. To make the EHR sufficiently secured and the information confidential in it.
4. To deeply understand the cloud and what type of cloud to use in the system.
5. To develop a multi level authentication system.

6. To implement an authorization technique.
7. To deeply understand which algorithm to use to encrypt and decrypt the data.
8. To fetch the data from the cloud efficiently.
9. To assess the model.
10. Discuss required updates after the initial model.

1.4 Thesis Orientation

The rest of the chapters in the paper are organized as follows. Chapter 2 contains a discussion on some works closely related to this research. Chapter 3 consists of all the background knowledge and theories that have been used in this thesis. After that, chapter 4 describes the proposed architecture of the model and methodology. Chapter 5 is a thorough description of the development procedure of 'Medicare' through which the model is implemented. It also shows various security testing and performance evaluations on the web application as well as the limitations and challenges of this work. Finally, chapters 6 contains conclusions and further plans respectively.

Chapter 2

Literature Review

There are many previous relevant works in the field of secure EHR. The goal of this part is to critically review these works. Different structures of EHR using different encryption or authentication systems are discussed or proposed in these works. Analysis of different approaches and structures taken by other articles on cloud storage or data security used in EHR are described here.

In an article [11], Khan et al. (2012) described the hopes and fears of implementing an EHR in Bangladesh. They did a qualitative study on two Bangladeshi hospitals. One of the hospitals already uses an EHR of some length. On the other hand, the other hospital is yet to be implementing one. They used the UTAUT model to guide their data. They interviewed five men and five women physicians based on the UTAUT model. Most interviewees seemed to expect EHR systems to be time saving, convenient, efficient and productive and thought using EHR systems may have a positive impact on the professional decision making as they could get better information about patients' medical backgrounds. Most of the interviewees stated that they would use an EHR if it was mandatory. Where young medical personnel are open to go into technology, some fear that the older personnel have fear of getting into new technology. They seem to have reliability and trust issues regarding completely switching to an automated system and having no manual record at all. They also seem to think new technology will be less productive with older physicians. Some consider manual data over anything.

EHR systems can be used by people in various stages. It is not only for doctors and patients. In an article [12], Schabetsberger et al. (2005) showed that there are different kinds of users in the EHR. For example, patients, medical professionals, pharmacies, researchers, health insurance agencies etc. All these different users must have different kinds of expectations from the system. The author said that a patient would want to access their basic medical records with a basic description of the medical terms but medical professionals would like to get their patient's descriptive medical history. Whereas, the pharmacy would only need to access the patient's prescription.

In another article [13], Mahmood et al. (2017) proposed a PHR or personal health record system which is divided into 2 parts - the personal domain (PSDs) and the public domain (PUDs). In PSDs, the owners assign access for personal users and encrypt a PHR file with its data attributes. Multi-authority based weighted attribute encryption scheme is used in this domain. Here, the PHR domain defines a public space of data attributes shared via every PSDs, such as personal details, health profile, etc. On the other hand, the PUDs include professional users such as doctors, nurses, medical researchers, etc. To ensure security, Attributed-based access control for the Multi authority model is implemented in this domain. The construction of the access control model consists of: initialization of system, key generation, encryption and decryption. Here, The author claims that their system provides privacy such that the cloud service providers or other unauthorized persons could not trespass the sensitive medical documents, and the patients can assign fine grained access control to maintain control over access to their PHRs. Furthermore, he claims the proposed system to be collusion resistant and secured in a multi owner environment. He adds, In the Multi-Authority Based Weighted Attribute Encryption Scheme, each user is assigned a unique and randomly generated identifier by the central authority. So, different users with different IDs never collude together by joining their attributes and decrypting the ciphertext. In the performance analysis, it is seen that encryption and decryption time increases with the increasing number of authorities.

As a developing country, focusing on the cost of developing an EHR is necessary. In a research work [14], Ogbodo, et. al. (2020) proposes an EHR model with a SaaS application hosted in the cloud. They unified an authentication server that is responsible for the authentication and authorization of the users. PC-CBEHR system is used to see if a user is authorized or not. To make the best use of the CPU, they used virtualization techniques so that it can create multiple virtual systems in a physical system. The model used Unified Network Interface Middleware (UNIM) for communication among the computers on that server. Mysql is used to manage, write and read the data on this system. The system is made using PHP scripting language and medical stuff, doctors and authorized people can view or print information from the system.

Data security is a very important issue to focus on in EHR as there will be many personal data of patients and doctors. A research work [15], Ahmed et al. (2018) proposed a system where sensitive personal health record data is mapped to a machine key as well as a secret key to access data for the third parties. These keys will be monitored and controlled by the service providers. According to the research [15], this ciphertext based security system brings a more secure and privacy protected system that makes it more reliable to the user. Search string and searching data would be more efficient. In the implementation part, data owners would have to register and login to save their data on the cloud platform. In this proposed system, the owner has the option to delete data at any time and can verify if the data is attacked by any attacker or not. There will also be a trapdoor where all the requests processed by the user will be shown in the generated trapdoor.

In an article [16], the author Zhang shows an EHR model by adding a secure energy-saving communication scheme and encryption algorithm to the traditional medical cloud model. This model integrates low-overhead communication establishment schemes with high security encryption algorithms. Secondly, he proposes a communication authentication algorithm ‘MedGreen’ based on elliptic curve and bilinear pair, where the two communication parties can complete the key establishment and identity authentication only after one communication. This scheme combines the two stages of key calculation and identity authentication, and improves the key authentication method. The author claims this system can balance the resource overhead of the key center and the user and also can resist the Man-in-the-middle attack effectively. Thirdly, Zhang presents a secure data storage algorithm ‘MedSecrecy’ based on Huffman compression and RC4. MedSecrecy enhances the randomness of the key stream and the confidentiality of the algorithm while maintaining the encryption efficiency of RC4. Moreover, keeping the large amounts of medical data and high repetition rate in mind, they have combined Huffman compression algorithms in MedSecrecy to reduce the ciphertext size. Author also shows how the system is secured, energy-saving and highly efficient for EHR which is validated by comprehensive analysis and extensive simulations.

Intel report [17] stated that EHR server databases are implemented with the way of using Intersystem cache and are very much increasingly systematized to be protected on a confidential basis in terms of sensitive healthcare data. The structure of intelligent AES by intel implements overall encryption and decryption very swiftly by reducing the associated processing time. The existence of advanced processing power given by the seven sets of instructions with four of these completing the core algorithm of AES, the system is swift than any other encryption system used previously and these are often configured and classified as High Performance Database to power a large scale EHR. Mapping and preservation of the encryption system creates a secure data hub with a probable cache system of data storage. As AES even has scope to work with block level of encryption, this ensures that the fixed initialization is done over large blocks. This makes the execution time less than the overall designed systems which were used in early days. The performance testing of AES in similar machines of existing DES and other encryption methods showed that AES took down the other competitors in terms of execution time, response time, data safety, data volume and possible blockage against any kind of threat attack.

In a research [18], Young, yang 2019 mentioned that a selective data analysis and encryption technique based on AES can solve the security and efficiency issues of electronic health record in both macro and micro level. In micro level the personal level of information and in macro level, the organizational level of information are protected with byte based symmetric block ciphers. The AES system with higher standard of security than the DES, 2DES and 3DES has played a crucial role in formulating the international standard as a de facto system for encryption. The total four operations : substitute bytes, shift rows, mixcolumns, and add round key ensure a properly managed swift, safe and secured data encryption system is ensured. The overall scope of working with AES depends on the necessity, safe and required level of accuracy of data for preservation into information and keeping them away from the breach of any kind of attack. The overall numbers of crypt analytical attacks on AES were never found to be existing but there were some possible probability of side attacks. From the utilization of permutations substitution based algorithm design, it was possible to build information safety by a very effective encryption system with faster check of information relevance and data query.

In another research, Hamdani in his Ph.D research paper [19], has discussed the development of cryptography based access control for healthcare record and web systems. He noted that while data is being stored on a large scale to generate information, there is a possible scope of losing data or getting changed data by threats and attacks. Therefore, any kind of cryptographic algorithm can make the systems less vulnerable and we'll be protected against such attacks. But the server or web design can be slower if the executing techniques of the encryptions are not speedy. By the permutations substitution based AES with byte based execution and overall faster design structure AES can work upto 256 bits which is much higher than the 56 bits in DES. The faster execution has solved the problem of time consumption to analyze the data but the security issue is the most important aspect to consider while constructing any data or information encryption system. Here, by using aggregate security technique, AES has totally covered the lackings left behind by the early created encryption systems. Such diverse and intense working chronology has made AES the prime of all the encryption systems techniques. In the last part of the analysis it was mentioned that the execution of the proper security systems are done by AES in both theoretical and practical ways. AES was tested in all the existing works built with the other systems and every time AES generated the best outcome and this implies that there was no other best option than AES to create EHR systems as the system can store sensitive and confidential data where security is the biggest concern.

The research papers discussed have proposed different approaches to form an EHR efficiently and securely. Some of them have used multiple authentication algorithms and methods of data security. One of the papers has introduced totally new algorithms and methods for their model. Mostly the works are security centric and focused on efficiency of storages. However, there is no discussion on management of big size data shown, such as MRI, USG, CT Scan reports which includes a set of many high resolution pictures. The big size data should be compressed or kept in a way so that data encryption-decryption and storing becomes efficient while maintaining the quality and privacy of the data. Though the research works are technologically very advanced and contain many features, there is no mention about whether the interface is user friendly or not. A population which is not well introduced to technologies cannot benefit from EHR if it is not easily understandable. Again, none of the researchers have considered load shedding and internet connectivity error problems in their works. If load shedding or connectivity error occurs during data transaction or authentication process, their whole EHR model will be interrupted. So, the EHR should have a back-up plan to hold and protect the data for a time being and resume the process when connectivity restores. This will prevent data corruption, data loss, data redundancy, data piracy and also will protect the data from attacks during load shedding and internet unavailability. The core of AES systems is very fast, secured and protected in both online and offline mode of data storage. The AES designed web model can ensure the maximum layer of safety by triggering the four operations that backup the AES system with the overall permutations substitution possible within the data and data nodes. Therefore, in developing a proper web based EHR system, the framework of AES can very easily come into action by devoting a fast and secured data server.

Chapter 3

Background Analysis

The Healthcare system is now adopting digital data more and more to the workplaces all over the world. These digital data are more convenient and efficient to the healthcare environment. Moreover, the shift from analog to digital data-keeping system connects the whole system as a network as the user is able to access it from anywhere. In an analysis of a third global survey on eHealth, it is found that EHR is highest in wealthier countries with two-thirds (66%) in the upper-middle-income group and roughly half of the high-income countries (52%). While only a third of lower-middle-income countries (35%) and low-income countries of only 15% reported having EHR [20]. This number is increasing day by day. This shows how important it is to implement a nationwide EHR.

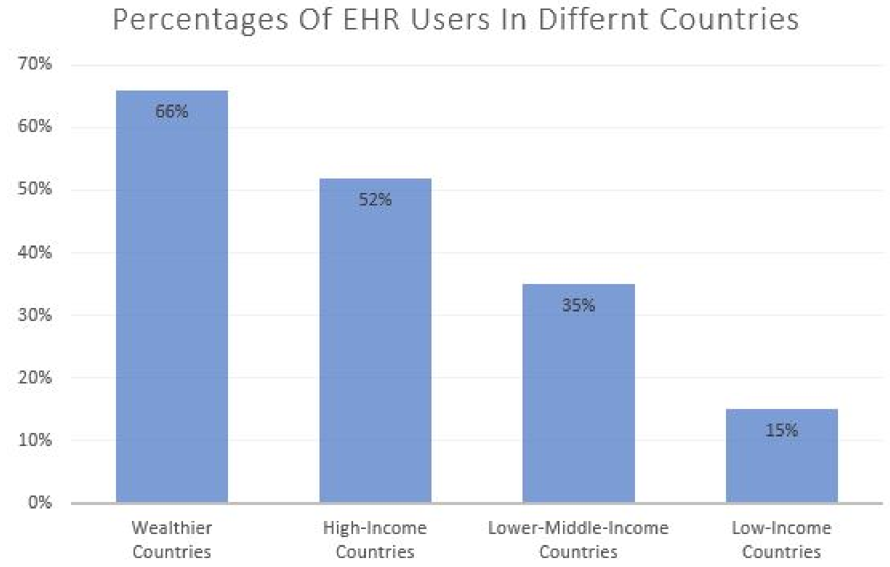


Figure 3.1: Uses of EHR in different countries according to income status

3.1 EHR

EHR or electronic health records is a system that consists of a patient's medical history. This provides the patient and a healthcare professional to access these records from anywhere just with a simple connection to the internet. According to HIMSS(Healthcare Information and Management System Society), the first EHRs appeared in the 1960s. The purpose of this EHR is to convert all the hard copies of a patient's medical report into digital format in a systematic way. They should be updated every time a patient visits a doctor or a hospital so that every authorized healthcare professional can get their patient's up-to-date medical history. An EHR can contain a patient's data such as treatment history, diagnoses report, important dates, list of medications, and other relevant sensitive information. Authorized specific users can upload, access, and modify specific data in the dedicated folder using the system. Electronic forms of files are much easier to store in the EHR and also can be managed with minimum effort. This not only has brought mobility to huge amounts of files but also has made sure zero loss of data, security to the sensitive medical reports, and ease of treatment. The benefits of EHR includes-

- Ease of access to health information and services
- Improvement in doctor-patient relationship and understanding
- Ease of tracking national health issues and predicting upcoming pandemics
- Accuracy and clarity in medical records
- Reducing medical errors and duplication of tests
- Protection of privacy of the patients

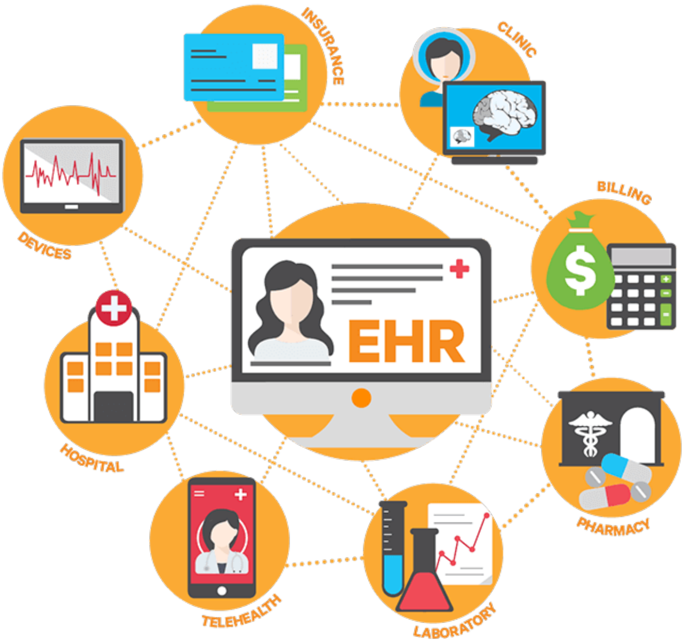


Figure 3.2: Functionality of EHR

Here, in figure 3.2, All the functionality of an EHR is shown. It gives a basic idea of what kind of data it will store [21].

3.2 EHR Architecture

EHR architecture from the viewpoint of content, it is essential to understand what the user needs from the EHR. According to an article [12], there are many types of users who will need access to the EHR. For example, medical practitioners, patients, pharmacies, researchers, health insurance companies, etc. They will require different data from the system. They can not all have the same access to the system. This brings us to the system structure. As many people from different stages need access to the EHR, Cloud here works as storage that will keep the data safe and accessible to the users. All the users can not have access to every data. So, it needs an authentication server, which will authenticate the users and take them to the data they have access to. Then security plays a big part in EHR architecture. As most of the data stored in the cloud are sensitive and confidential, there needs to be a certain encryption-decryption system for the data.

3.3 Web Farm

A web farm consists of 2 or more servers that work together to host a single website. A load balancer is typically used to connect the web servers, distributing incoming requests among the servers in the web farm [22]. It is widely used for a lot of traffic facilities as well as controlling and managing everything in an easier way. Web Farm can be implemented for more computing ability providing larger resources and managing areas. In a web farm, connecting multiple servers and exchanging data among them is possible. In this EHR model, the concept of load balancing will not be used, rather the basic concept of hosting a web application in multiple servers will be inherited for security enhancement.

3.4 Cloud Server

Cloud as a storage system works as a location for storing digital data. There are mainly three service models for the cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services can be provided according to the needs of the user. To keep data in a place where the cost is limited and maintenance is proper, the cloud comes first. Cloud storage has a dynamic storage system of updating when new data is stored. As a result, users get the flexibility of storage while keeping data on the cloud. Cloud also has the option to store data for an unlimited time period. There are different cloud computing available. For example, Private cloud, Hybrid Cloud, On-premise cloud, etc. Private clouds are owned by third-party service providers. End-users are given a dedicated server that is not shared by other entities. All the managing and maintenance are done by a third party. Hybrid cloud is the addition of different types of cloud. For example, in a hybrid cloud system, a user can store sensitive data and applications in a private cloud whereas they can use a public cloud for managing low-risk data or information. On-premise cloud needs IT, professionals and staff, to maintain the servers. It is a LAN network and needs a high-security safeguard. Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, Oracle, etc are some of the popular cloud service providers.

All these come up with a security system as it is quite impossible to leak any data from the cloud nowadays. There can be attacks, breaches, hacks, and leaks to the cloud data [23]. Though these attempts can be prohibited by using some of the advanced clouds which are available to date. All the benefits of using cloud storage are shown in the figure 3.3 given below [24].

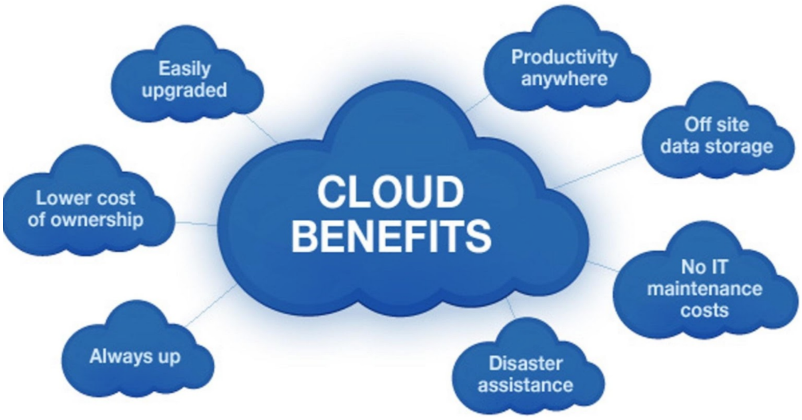


Figure 3.3: Benefits of Cloud computing

3.5 Data Security

The overall process and procedures with background measures for protecting data against any kind of destructive forces or in other words to create a shield for keeping the data secured as per the requirement of the interested parties. In general terms, we understand data security as an arrangement for keeping the data from any kind of theft in offline mode and from any kind of spam, cyberattack, and data leak in the online mode. In both micro and macro information environments, data security measures are very important for the proper operational excellence of any organization that uses sensitive and confidential data processing. The security process can be started from cryptography, and this might end up in multilayered protection systems such as two-factor authentication, authorized personnel unlocking, and biometric technology. There are several standards and measures in different parts of the world to ensure the proper security and safety of data handling, cleaning, communicating, processing, and reporting. One of the major implications of the data security system is realized by the U.K Data Protection Act as well as the European Union General Data Protection Regulation (GDPR) as enforced laws to ensure public, private, and organizational level of security under various acts and rules.

The data security of an EHR system reflects the privacy and protection of healthcare data in an EHR system. Three important factors for protecting health data by HIPAA are administrative safeguards, physical safeguards, and technical safeguards [25]. The administrative safeguards rely on the system's data secure layers. Keeping data safe takes a lot from physical safeguards as it would keep the data out of reach of the potential threats. As well as the technical safeguards that keep the malware away. Securing data is important as it keeps the data integrity intact and confined to the owners of the data and healthcare professionals connected to them. This also provides them with the security of keeping data for a long period of time which was kind of impossible for data in hard copies. The three main parts of data security of this project can be classified as authentication, authorization and cryptography.

3.5.1 Authentication

Authentication is the overall process of maintaining the proof and evidence of a general user as real in the web security system. It is the representation of the verification process of authorized users of the system to prevent any data breach or any kind of security threat. Mohammed, Lakshminarayanan, Ramalingam in their research [26] described authentication as a systematic procedure of creating a medium of verification to pass the entry system of the servers with proper security measures. If the verification phase is not completed, the authorized users can not even enter the work system.

Authentication is designed with maximum layers of security with various methods such as passwords, pins, biometric systems, and other encryption-based modules. The overall system ensures the flow of data controlling and proper access to reach the organizational goals properly.

3.5.2 Authorization and access control

The security mechanism that acts as the determination standard of various access levels of appropriate clients/users who are directly and indirectly related to the data system's resources is called authorization. This mechanism acts as the gateway to allow the interested parties to access the database and enable the data owner to create a denial shield towards the parties they are not interested or willing to share information.

In the web and online processes most data security systems are utilized and equipped with a two-step process where the first step consists with authentication of the actual and verified user onwards to the access sharing control with data monitoring in the second step. The access control process totally depends on the policies that are standardized by the stakeholders for the present and future use. This process is developed into two phases furthermore:

i. Policy determination for the access location and the authorization type

ii. The overall enforcement of the setup polices for data analysis and access by the users.

Therefore, in summary, authorization is the steps of creating a functional policy enforcement mechanism with some established standard to create a proper controlling environment in the data handling process.

3.5.3 Cryptography

Data security includes the procedure of making data safe. In this procedure, the implementation of cryptography which is encryption and decryption of data is a very crucial part. Cryptography refers to protocols which help to convert a simple plaintext into irrelevant codewords. The main purpose is to make it unreadable for third parties. The concept of cryptography has been used since ancient times. This was more prominent in the World War period as the forces used their own encryption-decryption techniques and also tried to break the codes of opponents. But the concept of modern cryptography is a bit different. The algorithms are highly mathematical which increases the computational difficulty and makes it harder to trespass.

Encryption: The process of creating or generating any layer of security to transform any data where the data in the sending process are represented differently than their actual meaning is called encryption. Encryption has four main foundations: confidentiality, authentication, integrity, and nonrepudiation [27]. The encryption process starts with the selection of the encryption system that will be used to make the information a ciphertext. After selecting the encryption method, the data is processed in an encrypted format by the relevant application and becomes ready to send to the other party. In the modern communication era, encryption is very important to keep the safety and security of sensitive personal information. In online platforms, confidential information such as passwords, card numbers, keywords are converted into the encrypted message in any browser and after completion of the process, the information is communicated with the approval party. In national security, the level and terms of encryption are broader as it deals with various threats and interested parties continuously.

Two common types of encryption methods are symmetric and asymmetric encryption. A single key is used for a symmetric method while in an asymmetric method, a public key is used for the encryption and a private key for decryption. As a result, the asymmetric method is more complicated which results in slower than the symmetric method. This symmetric method is more preferable for uploading mass volume of data. Some noteworthy symmetric methods are AES, DES, RC-4, RC-5, RC-6, Blowfish, etc.

Decryption: Decryption is the process of generating the actual meaning of any encrypted data by using the proper key to crack the encryption code. When the message is received by the last user, there are sets of codes that are to be applied against each element of encryption. These codes and systems are used as keys to form the encrypted message or data into their original form. Decryption involves the use of sets of machines and programs that are already programmed with the instructions needed to crack the encrypted codes. The same encrypted texts can generate two different data if they are decrypted using different decryption processes. Therefore, the decryption process is designed along with the encryption system altogether to maintain the surety of proper data regeneration. In modern times, there are programs that are dedicated to generating encryption and decryption keys that are unique with each separate entity in the data structure. Facebook passwords, WhatsApp messages use the most dynamic type of the decryption standard to ensure the data exchange is safe and up for maximum security.

In conclusion, proper and well-structured encryption-decryption systems can ensure the safety standard and reduce the scope of any kind of threat attacks.

3.6 Advanced Encryption Standard (AES)

AES which is also defined as Rijndael is the most developed and sophisticated encryption standard used in development of a maximized data security. From the growth of AES after developing it using block cipher, the standard has changed the scope and accuracy of overall data encryption in any possible field.

Abdullah (2017) in his research work [28] briefed in overall comparison about why AES is to be chosen as the main encryption method in any relevant case. He mentioned there were three primary measures to select AES as the standard of encryption which included: Security, Cost and Algorithm related Implementation. The key expansion of AES with the decryption process which is the reverse process of the initial encryption, devices the broader scope of security of the available data.

3.6.1 Basics of AES

AES is a block cipher that was created as a replacement for DES. The size of each block is 128 bits in AES. Three types of key lengths are used to encrypt or decrypt the blocks. The key length of 128, 192 and 256 bits needs 10, 12 and 14 rounds for the encryption/decryption process. These rounds can be divided into three kinds of rounds. The first round is called the initial round and after that the main rounds and then comes the final round. Each main round consists of 4 functions: ByteSub, ShiftRow, MixColumn and AddRoundKey. While the first round only contains AddRoundKey and the last round consists of ByteSub, ShiftRow and AddRoundKey. The ByteSub function converts the input into another value following a substitution table. ShiftRow is a 4*4 matrix that shifts the value row wise. The third function multiplies each column from the output of ShiftRow with a fixed matrix and gets another output. Lastly, AddRoundKey adds a key by running some operations with the value.

The below figure 3.4 illustrates a basic understanding of AES-128 [29].

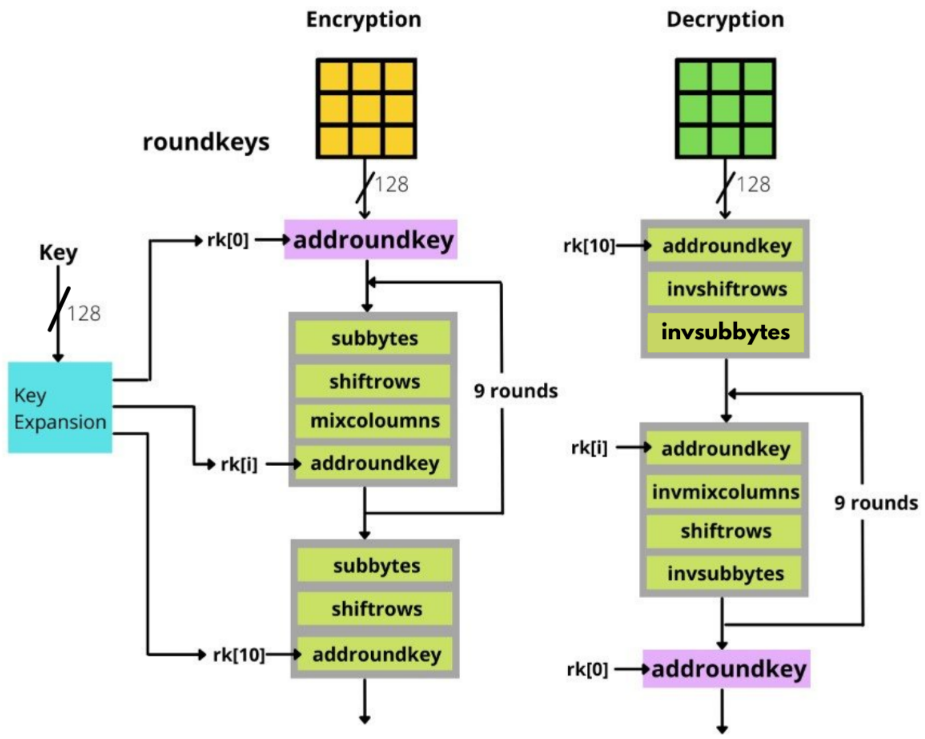


Figure 3.4: The basic AES-128 cryptographic architecture

3.6.2 Comparison between AES and a few other methods

There are various other standards such as DES, RSA, MD5, Blowfish to configure the security standard of the available data and overall comparison of AES with the other methods can be described as below:

The first paired comparison shown in table 3.1 is with the DES standard of Encryption [30].

Parameter of Comparison	**AES**	**DES**
Development Year	2000	1977
Standard Key Length	128,192,256 bits as different options	56 bits as standard
Cipher Used	Symmetric block cipher	Symmetric block cipher
Standard Block Size	128 bits of block	64 bits of block
Security	AES has a large secret key comparatively hence, more secure	DES has a smaller key which is less secure
Implementation of Hardware and Software	Better level of Implementation in hardware than software	Equal implementation in both scopes.
Speed of Encryption and Decryption	AES is faster	DES is comparatively slower

Table 3.1: Comparison table of AES vs DES

The next parameter of comparison shown in table 3.2 is measured with the standard RSA (Rivest, Shamir, and Adleman) algorithm that works with a publicly known key to initiate encryption. Babu (2016) in his research [31] described various comparison standards regarding the various important scope of features.

Parameter of Comparison	**AES**	**RSA**
Development Year	2000	1977
Standard Key Length	128,192,256 bits	Consisted of more than 1024 bits
Cipher Used	Symmetric block cipher	Symmetric block cipher
Standard Block Size	128 bits of block	512 bits as minimum size
Security	Security Level is Maximized	Less Secure than AES
Implementation of Hardware and Software	Higher and Efficient Implementation	Not efficient enough
Speed of Encryption and Decryption	Fast and Accurate	Slower and can lag at times

Table 3.2: Comparison table of AES vs RSA

Ahmed, Mahmod, Alabaichi (2013) described the overall scope and description of Blowfish Algorithm in their research work [32]. They described the infrastructure of a feasible Feistel network with iterating simple encryption. With the overall description of the procedural analysis of Blowfish Algorithm, the comparison in various features is represented in table 3.3.

Parameter of Comparison	**AES**	**Blowfish**
Development Year	2000	1993
Standard Key Length	128,192,256 bits	Consisted of 64 bits
Cipher Used	Symmetric block cipher	Symmetric block cipher
Structure	Substitution, permutation	Feistel
Security	Maximum Security	Excellent
Implementation of Hardware and Software	Higher and Efficient Implementation	Less Efficient than AES
Speed of Encryption and Decryption	Fast and Accurate	Cache can be slower
Flexibility	Higher	Higher

Table 3.3: Comparison table of AES vs Blowfish

MD5 in other words Message-Digest Algorithm which is a checking mechanism for data integrity checking was famous during the introduction but later on was found critically vulnerable for measuring security standards. Kioon, Wang and Das in their publication [33] described how the MD5 is functional in all broader security levels of data encryption and the description given there is not much relevant with the thesis and we are focusing on the features that are attributed for comparison with AES in general:

Parameter of Comparison	**AES**	**MD5**
Development Year	2000	1992
Standard Key Length	128,192,256 bits	128 bits
Cipher Used	Symmetric block cipher	Symmetric block cipher
Structure	Substitution, permutation	Feistel
Security	Maximum Security	Vulnerable
Implementation of Hardware and Software	Higher and Efficient Implementation	Less Efficient than AES
Speed of Encryption and Decryption	Fast and Accurate	Slower and risk averting
Flexibility	Higher	Moderate

Table 3.4: Comparison table of AES vs MD5

Chapter 4

Proposed Model

4.1 AES based secure EHR model with authentication

The purpose of the proposed system is to create a secure EHR model for the healthcare sector of Bangladesh which will be efficient and user friendly. The system is based on a website with separate interfaces for both medical professionals and patients. The website will have different types of actors depending on their activity including: doctor, patient, pathologist and administrator. In the proposed system, there will be authentication of the users every time they try to get access to the data. The basic concept of a web farm will be implemented here with two separate cloud servers that will be used to keep data. In our model, all the healthcare data will be divided into two categories based on their sensitivity and size. Those are: (i) personal information which are more sensitive and (ii) pathological reports which tend to be larger in size and less sensitive. Hence, personal information will be encrypted and kept in a locally set up secure private cloud server and pathological reports such as scan copies will be kept in a public cloud server.

The figure 4.1 use case diagrams showing the main points of the projects.

The whole work procedure can be divided into three important parts, maintaining data security. Those are (i) input data, (i) store data, (iii) output data.

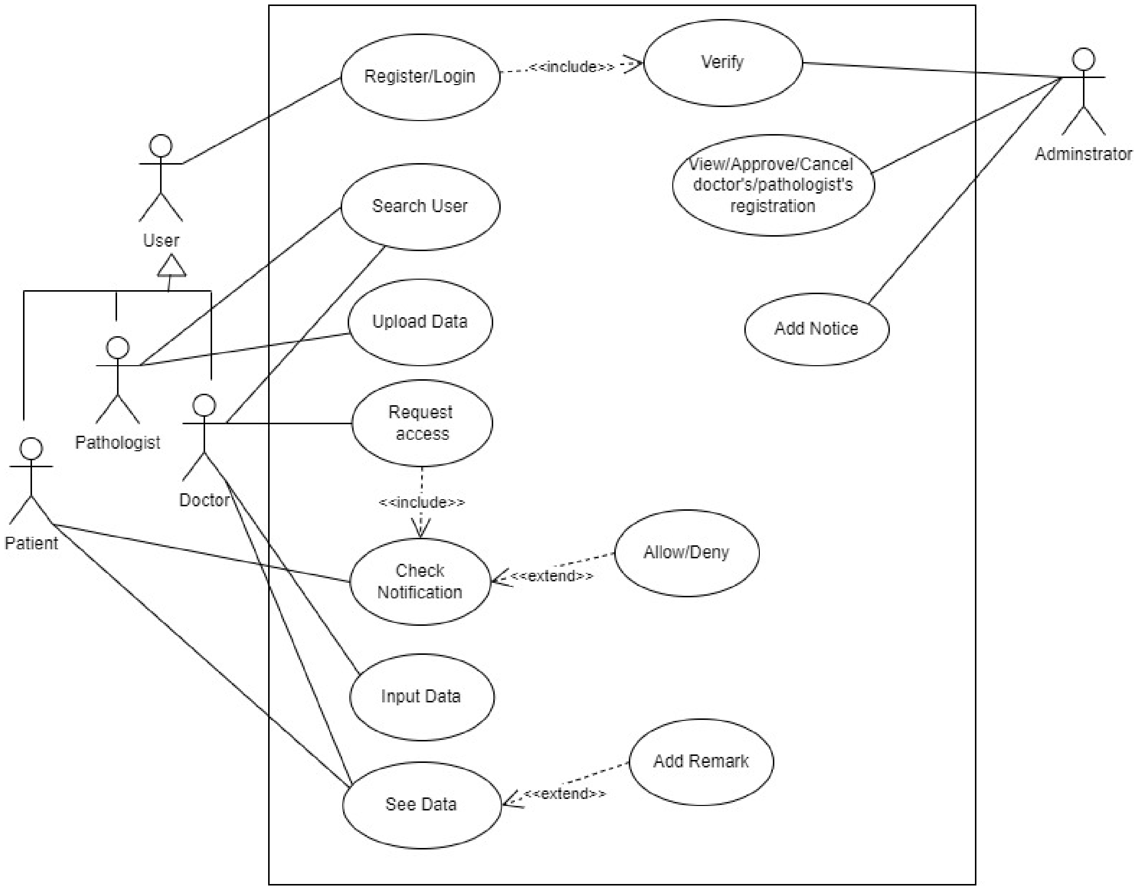


Figure 4.1: Use Case Diagram of EHR system

i. **Input data:** Only medical professionals can input and edit data in the system. The patients can input data (their information) only while registering. After that, the patient does not have the authority to input, edit or manipulate any data. Also, the pathologist can not see any patients' personal information but can upload lab reports only. Doctors can input data in the form of a prescription after getting permission from the patient. Furthermore, doctors can update the medication list and medical history of any patient.

ii. **Store Data:** All the healthcare data will be stored using a web farm of cloud servers. Everyday a lot of new healthcare data will be added to the server. Keeping and maintaining huge healthcare data in a local private server could be very expensive. On the other hand, keeping all sensitive healthcare data in a remote public cloud could make the whole system vulnerable to breach. Hence, we propose a system combining the both types of servers which will be secure enough and less costly. Mainly, two servers will be used in this model in the form of web farms, where load balancing concept will not be implemented. Other than that, both the servers will be serving different purposes. One locally set up private server for keeping the encrypted personal information of a user which is small in size and another public cloud server for keeping the pathological reports of a user which are large in size. As a result, any attack or theft on the public cloud server won't disclose any information about a patient. The public server will be linked to the private server through a secret foreign key. This will make hacking both the servers at a time quite impossible. The personal information server will be kept encrypted with AES and unauthorized persons cannot decode them even after trespassing. However, the server containing pathological reports of a patient will not be encrypted. It will minimize the cost and time of data encryption decryption. Users will be able to access these data from wherever they are, whenever they want through the internet. The doctors will be able to access the data with the permission of a patient.

iii. **Output data:** The data of a patient will be seen by both the patients and the medical professionals. However, the pathologist will not be able to see the data of a patient. Patients will see basic information and download the reports of their medical dataset whereas doctors will be able to view the descriptive information of patients dataset with access permission. The system will first decrypt the user ID from the private cloud server and match the key of that data to the public cloud server to get the pathological report of a patient. After that, the data will be shown to the user.

Here, every user needs to register themselves to the system before accessing the whole system. An administrator approves the requests of the users trying to register to the system. In this way every user will be verified by the admin. As verification is done for every user, the doctor and pathologists also get verified by the admin. So, there will be no chance of any illegitimate user to get access into the system. When a doctor tries to access a patient's data, the patient will be notified.. The doctor won't be able to access patients data unless the patient allows. The system will also use OTP because it will be easier for the general mass to understand. In this way the patient controls the access over his/her data.

The next figure 4.2 gives the basic idea of what the system will do.

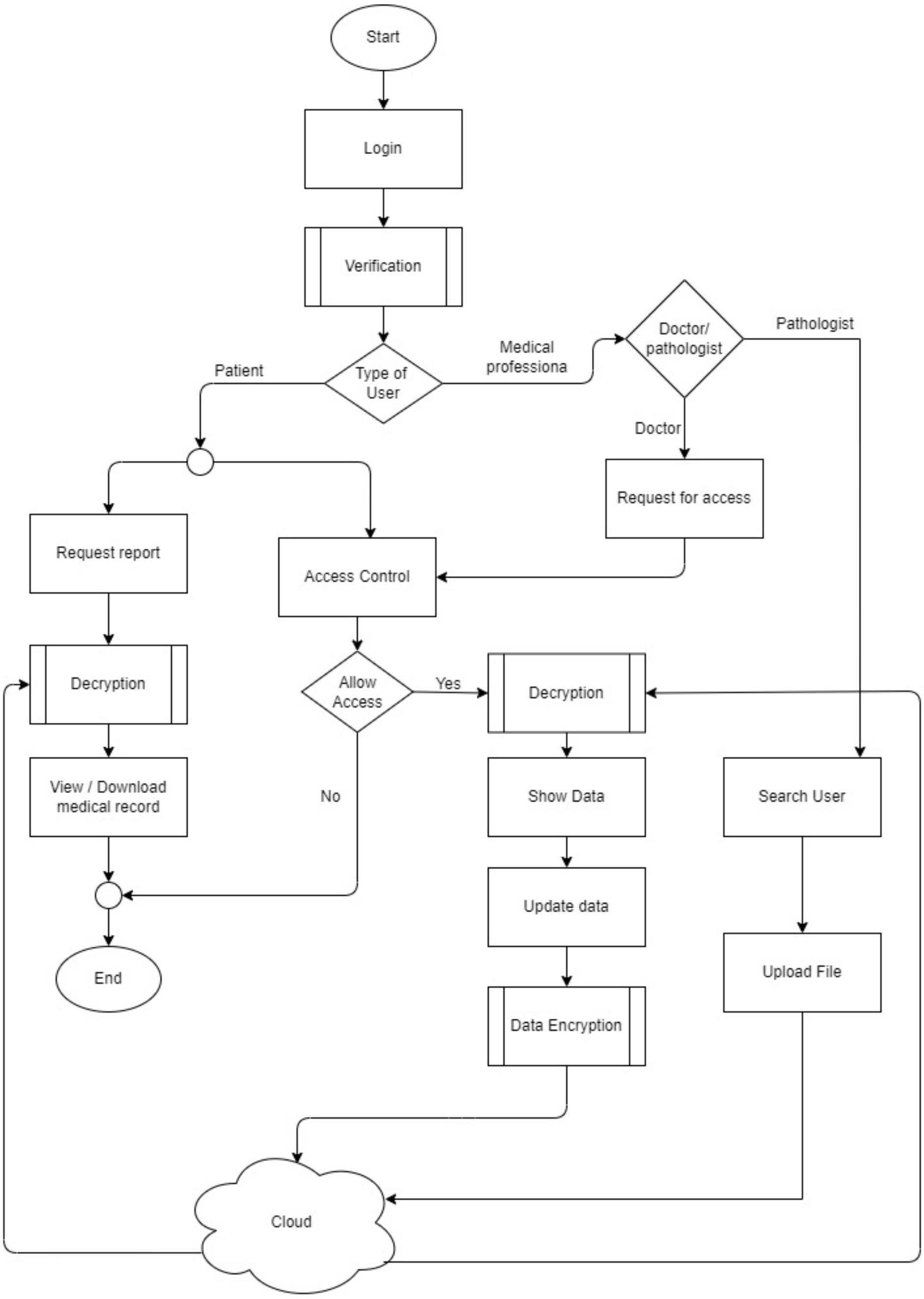


Figure 4.2: A basic model of an EHR system.

4.2 System Architecture

As a development project, it is important to understand what should be done first. For that a thorough analysis of the project is needed. The system architecture discusses the system structure and its arrangements. For this case the system architecture will be useful to produce an end product that should be a secure data keeping system with quality measures to prevent data piracy. This is also important for a better and easier user experiance.

As mentioned before, to implement the system securely with more cost and time efficiency, two servers will be set up separately with a link in between. The private server will direct to the pathological data of any specific patient. This is basically the gateway to the public cloud server where all the medical documents will be stored. This means, the public server can only be accessed through the local server. The information in the local server will be kept more secure so that the documents in the public server do not get compromised.

To develop a project, the analization of how the structure of the database will be is important. In figure 4.3, the ER diagram will help us to create the architecture of the database of the system. The following ER diagram shows the relationship between each entity associated with the database. With the help of it, the structure of the database can be visualized which will be used to keep track of the data in the system.

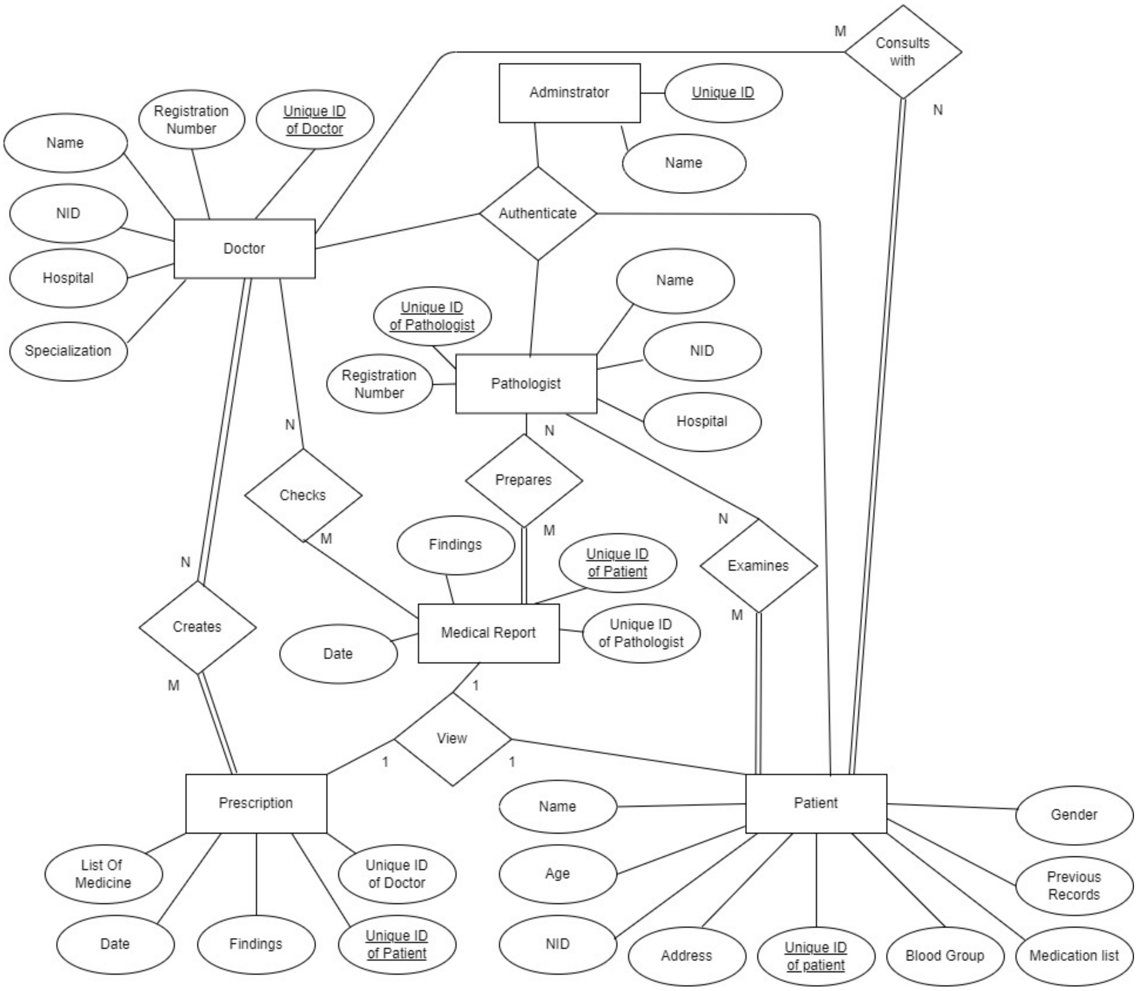


Figure 4.3: ER Diagram of EHR database system

4.2.1 Authentication

The authentication procedure starts when a user registers to the system. The system then sends an OTP to verify whether the person is the correct person or not.

After verifying by the system, there is another authentication procedure which can be governed by the administrator. The administrator will be able to see the registration number of the doctor and verify if the person is a real doctor or not before they get access to the website. Same procedure will be followed by the administrator to identify and verify other forms of user with other forms of identification.

Sentinel is one of the most popular and framework agnostic authentication and authorization packages right now. Besides authentication and authorization, registration, users & roles management, multiple sessions, custom hashing strategies etc are the key features of sentinel. It is supported by laravel framework and with the help of this package, users can be authenticated in various ways. Sentinel supports different types of authentication such as single factor authentication (SFA), Kerberos authentication, multi factor authentication (MFA), OAuth authentication etc [34]. SFA is actually the default authentication method for Sentinel. The SFA uses a password to verify a user. If the user puts the password correctly, he is authenticated. In this proposed model , multi factor authentication (MFA) will be used that will verify the user when a user tries to register or get access to any features of the system. With the help of Sentinel the administrator will be notified if a new user is trying to register into the system. Only the administrator will have the authority to see the new users trying to register into the system and approve or decline them. We will also integrate some features of the kerberos authentication system in this authentication procedure. For example, the users will get limited access to the system for a specific time period after they get authenticated. Also the timestamp of their access and activity will be stored safely for security purposes. The figure below shows the authentication from the administrator.

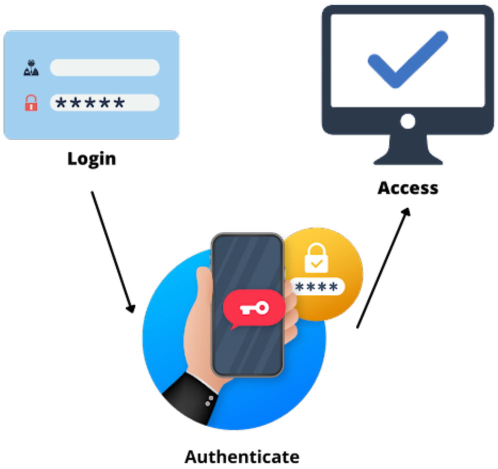


Figure 4.4: Authentication system

4.2.2 Authorization

At first to get access to the system, every user will need to register in the system and then needs to get authorized by the admin personnel. After getting the authorization by the admin users will be able to get into their own dashboard. As there will be different kinds of users in the system, their access and work in the system will also be different. In this system, only patients, pathologists and doctors will be shown as users. Here, every one of these users needs to update their data at the start of their registration. No user will further be able to change or edit their data without an admin's permission or interference.

The access in the systems will also differ from user to user. A patient will only be able to see their own medical history and reports in the dashboard. A doctor will be able to see a patient's medical data with that patient's consent. And then allowed to write prescriptions on that patient. But a pathologist will not be able to see any data on their dashboard. Pathologists are only allowed to upload a patient's test result or data in the system.

4.2.3 Communication Between Servers

On our system, we plan to use two different servers to store our data. These two servers have their own parts in their system. Between the two servers, one will be a private or local server whereas the other will be a public server. The private server will have all the personal information about a patient, whereas the third party server will have all the pathological reports of the patients. Whenever our user tries to fetch any data from the website, there will be communication between these two servers.

For patients, whenever they want to see their data from the website, they will first be visited to the local server where they will be verified. Then the local server will communicate with the public server where all the pathological reports of the users are and that public server will send the information to the user's device.

Then in a doctor's case things get a little complicated as whenever a doctor tries to access a patient's information they need to get that access from the patient.

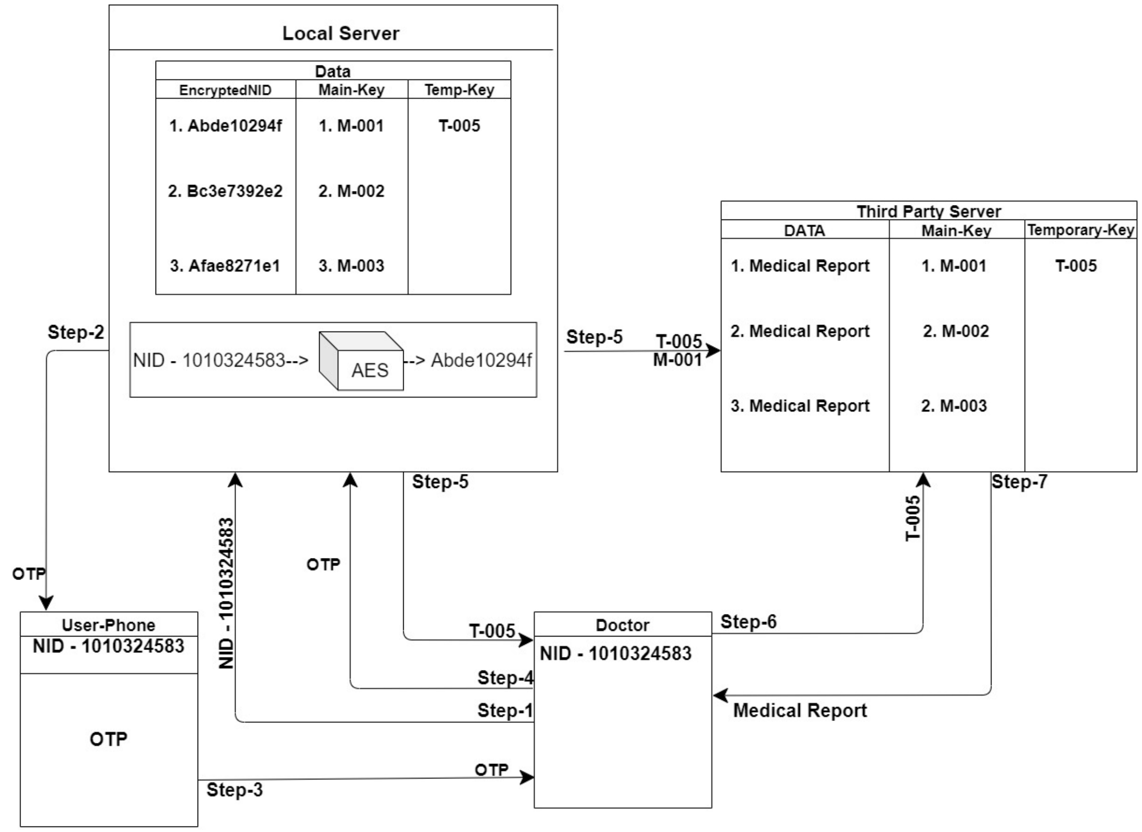


Figure 4.5: Authorization and Communication between Servers.

The diagram in figure 4.5, shows the encrypted data in the local server, authorization from the patient to access the data and communication between the two servers and doctor. After a doctor gets accessed to the local server, he can search the ID of a patient on the local server. The IDs and all other information of the patient is stored encrypted in the server. So when a doctor searches, the ID will get encrypted first and then it will find out the match. After the doctor finds the patient's profile he can ask for access to data. The patient will get an OTP code in his phone immediately. The patient will allow access to the data by providing the OTP to the doctor. After the doctor enters the OTP in the system, he will be directed to the data server and will be given a temporary key. The same key will be sent from the local server to the second server at once. The doctor will enter the code to the data server, if both the keys match then the doctor will be able to see all the medical documents of the patient. If the code doesn't match, there will be an error report. All these communications in the system will be secured using Symmetric cryptography, to be more precise AES algorithm. AES has been selected because it is a mathematically more efficient and advanced cryptographic algorithm. It also supports various key lengths. AES gives the option to choose a 128-bit, 192-bit or 256-bit key.

In the case of pathologists, the system almost works like the patients. As pathologists are only supposed to upload data in the system, they at first like any other user will get verified by the local server. Then pathologists will search patients by their id's and then the local server will communicate with the public server and then pathologists will be able to upload the data which will be saved in the public server.

4.2.4 The Central Administration Of The System

The Administrator will have the authority to control and manage the whole system. Action will be taken immediately if any kind of discrepancy is noticed by the administrator. Any unusual activities like trying to log in several times using the wrong password or giving the wrong OTP several times will result in sending a notification to the administrator. The administrator will be able to observe the scenario and take necessary steps accordingly. He will also be able to track any user with their IP address, browser agent, etc, and can observe their activity in the system. The process of accepting or declining any user registering for the first time in the system will depend on the administrator. Hence, the administrator will match the registration key of the doctor and pathologist to verify their identity. However, the patient's verification will be done with the NID or birth certificate number of the patient. This process will make sure that each patient will have only one account. The administrator will also have the authority to disable a user anytime from the system restricting the user from future access to the system. Furthermore, alll the users combinedly or separately can be contacted by email from the admin's panel.

4.3 Workflow

The system is built in a way to service three types of users: doctors, patients and pathologists. The workflow would vary according to the user. The users get different interfaces and activity lists when they login to the system. As the interfaces are different, the workflow can be drawn from three different perspectives. Doctor's, patient's and pathologist's.

4.3.1 Workflow Of Patient

Below in figure 4.6 is shown the activity diagram of the system in response to the perspective of a patient. The activity diagram clearly describes how the patient and the interfaces are working.

it is showing that the users can log in or register in the system after the authentication. Then they can view their personal information and medical reports from the EHR. However, a patient can not input data or edit medical data. Patients can also see their medical history and any appointments of them with the doctors. Also, they will be able to download their data into their devices.

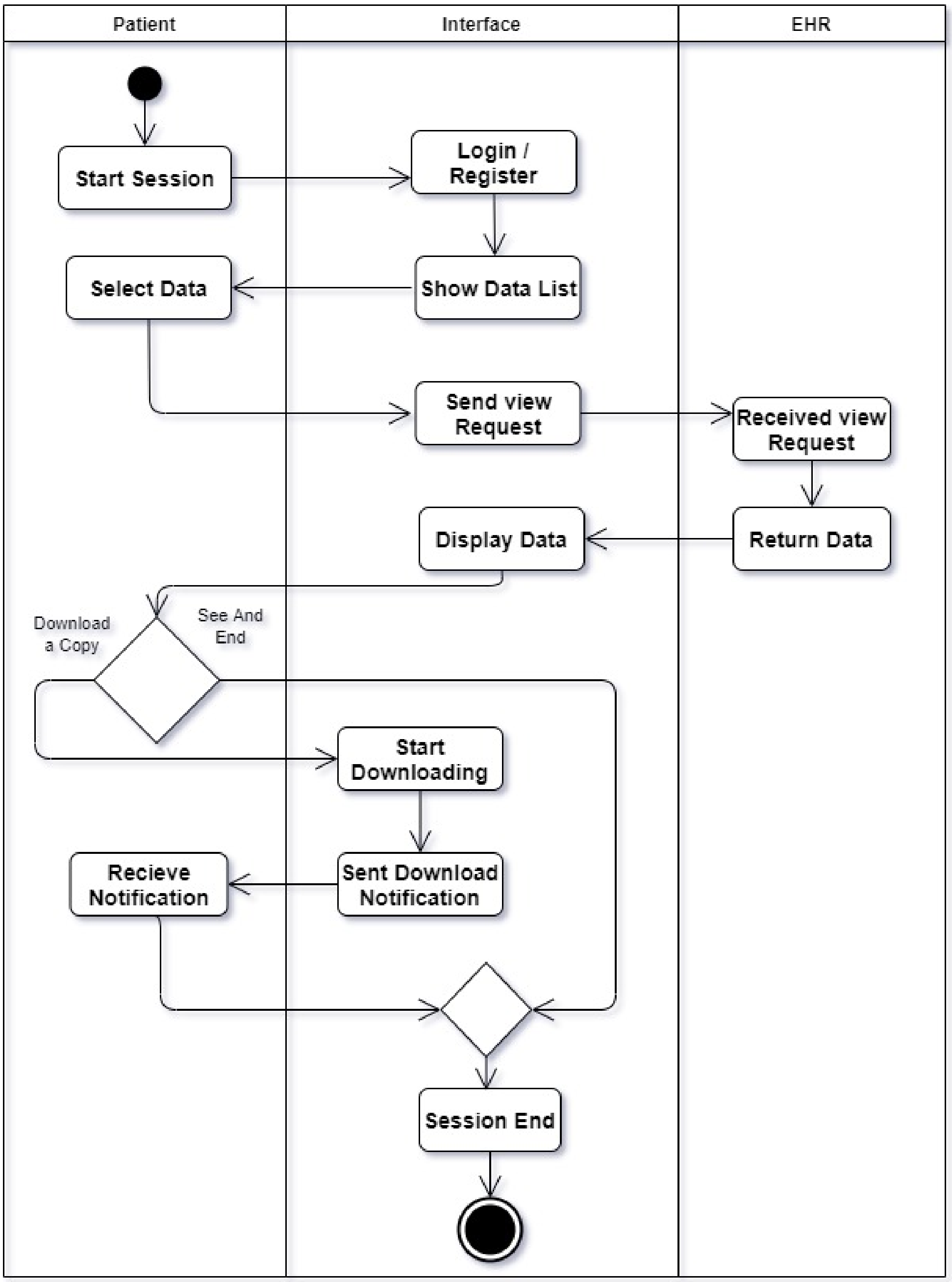


Figure 4.6: Activity diagram of the system - Patient's perspective

4.3.2 Workflow Of Pathologist

In figure 4.7, the activity diagram in response to pathologists is given. The pathologists have the responsibility to examine patients or perform various lab testing. The results of those tests are uploaded matching the patients' ID's by the pathologists. They can only search the patients' ID's and upload reports or tested results to their accounts. However, any other information of the patients are not visible to the pathologists including the personal information. Also, they are not allowed to download any additional data from the patients' accounts. As every login session is timed, the pathologists will be logged out of the system after that time bound.

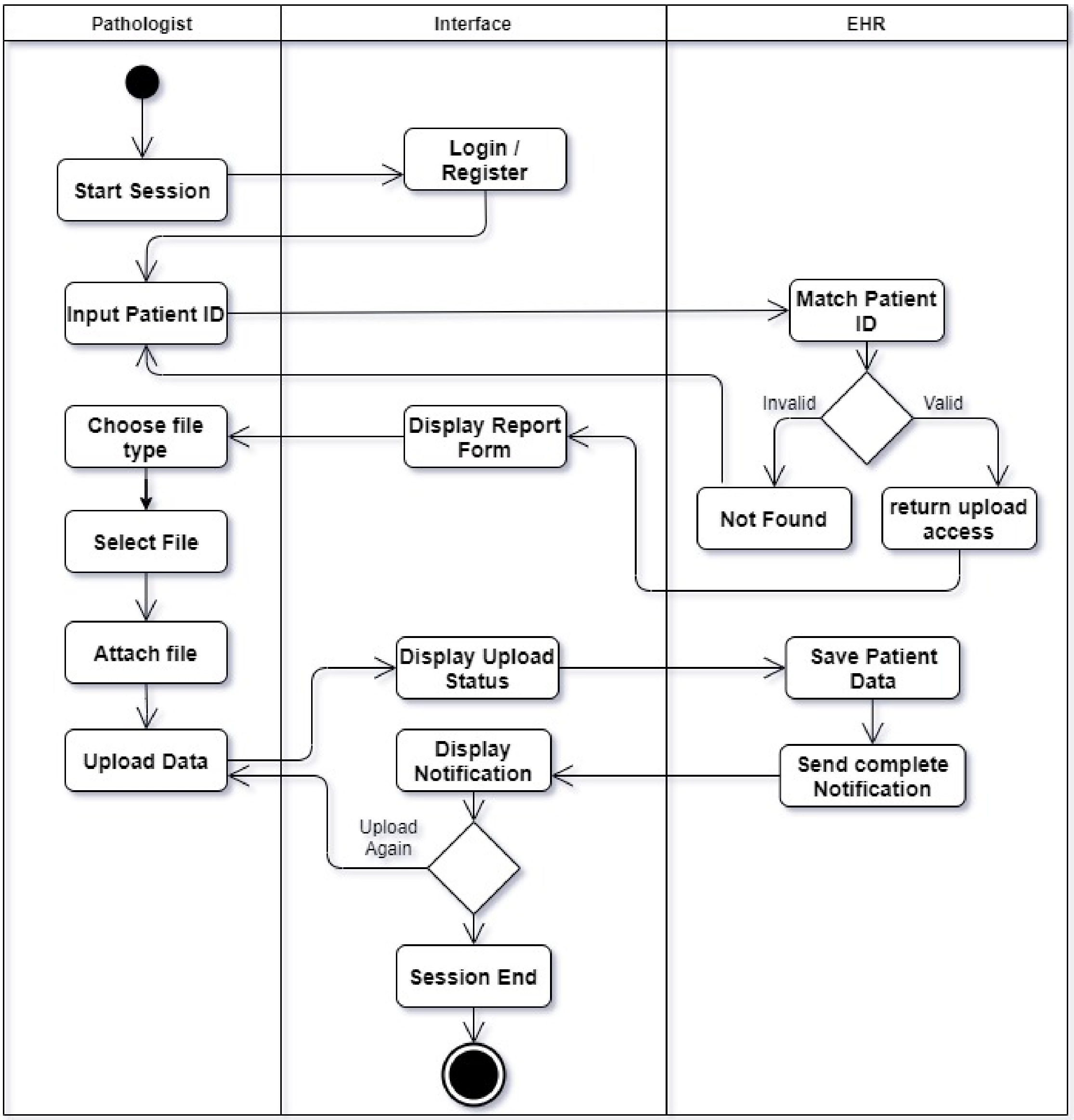


Figure 4.7: Activity diagram of the system - Pathologist's perspective

4.3.3 Workflow Of Doctor

In figure 4.8, the activity diagram for doctors is shown. A doctor can not access a patient's data without their consent. So, an OTP is sent to the user once a doctor wants to access their medical history. Doctors can search any patient's ID and request the patients to access their accounts. Doctors can access their data by getting the OTP that was sent for authorization permission from the patients. A doctor can also download the data of a patient. Every login session will have a time limit. After that time the doctors will be logged out of the system. As a result, the access of the patient's account will no longer be available to the doctors. If a doctor wants to access a patient's account for the second time, the doctor needs to request for access again.

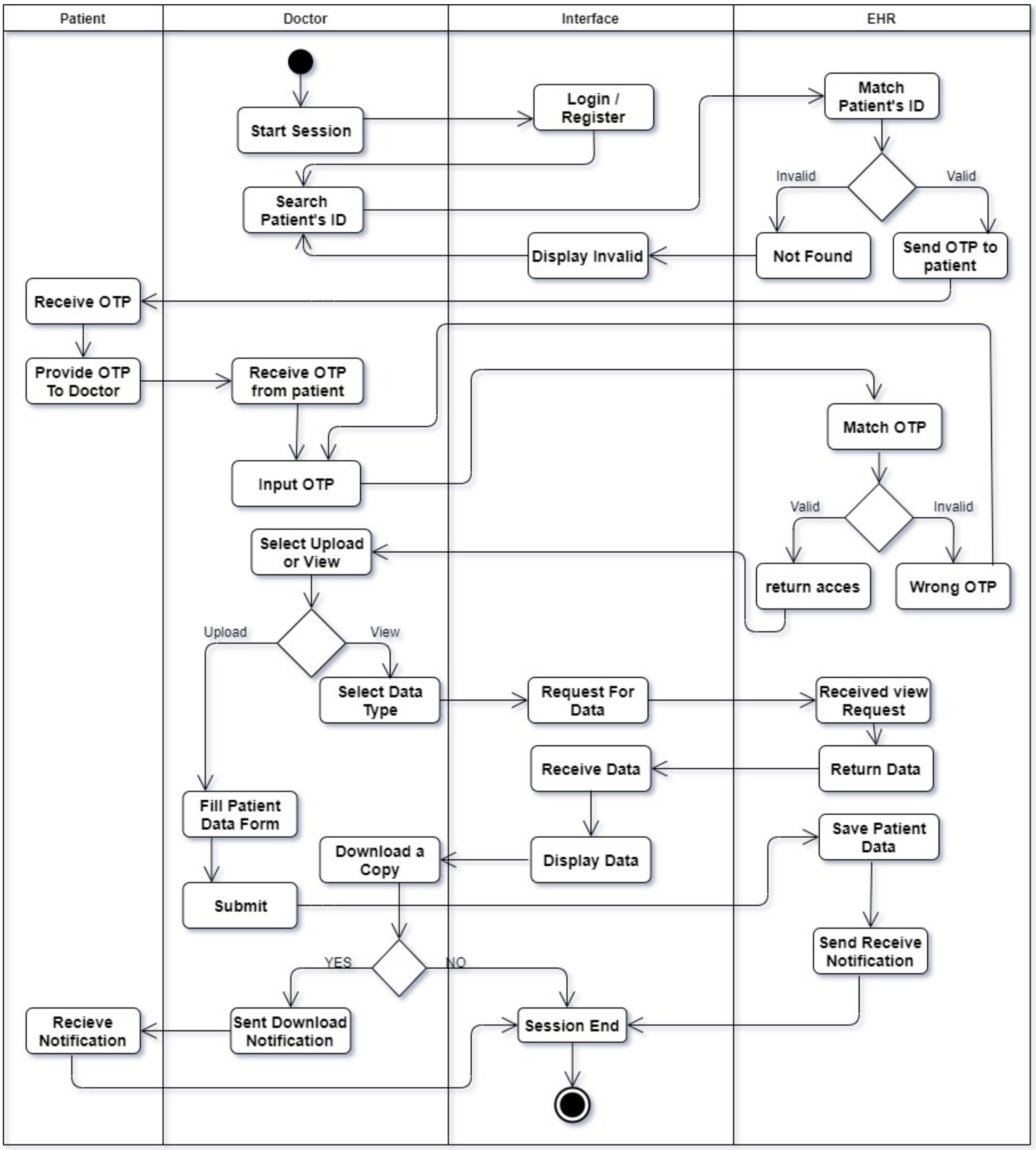


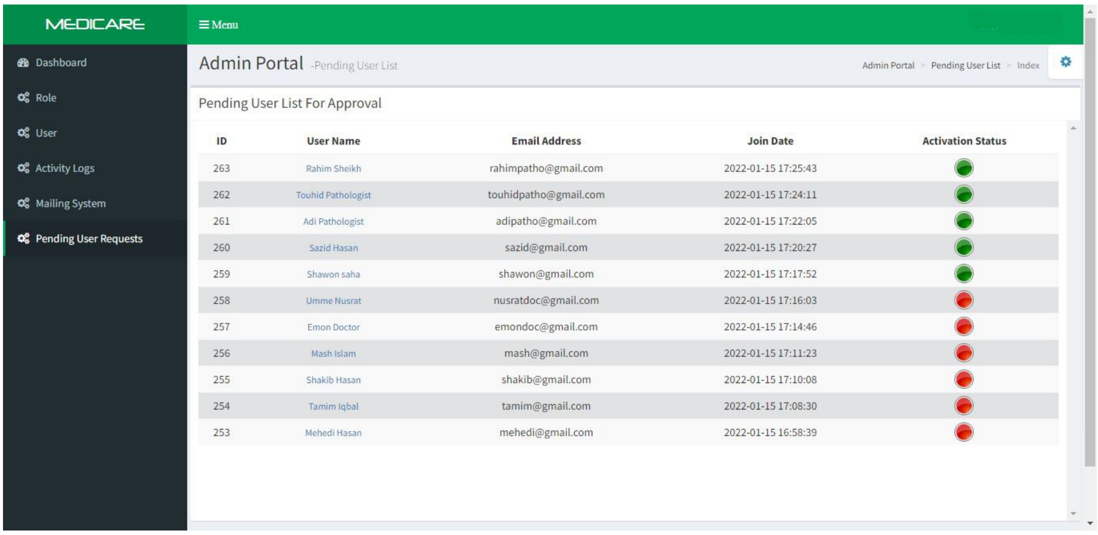
Figure 4.8: Activity diagram of the system - Doctor's perspective

Chapter 5

Experimental Evalution

5.1 Experimental Implementation

The EHR system that is implemented here is named 'Medicare'. Medicare is a web-based secure application that has a simple and easily understandable interface. The System has a login and registration page. Every user needs to register to the system before accessing the features of medicare. While registering the user needs to enter their personal information including their national ID number. The National ID is verified by the administrator. Without verification, no user will have permission to access the system as the admin will not approve them. The website is very lightweight and accessible through different devices such as mobile phones, tablets, etc. The following figure 5.1, shows the admin approval system.



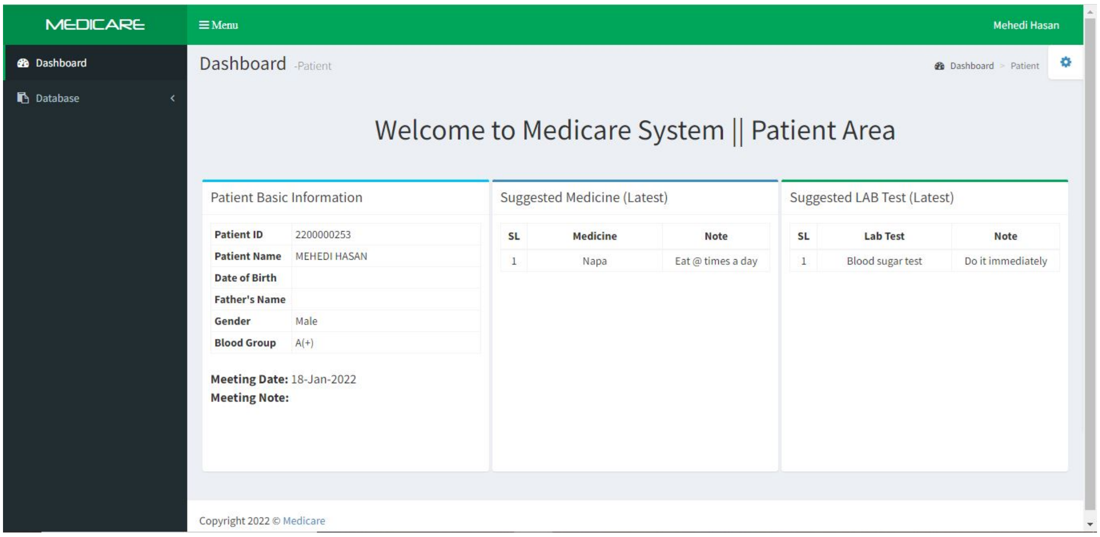
Pending User List For Approval

ID	User Name	Email Address	Join Date	Activation Status
263	Rahim Sheikh	rahimpatho@gmail.com	2022-01-15 17:25:43	🟢
262	Touhid Pathologist	touhidpatho@gmail.com	2022-01-15 17:24:11	🟢
261	Adi Pathologist	adipatho@gmail.com	2022-01-15 17:22:05	🟢
260	Sazid Hasan	sazid@gmail.com	2022-01-15 17:20:27	🟢
259	Shawon saha	shawon@gmail.com	2022-01-15 17:17:52	🟢
258	Umme Nusrat	nusratdoc@gmail.com	2022-01-15 17:16:03	🔴
257	Emon Doctor	emondoc@gmail.com	2022-01-15 17:14:46	🔴
256	Mash Islam	mash@gmail.com	2022-01-15 17:11:23	🔴
255	Shakib Hasan	shakib@gmail.com	2022-01-15 17:10:08	🔴
254	Tamim Iqbal	tamim@gmail.com	2022-01-15 17:08:30	🔴
253	Mehedi Hasan	mehedi@gmail.com	2022-01-15 16:58:39	🔴

Figure 5.1: Admin Portal Of Activating Users

The national ID also makes sure that every single user has only one account and prevents a single user from creating multiple accounts. After getting access, the users can log into their accounts. Every login session is 60 minutes, so users will be logged out of the system after the login session ends. After login different interfaces will be shown to the different users.

The patient's dashboard contains the patient's basic information, suggested medicine list, and suggested lab test. There is an option called meeting where patients can also make appointments with a doctor by searching the doctor's name. A patient also has the ability to give access only to the doctors they wanted to. There is another option called medical history where the patients can see their medical history of medicines and a doctor's note and lab reports. The following figure 5.2, shows how the patient dashboard will look like.



Welcome to Medicare System || Patient Area

Patient Basic Information

Patient ID	2200000253
Patient Name	MEHEDI HASAN
Date of Birth	
Father's Name	
Gender	Male
Blood Group	A(+)

Meeting Date: 18-Jan-2022
Meeting Note:

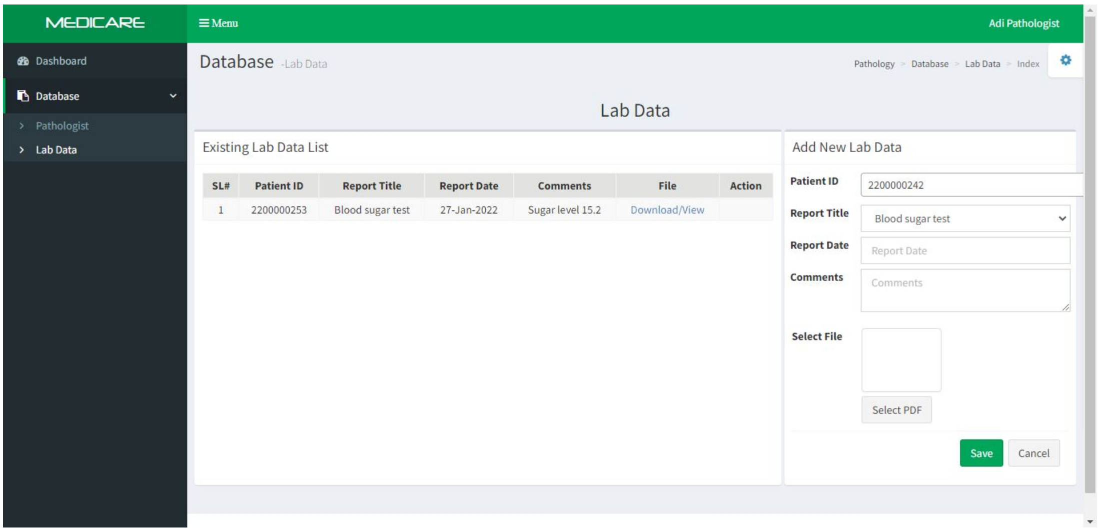
Suggested Medicine (Latest)

SL	Medicine	Note
1	Napa	Eat @ times a day

Suggested LAB Test (Latest)

SL	Lab Test	Note
1	Blood sugar test	Do it immediately

Figure 5.2: Dashboard Of Patient



Lab Data

Existing Lab Data List

SL#	Patient ID	Report Title	Report Date	Comments	File	Action
1	2200000253	Blood sugar test	27-Jan-2022	Sugar level 15.2	Download/View	

Add New Lab Data

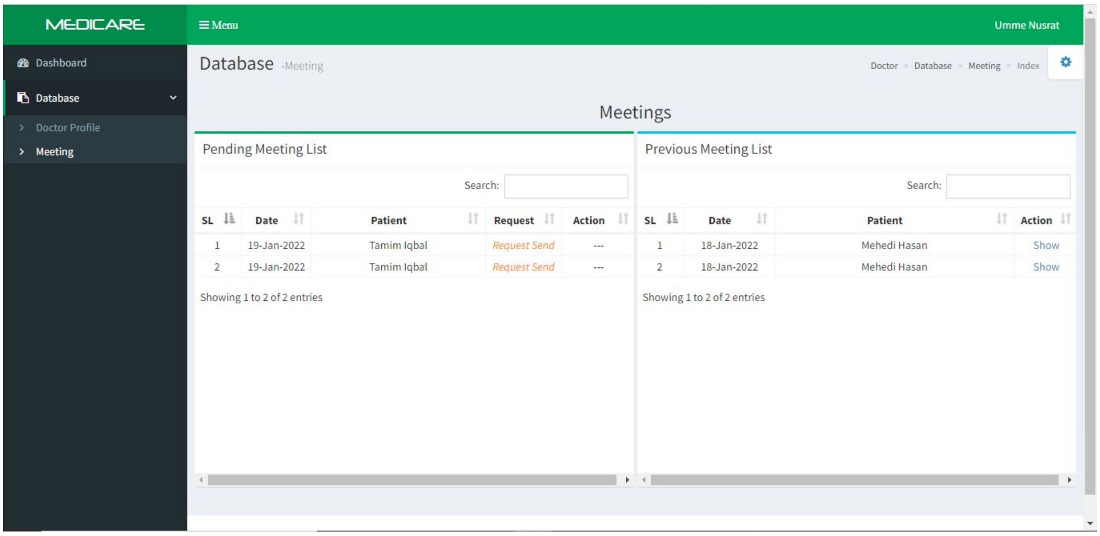
Patient ID	2200000242
Report Title	Blood sugar test
Report Date	Report Date
Comments	Comments
Select File	

Figure 5.3: Dashboard of Pathologist

The pathologist's dashboard is the simplest. They can only upload the lab data of the patients. From the interface, they will be able to find a patient, select a report type and date of the upload, and comment on the lab if any. Pathologists will only be able to upload the lab reports to a patient's profile that has been suggested by the doctors. They will be able to see the lab reports uploaded by them in the last

24 hours timeline. Furthermore, they will be able to edit them if necessary for a limited amount of time. The figure 5.3, views the dashboard of a pathologist.

In the doctor's dashboard, they will be able to see a pending meeting list side by side with a previous meeting list. On the pending meeting list, the doctor will be able to see all the pending requests from the patient. If a doctor accepts any of the requests, a patient then needs to allow the doctor to see their details. After getting the approval to see a patient's details, a doctor can access the patient's medical history. The doctor then will be able to see the patient's details, patient's previous medical history, and the patient's lab reports. Then there is a prescription interface where the doctor will be able to give necessary medication to the patient and give a note on that. On the prescription interface, the doctor can also suggest a lab report to the patient. These things will then be updated to the current meeting's medical details. The figure 5.4, shows the working dashboard of a doctor.



Database -Meeting

Meetings

Pending Meeting List

Search:

SL	Date	Patient	Request	Action
1	19-Jan-2022	Tamim Iqbal	Request Send	---
2	19-Jan-2022	Tamim Iqbal	Request Send	---

Showing 1 to 2 of 2 entries

Previous Meeting List

Search:

SL	Date	Patient	Action
1	18-Jan-2022	Mehedi Hasan	Show
2	18-Jan-2022	Mehedi Hasan	Show

Showing 1 to 2 of 2 entries

Figure 5.4: Dashboard Of Doctor

5.1.1 Technology And Framework

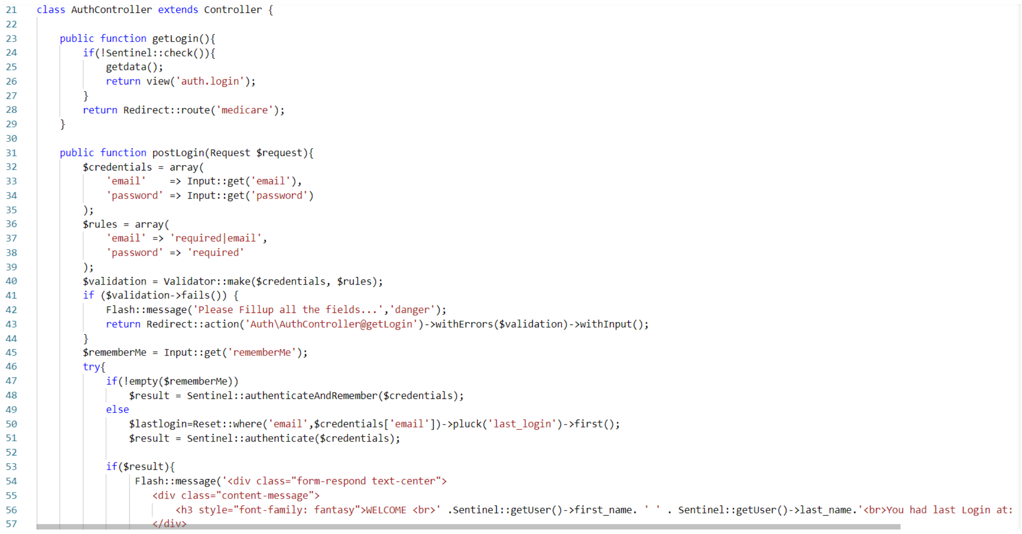
Medicare is developed with PHP and the framework that has been used to develop the website is Laravel. Laravel is used as it is a fast, secure and convenient framework for developing purposes. Laravel framework makes it easy to organize and connect. Laravel is great in terms of security for any web application. It has many inbuilt security features and packages to prevent various types of attacks and common vulnerabilities [35]. Laravel helps to use everything securely and keeps all the data sanitized where needed. Also, while programming with a database structure, it becomes easier to communicate using the laravel framework.

To host the website and control all the tools, the web application is deployed using cPanel after development. With the help of cPanel, the server and domain can be maintained keeping all the web files organized. cPanel helps to manage a server providing necessary tools where one can find everything needed to host a website and manage a server. Every cPanel has an additional storage to keep the necessary files and database in it. Clicking the disk usage option in cPanel shows the space taken by the directories, subdirectories, and other options. As cPanel has some storage for each user account, it can act as a server for storing necessary files. So, cPanel is used both as a control panel and a live server for this project.

For storing data organized, retrieving them easily, and running queries, Medicare uses MySQL as a relational database management system. It is a link between a user and the database of a cloud-native web application. It's frequently used with PHP scripts to build sophisticated and dynamic server-side or web-based organizational applications [36]. Users can read, update, delete or create new data in the database of the application with this. In the system, we have two types of tables: encrypted and unencrypted. Some of the tables contain very sensitive healthcare data, hence all the cells are kept encrypted there. They are encrypted at the time of their input and they are decrypted before retrieving.

5.1.2 Authentication With Sentinel

Authentication is handled by Sentinel. For login purposes, SFA is provided by the Sentinel. After the user puts the password to log in, the password is hashed and saved. When a user tries to log in again, the password that is input during the login session is also hashed and compared with the password that was saved before. When both the hash value matches the user is given access to the website to continue. Also, every user's national ID That is given during registration is used to authenticate if a person is real or not. The following figure 5.5, shows the use of sentinel for the authentication purpose.



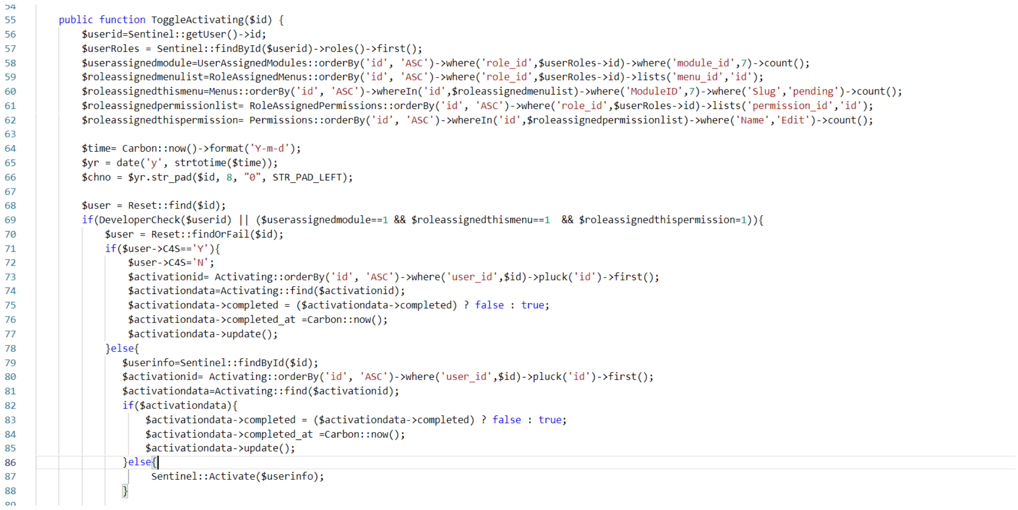
```
class AuthController extends Controller {

    public function getLogin(){
        if(!Sentinel::check()){
            getdata();
            return view('auth.login');
        }
        return Redirect::route('medicare');
    }

    public function postLogin(Request $request){
        $credentials = array(
            'email'    => Input::get('email'),
            'password' => Input::get('password')
        );
        $rules = array(
            'email' => 'required|email',
            'password' => 'required'
        );
        $validation = Validator::make($credentials, $rules);
        if ($validation->fails()) {
            Flash::message('Please Fillup all the fields...','danger');
            return Redirect::action('Auth\AuthController@getLogin')->withErrors($validation)->withInput();
        }
        $rememberMe = Input::get('rememberMe');
        try{
            if(!empty($rememberMe))
                $result = Sentinel::authenticateAndRemember($credentials);
            else
                $lastlogin=Reset::where('email',$credentials['email'])->pluck('last_login')->first();
                $result = Sentinel::authenticate($credentials);

            if($result){
                 Flash::message('<div class="form-respond text-center">
                    <div class="content-message">
                        <h3 style="font-family: fantasy">WELCOME <br>' .Sentinel::getUser()->first_name. ' ' . Sentinel::getUser()->last_name.'<br>You had last Login at:
                    </div>
```

Figure 5.5: Using Sentinel For Authentication

In the figure, the function getLogin will be called whenever a user tries to login to the ‘Medicare’. If the login procedure is not authenticated by Sentinel, the user will be redirected to the login page again. Also at line 31, the function postLogin checks if the credentials of the user are alright or not. The fields are checked in line 36. If the fields are empty, the user will be asked to give credentials again. The function will also check the validation of the email and password and then match the hashed password for authentication. After login the function also shows the time of last login.

5.1.3 Authorization Implementation

The authorization procedure starts from the very beginning when the users are given permission to access the websites by the admin. Each role is given to the user by the admin after the authentication. The following figure 5.6, shows the implementation of the procedure of activating the users and making them authorized by the administrator.

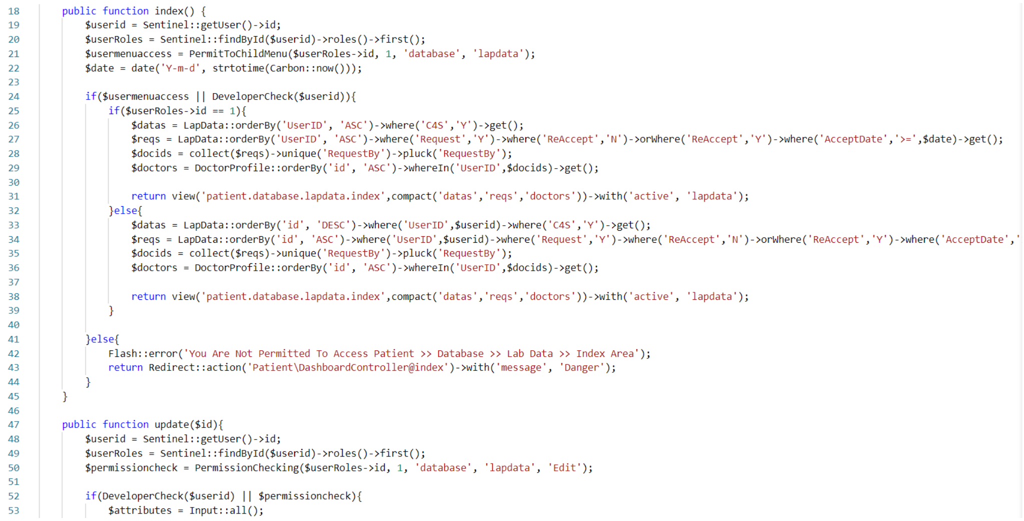


```
55      public function ToggleActivating($id) {
56          $userid=Sentinel::getUser()->id;
57          $userRoles = Sentinel::findById($userid)->roles()->first();
58          $userassignedmodule=UserAssignedModules::orderBy('id', 'ASC')->where('role_id',$userRoles->id)->where('module_id',7)->count();
59          $roleassignedmenulist=RoleAssignedMenus::orderBy('id', 'ASC')->where('role_id',$userRoles->id)->lists('menu_id','id');
60          $roleassignedthismenu=Menus::orderBy('id', 'ASC')->whereIn('id',$roleassignedmenulist)->where('ModuleID',7)->where('Slug','pending')->count();
61          $roleassignedpermissionlist= RoleAssignedPermissions::orderBy('id', 'ASC')->where('role_id',$userRoles->id)->lists('permission_id','id');
62          $roleassignedthispermission= Permissions::orderBy('id', 'ASC')->whereIn('id',$roleassignedpermissionlist)->where('Name','Edit')->count();
63
64          $time= Carbon::now()->format('Y-m-d');
65          $yr = date('y', strtotime($time));
66          $chno = $yr.str_pad($id, 8, "0", STR_PAD_LEFT);
67
68          $user = Reset::find($id);
69          if(DeveloperCheck($userid) || ($userassignedmodule==1 && $roleassignedthismenu==1  && $roleassignedthispermission=1)){
70              $user = Reset::findOrFail($id);
71              if($user->C4S=='Y'){
72                  $user->C4S='N';
73                  $activationid= Activating::orderBy('id', 'ASC')->where('user_id',$id)->pluck('id')->first();
74                  $activationdata=Activating::find($activationid);
75                  $activationdata->completed = ($activationdata->completed) ? false : true;
76                  $activationdata->completed_at =Carbon::now();
77                  $activationdata->update();
78              }else{
79                 $userinfo=Sentinel::findById($id);
80                 $activationid= Activating::orderBy('id', 'ASC')->where('user_id',$id)->pluck('id')->first();
81                 $activationdata=Activating::find($activationid);
82                 if($activationdata){
83                     $activationdata->completed = ($activationdata->completed) ? false : true;
84                     $activationdata->completed_at =Carbon::now();
85                     $activationdata->update();
86                 }else{
87                      Sentinel::Activate($userinfo);
88                 }
```

Figure 5.6: Implementation Of User Activation Procedure

Here, the function ToggleActivation first fetches the user ID. Matching the ID the roles and module lists are put into variables. There is also a variable called ‘$time’ that saves the timeframe of that moment at line 64. In line number 69, the if condition checks if the user ID is verified and checked by the admin or not. If it is checked, the user will be activated and all the modules and menus will be available for the user.

Furthermore, the doctor-patient permission procedure is also implemented. The following figure shows the codes that were implemented for the procedure.



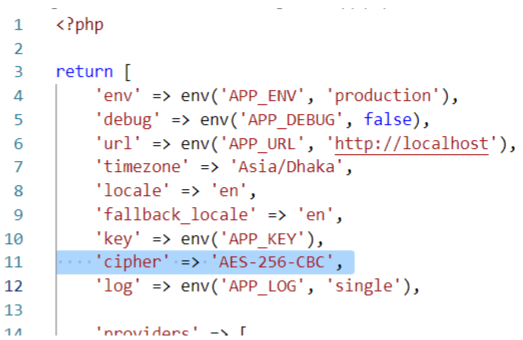
```php
    public function index() {
        $userid = Sentinel::getUser()->id;
        $userRoles = Sentinel::findById($userid)->roles()->first();
        $usermenuaccess = PermitToChildMenu($userRoles->id, 1, 'database', 'lapdata');
        $date = date('Y-m-d', strtotime(Carbon::now()));

        if($usermenuaccess || DeveloperCheck($userid)){
            if($userRoles->id == 1){
                $datas = LapData::orderBy('UserID', 'ASC')->where('C4S','Y')->get();
                $reqs = LapData::orderBy('UserID', 'ASC')->where('Request','Y')->where('ReAccept','N')->orWhere('ReAccept','Y')->where('AcceptDate','>=',$date)->get();
                $docids = collect($reqs)->unique('RequestBy')->pluck('RequestBy');
                $doctors = DoctorProfile::orderBy('id', 'ASC')->whereIn('UserID',$docids)->get();

                return view('patient.database.lapdata.index',compact('datas','reqs','doctors'))->with('active', 'lapdata');
            }else{
                $datas = LapData::orderBy('id', 'DESC')->where('UserID',$userid)->where('C4S','Y')->get();
                $reqs = LapData::orderBy('id', 'ASC')->where('UserID',$userid)->where('Request','Y')->where('ReAccept','N')->orWhere('ReAccept','Y')->where('AcceptDate','
                $docids = collect($reqs)->unique('RequestBy')->pluck('RequestBy');
                $doctors = DoctorProfile::orderBy('id', 'ASC')->whereIn('UserID',$docids)->get();

                return view('patient.database.lapdata.index',compact('datas','reqs','doctors'))->with('active', 'lapdata');
            }

        }else{
            Flash::error('You Are Not Permitted To Access Patient >> Database >> Lab Data >> Index Area');
            return Redirect::action('Patient\DashboardController@index')->with('message', 'Danger');
        }
    }

    public function update($id){
        $userid = Sentinel::getUser()->id;
        $userRoles = Sentinel::findById($userid)->roles()->first();
        $permissioncheck = PermissionChecking($userRoles->id, 1, 'database', 'lapdata', 'Edit');

        if(DeveloperCheck($userid) || $permissioncheck){
            $attributes = Input::all();
```

Figure 5.7: Implementation Of Authorization Permission

In the figure 5.7, inside the function 'index' the if condition checks if the doctor has permission to access the data of the patient or not. If the access is given by the patient, the variable '$usemenuaccess'will be true and the function will fetch the user data from the database with the patient's ID and the doctor will get authorization of adding or updating patient's data. On the other hand, if it goes to the else condition, the doctor will not be able to access and a pop up message will appear containing "You are not permitted to access this patient" to the doctor's screen.

5.1.4 Encryption

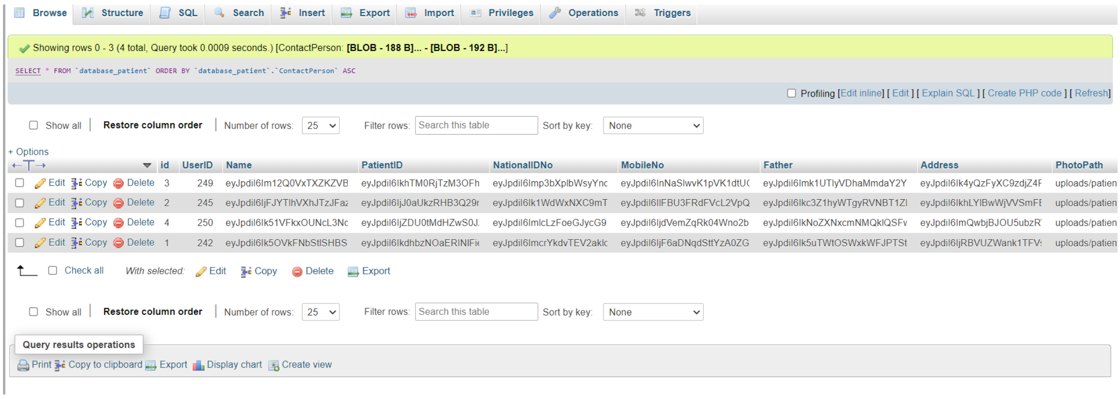
For encryption AES-256 is used at line 11. The following figure 5.8, shows the 'AES-256-CBC' function that is called and saved as 'cipher'. When encryption is needed, 'cipher' is called and used before data.



```php
 1  <?php
 2
 3  return [
 4      'env' => env('APP_ENV', 'production'),
 5      'debug' => env('APP_DEBUG', false),
 6      'url' => env('APP_URL', 'http://localhost'),
 7      'timezone' => 'Asia/Dhaka',
 8      'locale' => 'en',
 9      'fallback_locale' => 'en',
10      'key' => env('APP_KEY'),
11      'cipher' => 'AES-256-CBC',
12      'log' => env('APP_LOG', 'single'),
13
14      'providers' => [
```

Figure 5.8: Implementing Encryption Method Of Block Cipher AES

After the encryption of the personal information of the users, the data will be saved in the database. This encryption procedure takes place when the personal information or medication is given input. The input data becomes encrypted and the plaintext is converted to ciphertext. As a result, the database of the personal information will contain the ciphertext only. This is done to prevent any kind of leak or privacy threat of the data.



Showing rows 0 - 3 (4 total, Query took 0.0009 seconds.) [ContactPerson: **[BLOB - 188 B]... - [BLOB - 192 B]...]**

```
SELECT * FROM `database_patient` ORDER BY `database_patient`.`ContactPerson` ASC
```

☐ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

☐ Show all | **Restore column order** | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

	id	UserID	Name	PatientID	NationalIDNo	MobileNo	Father	Address	PhotoPath
☐ Edit Copy Delete	3	249	eyJpdil6Im12Q0VxTXZKZVB	eyJpdil6IkhTM0RjTzM3OFh	eyJpdil6Imp3bXplbWsyYnc	eyJpdil6InNaSlwvK1pVK1dtU	eyJpdil6Imk1UTlyVDhaMmdaY2Y	eyJpdil6Ik4yQzFyXC9zdjZ4F	uploads/patien
☐ Edit Copy Delete	2	245	eyJpdil6IjFJYTlhVXhJTzJFaz	eyJpdil6IjJ0aUkzRHB3Q29	eyJpdil6Ik1WdWxNXC9mT	eyJpdil6IlFBU3FRdFVcL2VpQ	eyJpdil6Ikc3Z1hyWTgyRVNBT1Z	eyJpdil6IkhLYlBwWjVVSmFE	uploads/patien
☐ Edit Copy Delete	4	250	eyJpdil6Ik51VFkxOUNcL3Nc	eyJpdil6IjZDU0tMdHZwS0J	eyJpdil6ImlcLzFoeGJycG9	eyJpdil6IjdVemZqRk04Wno2b	eyJpdil6IkNoZXNxcmNMQklQSFv	eyJpdil6ImQwbjBJOU5ubzR	uploads/patien
☐ Edit Copy Delete	1	242	eyJpdil6Ik5OVkFNbStlSHBS	eyJpdil6IkdhbzNOaERINlFi	eyJpdil6ImcrYkdvTEV2aklc	eyJpdil6IjF6aDNqdSttYzA0ZG	eyJpdil6Ik5uTWtOSWxkWFJPTSt	eyJpdil6IjRBVUZWank1TFV	uploads/patien

☐ Check all *With selected:* Edit Copy Delete Export

☐ Show all | **Restore column order** | Number of rows: 25 Filter rows: Search this table Sort by key: None

Query results operations

Print Copy to clipboard Export Display chart Create view

Figure 5.9: Encrypted Data In Database

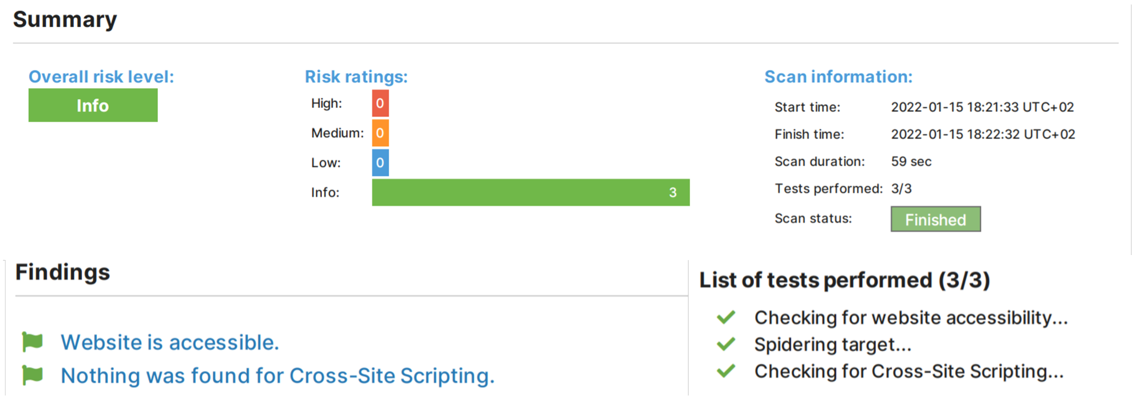
The figure 5.9, shows the encrypted data that is saved into the database.

5.2 Experimental Testing and result

To assess the security measures of Medicare against vulnerabilities and breaches, we have tested the web application and performed various scannings with Pentest-Tools.com, a reliable penetration testing, and vulnerability assessment platform [37]. We have Performed XSS scanning, SQLi scanning, and website vulnerability scanning with this tool. We have performed a performance analysis test of the web application too with the PageSpeed Insights tool by Google Developers [38]. This test portrays how smooth the operation of a website is on all types of devices.

5.2.1 Cross-Site Scripting (XSS)

XSS is a security vulnerability. The websites that take input are at risk of this security threat. For example, taking input of login credentials or other information [39]. Malicious code is given as input in those websites that can affect the source code of the website and change its functionality. This can largely act on the people who try to use those websites. This can be avoided by checking the input strings of the user before using the input. With the help of Pentest-Tools.com, the vulnerability XSS is checked and the following result is generated in the figure 5.10 below where it is seen that the website is secure and free from XSS vulnerability.



Summary

Overall risk level:
Info

Risk ratings:

High:	0
Medium:	0
Low:	0
Info:	3

Scan information:

Start time:	2022-01-15 18:21:33 UTC+02
Finish time:	2022-01-15 18:22:32 UTC+02
Scan duration:	59 sec
Tests performed:	3/3
Scan status:	Finished

Findings

- Website is accessible.
- Nothing was found for Cross-Site Scripting.

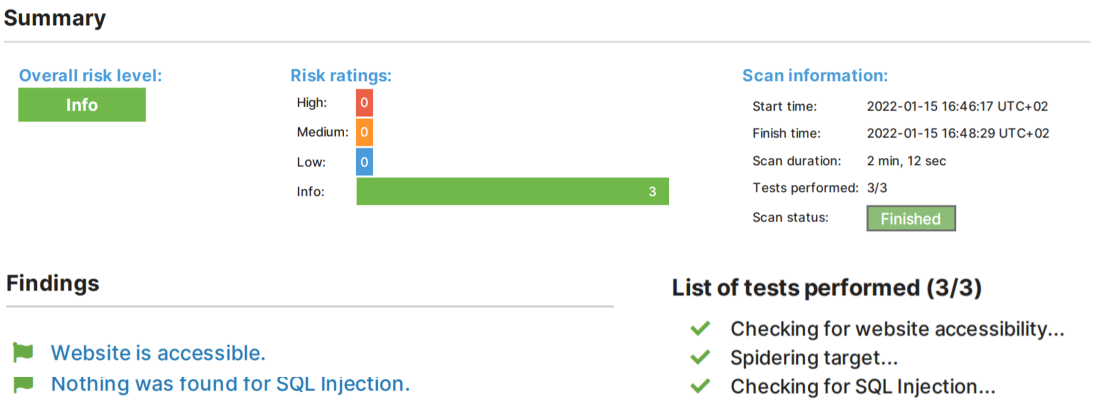
List of tests performed (3/3)

- ✓ Checking for website accessibility...
- ✓ Spidering target...
- ✓ Checking for Cross-Site Scripting...

Figure 5.10: Testing Summary Of XSS

5.2.2 SQL Injection

SQL Injection is the procedure of putting malicious code in the input section of a website in the form of a SQL statement. When the input box is filled with malicious code, different queries are run to check the value in the database. With the help of SQL injection the attacker is able to view the data of other users present in the database. The attacker may also change or delete important data from the database [40]. This makes it more dangerous as the attacker can exploit data in their own way. The following figure 5.11, shows the result of SQL injection that was produced to check the website's standings.



Summary

Overall risk level:
Info

Risk ratings:

High:	0
Medium:	0
Low:	0
Info:	3

Scan information:

Start time:	2022-01-15 16:46:17 UTC+02
Finish time:	2022-01-15 16:48:29 UTC+02
Scan duration:	2 min, 12 sec
Tests performed:	3/3
Scan status:	Finished

Findings

- Website is accessible.
- Nothing was found for SQL Injection.

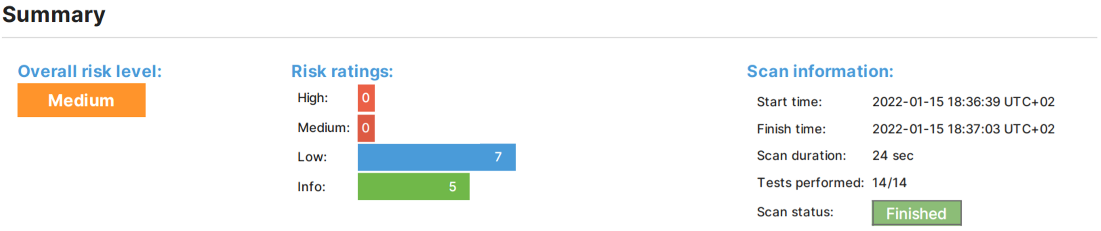
List of tests performed (3/3)

- ✓ Checking for website accessibility...
- ✓ Spidering target...
- ✓ Checking for SQL Injection...

Figure 5.11: Testing Summary Of SQL Injection

5.2.3 Website Vulnerabilities

Website Vulnerabilities are weak points of a website that makes it easier for the attackers to operate different attacks on the website. These vulnerabilities can provide the cybercriminals different opportunities to modify or steal data that may result in severe data piracy. The accessibility of a website, the secure flag cookie, HTTP header are the common points where there vulnerabilities may appear. The figure 5.12, below shows the website vulnerability testing and results.



Summary

Overall risk level: Medium

Risk ratings:

High:	0
Medium:	0
Low:	7
Info:	5

Scan information:

Start time:	2022-01-15 18:36:39 UTC+02
Finish time:	2022-01-15 18:37:03 UTC+02
Scan duration:	24 sec
Tests performed:	14/14
Scan status:	Finished

Figure 5.12: Testing Summary Of Website Vulnerabilities

5.2.4 Performance Testing

The performance testing is done by the PageSpeed Insights tool [38]. For desktop or laptops, the performance is impressive where the overall score is 98 on a scale of 100. From the table 5.1, the total blocking time measured is 10ms. This means that the usability of the webpage during loading is very convenient. The largest contentful paint takes time of only 1s. Also, the speed index is only 1.1s meaning the content of the pages would not take more than 1.1s to appear. Lastly, to become fully interactive the web page takes 1.2s only. So, performance-wise the website is in great condition. The following table 5.1 shows the overall performance details of the website.

Performance Metrics	Time Taken
First Contentful Paint	0.6s
Speed Index	1.1s
Largest Contentful Paint	1.0s
Time To Interactive	1.2s
Total Blocking Time	10ms
Cumulative Layout Shift	0s

Table 5.1: Results Of Performance Metrics

In the case of Mobile phones, Medicare performs moderately. The Total Blocking Time increases to 470 ms which eventually affects the smooth operation of the application. The reason according to the diagnosis of PageSpeed Insights is, resources are blocking the first paint of the page. As a result, the performance score comes down to 74.

5.3 Challenges And Limitations

The biggest challenge that we faced is, continuing our research during the pandemic situation. There were some more challenges like learning or getting introduced to a new programming language and framework, implementing a web application and hosting it. Also, the tools for testing the whole system were costly. As a result, the authentic and dependable tools were hard to find. Buying a cloud server was also a costly procedure.

For implementing this whole project nationwide, the local server has to be set up and maintained. But setting up a local server is not easy as the local server needs a dedicated device for it. So, having little resources, the implementation of two servers was not possible. Thus the concept of a web farm was not possible. So, data was kept in a database in different tables connected with a key. Moreover, MFA or multi factor authentication was not possible as the OTP gateway was expensive to implement. Instead, SFA or single factor authentication was used. But for authorization of users, instead of OTP, a request system was created where one can request for some specific files from another user. Another limitation was not using paid tools for testing as the paid tools were expensive.

Though there were many challenges and limitations, the implementation of the web app was possible and data was kept securely in the server. Many attacks were produced and the web app gave a positive outcome. No data breach was found and getting access to the data was not possible. So, even with all these challenges and limitations, the system was secure and trustable. So, developing the whole system with two servers would give higher security and create a user friendly environment in the web application.

Chapter 6

Conclusion and Future plan

With the advancement of information technologies, the healthcare system has also been modernised in the developed countries with the use of the secure EHR system. However, developing countries like Bangladesh are still using the traditional way to keep health records which are not efficient and reliable anymore. In this respect, it can be concluded that a quality based EHR system with proper data security needs to be built which must be easily and widely applicable throughout the country. Here, a secured electronic health record (EHR) system is proposed in the perspective of Bangladesh which will be cost effective, user friendly and efficient. In this regard, a web-based application is developed named 'Medicare' which is tested and proved secure. As for authentication, similar approaches like Kerberos are implemented which makes the system harder for the intruders to break in. Moreover, the addition of the AES encryption method will safeguard the whole system from being compromised. This research will motivate the people of Bangladesh to analyze the drawbacks of the existing system and jump into the highest security standard.

The primary and obvious future work is the addition of solutions to the power backup issues. The data can be lost in case of power, machine, and hardware failures in both wanted, unwanted, and contingency situations. But an improvement in AES by enhancing the cache memory occupation in temporary memories will eliminate the waste of time and money to a relevant extent. In addition, the implementation of such a plan will ensure that if there is any planned power cut by the spammers to make the system freeze and launch an attack, as soon as the machines get power again, the attack will be prevented without any further layer of security. In the extension of the theoretical and practical framework-based works of the report, the construction of one web farm concept was not possible because of the absence of a configured Computer that will act as a local server for the designed proposition. For the time being, the architecture is being implemented by placing the two databases into a single server. But in the future, the introduction of a locally set up private server will enhance it for personal information storage by keeping sensitive information safe and secured.

We believe that countrywide successful implementation of this EHR model will take the healthcare system to a whole different dimension.

Bibliography

[1] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, “5g communication: an overview of vehicle-to-everything, drones, and healthcare use-cases,” *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[2] A. Sayin, M. Cherniakov, and M. Antoniou, “Passive radar using starlink transmissions: A theoretical study,” in *2019 20th International Radar Symposium (IRS)*, pp. 1–7, IEEE, 2019.

[3] R. Mostafa, G. E. Rahman, G. M. Hasan, A. Kabir, A. Rahman, and S. Ashik, “Proposed deployments to provide e-healthcare in bangladesh: Urban and rural perspectives,” in *The 12th IEEE International Conference on e-Health Networking, Applications and Services*, pp. 361–366, IEEE, 2010.

[4] “Bangladesh.” http://uis.unesco.org/en/country/bd, Apr 2017. Accessed: June 2021.

[5] N. Netanel, “what everyone needs to know.” https://aws.amazon.com/what-is-cloud-storage/, 2018. Accessed: June 2021.

[6] M. L. Graber, C. Byrne, and D. Johnston, “The impact of electronic health records on diagnosis,” *Diagnosis*, vol. 4, no. 4, pp. 211–223, 2017.

[7] T. T. . November and T. Tajmim, “Aggressive drug promotion practices bane for patients.” https://www.tbsnews.net/bangladesh/health/aggressive-drug-promotion-practices-bane-patients, Nov 2019. Accessed: June 2021.

[8] A. Vaidya, “Report: Healthcare data breaches spiked 55%-symbol in 2020.” https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/, Feb 2021. Accessed: June 2021.

[9] “Patient, doctors, nurses ratio: Bangladesh lags far behind its neighbours.” https://archive.dhakatribune.com/health/2019/07/21/patient-doctors-nurses-ratio-bangladesh-lags-far-behind-its-neighbours, Jul 2019. Accessed: June 2021.

[10] “Overview.” https://www.worldbank.org/en/country/bangladesh/overview. Accessed: June 2021.

[11] S. Z. Khan, Z. Shahid, K. Hedstrom, and A. Andersson, “Hopes and fears in implementation of electronic health records in bangladesh,” *The Electronic*

Journal of Information Systems in Developing Countries, vol. 54, no. 1, pp. 1–18, 2012.

[12] T. Schabetsberger, E. Ammenwerth, G. Göbel, G. Lechleitner, R. Penz, R. Vogl, and F. Wozak, "What are functional requirements of future shared electronic health records?," *health care*, vol. 9, p. 10, 2005.

[13] G. S. Mahmood, T. M. Hasan, and A. M. Badr, "Multi-authority system based personal health record in cloud computing," *Journal of AL-Qadisiyah for computer science and mathematics*, vol. 9, no. 1, pp. 108–116, 2017.

[14] I. Ogbodo and F. Bakpo, "Patient-centric cloud-based ehr system for government hospitals in developing countries," *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 53–61, 2020.

[15] M. Ahmed and T. S. Shavali, "Privacy protection of encrypted medical data over multi-authority cloud system," Apr 2018.

[16] J. Zhang, H. Liu, and L. Ni, "A secure energy-saving communication and encrypted storage model based on rc4 for ehr," *IEEE Access*, vol. 8, pp. 38995–39012, 2020.

[17] S. Gueron, "Intel® advanced encryption standard (aes) new instructions set." https://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf, May 2010. Accessed: June 2021.

[18] J.-Y. Oh, D.-I. Yang, and K.-H. Chon, "A selective encryption algorithm based on aes for medical information," *Healthcare informatics research*, vol. 16, no. 1, pp. 22–29, 2010.

[19] W. A. Al-Hamdani, "Cryptography based access control in healthcare web systems," in *2010 Information Security Curriculum Development Conference*, pp. 66–79, 2010.

[20] "Electronic health records." https://www.who.int/gho/goe/electronic_health_records/en/, Nov 2019. Accessed: June 2021.

[21] "Building a stronger foundation for the future of healthcare." https://www.vertiv.com/pl-emea/solutions/healthcare/. Accessed: June 2021.

[22] N. Tomar, "Web farm and web garden." https://www.c-sharpcorner.com/uploadfile/nipuntomar/web-farm-and-web-garden/, Apr 2011. Accessed: December 2022.

[23] "What are cloud leaks?: Upguard." https://www.upguard.com/blog/what-are-cloud-leaks. Accessed: June 2021.

[24] blue1914, "Advantages of cloud storages." https://www.bluemogulenterprise.com/advantages-of-cloud-storages/, Jan 2019. Accessed: June 2021.

[25] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf. Accessed: June 2021.

[26] S. Mohammed, L. Ramkumar, and V. Rajasekar, "Password-based authentication in computer security: Why is it still there," *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)*, vol. 5, no. 2, pp. 33–36, 2017.

[27] P. Loshin and M. Cobb, "What is encryption and how does it work?." https://searchsecurity.techtarget.com/definition/encryption, Apr 2020. Accessed: June 2021.

[28] A. Abdullah, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, pp. 1–11, 2017.

[29] A. Nadjia and A. Mohamed, "Aes ip for hybrid cryptosystem rsa-aes," in *2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15)*, pp. 1–6, IEEE, 2015.

[30] P. says and Pushpanjali, "Difference between des and aes (with comparison chart)." https://techdifferences.com/difference-between-des-and-aes.html, Dec 2019. Accessed: June 2021.

[31] M. Babitha and K. R. Babu, "Secure cloud storage using aes encryption," in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, pp. 859–864, IEEE, 2016.

[32] A. Alabaichi, F. Ahmad, and R. Mahmod, "Security analysis of blowfish algorithm," in *2013 Second International Conference on Informatics & Applications (ICIA)*, pp. 12–18, IEEE, 2013.

[33] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, "Security analysis of md5 algorithm in password storage," in *Applied Mechanics and Materials*, vol. 347, pp. 2706–2711, Trans Tech Publ, 2013.

[34] "5.0 authentication methods." https://www.microfocus.com/documentation/sentinel/8.5/s85-admin/t42ki04m98od.html. Accessed: June 2021.

[35] P. Kumar, "An overview of the best laravel security practices." https://www.cloudways.com/blog/laravel-security/, Jun 2021. Accessed: December 2022.

[36] "Learn mysql tutorial - javatpoint." https://www.javatpoint.com/mysql-tutorial. Accessed: December 2022.

[37] Pentest-Tools.com, "Website scanner online - find vulns fast." https://app.pentest-tools.com/website-vulnerability-scanning/website-scanner#. Accessed: January 2022.

[38] "Make your web pages fast on all devices." https://pagespeed.web.dev/. Accessed: January 2022.

[39] "Cross-site scripting (xss)." https://www.trendmicro.com/vinfo/us/security/definition/cross-site-scripting-(xss). Accessed: January 2022.

[40] "What is sql injection? tutorial examples: Web security academy." https://portswigger.net/web-security/sql-injection. Accessed: January 2022.