DESIGN AND DEVELOPMENT OF SECURITY SOLUTIONS FOR HEALTHCARE SYSTEMS

A Project Report Submitted by

Salian Vikrant
(4NM16CS125)

Terril Joel Nazareth
(4NM16CS162)

Vipin M S
(4NM16CS174)

Vishal Mada
(4NM16CS177)

Yathiraj G N
(4NM16CS183)

UNDER THE GUIDANCE OF

Mrs. Asmita Poojary
Asst. Professor Gd II

Department of Computer Science and Engineering

In partial fulfillment of the requirements for the award of the Degree of

Bachelor of Engineering in Computer Science & Engineering

From

Visvesvaraya Technological University, Belagavi

NITTE EDUCATION TRUST

N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India
(ISO 9001:2015 Certified), Accredited with 'A' Grade by NAAC
08258 - 281039 – 281263, Fax: 08258 – 281265
B.E.CSE Program Accredited by NBA, New Delhi from 1-7-2018 to 30-6-2021

April 2020

NITTE EDUCATION TRUST | N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India
(ISO 9001:2015 Certified), Accredited with 'A' Grade by NAAC
☎ : 08258 - 281039 – 281263, Fax: 08258 – 281265
Department of Computer Science and Engineering
B.E. CSE Program Accredited by NBA, New Delhi from 1-7-2018 to 30-6-2021

CERTIFICATE

Certified that the project work entitled

"Design and Development of Security Solutions For Healthcare Systems"

is a bonafide work carried out by

Salian Vikrant (4NM16CS125) Terril Joel Nazareth (4NM16CS162)
Vipin M S (4NM16CS174) Vishal Mada (4NM16CS177)
Yathiraj G N (4NM16CS183)

in partial fulfilment of the requirements for the award of ***Bachelor od Engineering Degree in Computer Science and Engineering***

prescribed by

Visvesvaraya Technological University, Belagavi

during the year 2018-2019.

It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library.

The project report has been approved as it satisfies the academic requirements in respect of the project work prescribed for the Bachelor of Engineering Degree.

Signature of Guide **Signature of HOD** **Signature of Principal**

Semester End Viva Voce Examination

Name of the Examiners **Signature with Date**

1. _____

2. _____

ACKNOWLEDGEMENT

We believe that our project will be complete only after we thank the people who have contributed to make this project successful.

First and foremost, our sincere thanks to our beloved principal, **Dr. Niranjan N. Chiplunkar** for giving us an opportunity to carry out our project work at our college and providing us with all the needed facilities.

We express our deep sense of gratitude and indebtedness to our guide **Mrs. Asmita Poojary,** Asst. Professor Gd II, Department of Computer Science and Engineering, for his inspiring guidance, constant encouragement, support and suggestions for improvement during the course for our project.

We acknowledge the support and valuable inputs given by, **Dr. Uday Kumar Reddy** the Head of the Department, Computer Science and Engineering, NMAMIT, Nitte.

We express our gratitude to the project co-ordinators **Mrs. Pallavi K N, Mr. Ranjan Kumar HS** and **Mr. Raju K.** for their constant support.

We also thank all those who have supported us throughout the entire duration of our project.

Finally, we thank the staff members of the Department of Computer Science and Engineering and all our friends for their honest opinions and suggestions throughout the course of our project.

Salian Vikrant (4NM16CS 125)

Terril Joel Nazareth (4NM16CS162)

Vipin M S (4NM16CS174)

Vishal Mada (4NM16CS177)

Yathiraj G N(4NM16CS183)

ABSTRACT

The security of patient's data is the most overbearing barrier to access when considering the adoption of Healthcare devices. Several studies show that there is a lot of risk in storing and accessing the patient's information in a traditional method. The project is undertaken in order to attain a secured health care system. It is essential to ensure trust and data secrecy from the starting point-sensors throughout the medical treatment to prevent any unauthorized access or unnecessary interruption. In order to protect the private medical data in the IOT field, a lightweight encryption algorithm is must. The project aims at building a portable secure means of storing the patient's information. This project helps to implement several realistic lightweight encryption algorithms suitable for IOT medical systems. The project aims at implementing a cryptographic algorithm resulting in fair analysis in terms of memory utilization and speed. The project is undertaken in order to attain a secure healthcare system considering the balance between the optimal requirement and the future threats

Keywords: Security, Lightweight Encryption Algorithm, Healthcare, Authentication, IOT

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Data collection in healthcare allows health systems to create holistic views of patients, personalize treatments, advance treatment methods, improve communication between doctors and patients, and enhance health outcomes. Cyberattacks, data breaches, and hacking are key concerns for healthcare executives and a growing problem in the industry. A recent report showed that data breaches were up in 2018, with 503 incidents impacting almost 15.1 million patient records, compared to 477 breaches impacting 5.6 million records in 2017. As hackers get more sophisticated, hospitals need to be increasingly vigilant about their healthcare IT and cybersecurity practices.

The project is undertaken in order to attain a secured health care system. It is essential to ensure trust and data secrecy from the starting point-sensors throughout the medical treatment to prevent any unauthorized access or unneeded interruption. In order to protect the private medical data in the IoT field, a lightweight encryption algorithm is must. The sheer number of disparate IT systems used in healthcare is perhaps unrivaled in any other industry. Every system, every vendor, every connection, and every employee with access and responsibility for transferring sensitive data is a cybersecurity risk. The project aims at building a portable secure means of storing the patient's information.

Cryptography in digital world offers three core area that protect you and your data from attempt theft, theft or an unauthorized use of your data and possible fraud. Cryptography cover these essential areas; authentication, integrity, and confidentiality. Lightweight cryptography is an encryption method that features a small footprint and/or low computational complexity. It is aimed at expanding the applications of cryptography to constrained devices .This project helps to implement several realistic lightweight encryption algorithms suitable for IoT medical systems. The project aims at implementing a cryptographic algorithms resulting fair analysis in terms of memory utilization and speed. The project is undertaken in order to attain a secured health care system considering the balance between the optimal requirement and the future threats.

The objective of the developed Software is to provide a platform for the healthcare industry where the doctors can access the patient's data in a secured way. This project provides a medium for doctor to access patient's reading taken in a real time. We are implementing a software in which patient's data can be encrypted and uploaded after examining him/her at a remote place and send it to a doctor for evaluation of patient's health so that the doctor can diagnose or confirm about patient's health..

1.1 OVERVIEW

Data quality in healthcare must possess accuracy, consistency, and relevancy. Health information technology and health information exchanges enhance data quality by reducing redundancy, decreasing medical errors, and enhancing health outcomes. Technology has brought about a massive and welcome change to the healthcare industry. Patients now have access to some of the best diagnostic tools, new and cutting-edge treatments, and a myriad of minimally-invasive procedures resulting in less pain and quicker healing**.** Remote consultations with specialists, targeted treatments, and the availability of intuitive mobile apps have led to improved patient care and a superior healthcare experience overall. Additionally, the availability of newer treatment technologies leading to better outcomes has enhanced the quality of life of the patients as well**.** Since there are various kinds of technology being used such as Mobile App technology, Big Data and cloud, Information and communication. All of these use very sensitive data related to patient. Hence it becomes important to protect all of this information. This is where light weight cryptography comes into the picture. This is why the patient's data must be secured by encrypting it before uploading it to server or storage units so that accurate data is delivered to doctors for examining the patient's case. To do this we are using lightweight cryptography algorithms in order to obtain low computational complexity, faster processing and efficient memory utilization constrained to devices in which encryption takes place. This way the data can be made secure so that if there's a security threat or attack it can be prevented.

PROBLEM STATEMENT

Different applications require different level of security where the scarce of resource plays effective role. In order to protect the private medical data in the internet of things (IoT)

field, the search for the optimal encryption algorithm is a must. Electronic sensors are used to collect medical data from the patient's body acquiring its transmission to the Healthcare system securely.

It is essential to ensure trust and data secrecy from the starting pointsensors throughout the medical treatment to prevent any unauthorized access or unneeded interruption. Thus, data encryption from the beginning sensors is necessary but facing all limitations in computing complexity, power consumption and communication bandwidth, where the normal available crypto-algorithms are considered heavyweight is completely unpractical. This project helps to implement several realistic lightweight encryption algorithms suitable for IoT medical systems.

1.2 STUDY AREA

Healthcare technology presents numerous opportunities for improving and transforming healthcare which includes; reducing human errors, improving clinical outcomes, facilitating care coordination, improving practice efficiencies, and tracking data over time. In order to protect all the data involved in this we use light weight cryptography algorithms. The motivation of lightweight cryptography is to use less memory, less computing resource and less power supply to provide security solution that can work over resource-limited devices. The lightweight cryptography is expected to work simpler and faster compared to conventional cryptography.

1.3 OBJECTIVE

In this project, we have designed a software in a such a way that it satisfies the requirements of doctors who use the data and the staff who upload the data into the storage units. The sensors are also connected via Raspberry Pi .Raspberry Pi is faster than Arduino in terms of interfacing the sensors to the PC. The front end is developed by using Web Technologies like HTML and styling is done using CSS, bootstrap, with doctor and staff access. The admin can upload the videos and the students as users can view these uploaded videos. We are maintaining a database to store the video locations and other details of the videos. The PHP is the backend for all the operations. The software also

provides multiple additional features for the users which makes their interaction with the software flexible. By using light weight cryptography algorithm, we are encrypting the data and decrypting it. The main objective is to generate a key which makes the encryption highly secure using the lightweight cryptography algorithm. The project also aims at also making the hardware part i.e interfacing the sensors with the system more reliable and fast.

1.4 MOTIVATION

The traditional cryptography method used for encryption is suitable on computing system which can satisfy all the resource requirements. It is not suitable to encrypt data on small devices since it takes more computing capacity and also time. But in case of healthcare we need to ensure that the data is transferred faster from source to destination with good security. In order to do this we choose light weight cryptography to do the above task. With the IoT systems that make use of data in the real world, the data collection from devices can also be a target of cyberattacks. It is because of this that countermeasures based on encryption are currently gaining in importance. Lightweight cryptography is an encryption method that features a small footprint and/or low computational complexity. It is aimed at expanding the applications of cryptography to constrained devices and its related international standardization and guidelines compilation are currently underway.

1.5 ORGANIZATION OF THE CHAPTERS

The project report has been organized under nine chapters, which are as follows:

Chapter I: Introduces to the main idea of the project. It gives a brief knowledge about the aim and methodology of the same.

Chapter II: It includes literature survey of related works.

Chapter III: Discusses the system requirements that are needed for the project. These include functional requirements, non-functional requirements, user requirements and hardware requirements.

Chapter IV: Includes the system design details which includes flowchart, sequence diagram.

Chapter V: Includes the implementation details of the project, application is explained in detail. It also deals with software approach.

Chapter VI: Deals with system testing concepts and the various test cases for the project.

Chapter VII: Includes the screenshots of the application and the database.

Chapter VIII: Discuss the results of the project.

Chapter IX outlines conclusions and future work that can be done

CHAPTER 2

LITERATURE SURVEY

Lightweight cryptography methods are proposed to overcome many of the problems of conventional cryptography. This includes constraints related to physical size, processing requirements, memory limitation and energy drain.

In IoT, many interconnected resource-constrained devices are not designed to carry out expensive conventional cryptographic computation, which makes it difficult to implement sufficient cryptographic functions [1]. To guarantee security and privacy protection in the IoT becomes a serious concern when integrating resource-constrained devices into the IoT securely since they are incapable of carrying out sufficient cryptographic algorithms.

Methods defined by William J. Buchanan we as follows:

1. Hashing
2. Streaming
3. Block
4. Signing
5. Asymmetric encryption

The lightweight cryptography trade-offs implementation cost, speed, security, performance and energy consumption on resource-limited devices. The motivation of lightweight cryptography is to use less memory, less computing resource and less power supply to provide security solution that can work over resource-limited devices. The lightweight cryptography is expected simpler and faster compared to conventional cryptography. The disadvantage of lightweight cryptography is less secured.

The most available researches were focusing on the challenges that are related to optimizing for a specific platform. It is important to realize that if the block cipher achieves the highest performance on dedicated platform, this one can be out of the comparison on most other platforms [3]. Moreover, it may face a limit in usability on the end of the platform's life which is continually changing very fast. From the other side, it will not be sufficient to delay the discussion until the future devices or the IoT devices appear, but we can study the performance of ciphers to find simple algorithm that can be efficiently everywhere. With all this in mind, the SIMON and the SPECK algorithms were found the best. Both of them are designed especially to improve the security on the very constrained environments such as our IoT medical application. They are currently built as general block

ciphers expected to be important involved in many future applications of the IoT area. In addition, the two of them, the SIMON and the SPECK, are practically flexible working well on many different platforms that can be adjustable for the innovative future use. As a matter of fact, our study found that the SPECK algorithm is better than SIMON procedure in the software implementation; that's because the SIMON needs some preparation bit moves and that is due to the fact that several operations made by using single word of the intermediate cipher-text.

EXISTING SYSTEM:

In this the encryption of the medical records is done using traditional cryptographic methods. It is done mostly by utilization pixels arrangement and random permutation to encrypt medical image for transmission security. The objective of this scheme is to obtain a high speed computation process and high security. Among other algorithms such as transform method and traditional method, pixels arrangement and permutation provide simple and quick processes; it particularly does not need any mathematical manipulation. This feature is especially very useful for medical image where the image can be very big. We tested the algorithm using gray-scale images. The scheme shows a good randomness and quick computation process. But this includes constraints related to physical size, processing requirements, memory limitation and energy drain.

PROPOSED SYSTEM:

We try to overcome the above constraints by using Lightweight Cryptography to secure medical records in IOT systems. We are going take the patient readings such heart rate, blood pressure etc, through the sensors and encrypt and decrypt using Lightweight crytography. Lightweight cryptography (LWC) is defined as a crypto algorithm suitable for limited resource constrained environment such as medical sensors, RFID tags, and portable health care devices . Its data security can be stream based or block based, but must be keeping acceptable level of immediate usage security ; i.e. researchers can misunderstand the lightweight concept as less secure protocol, but it's not the case. The lightweight crypto security is only lightweight in resource consuming for instantaneous treatment and not reduction in the security or privacy weight . In general, the LWC the adequate amount of (80 to 128 bit) security for direct usage of IoT medical application tuned for the significant reduced amount of resources .

CHAPTER 3

SYSTEM ANALYSIS AND REQUIREMENTS

3.1 SYSTEM ANALYSIS

3.1.1 Relevance of Platform

While many popular website applications (WordPress, Drupal, Joomla, etc.) are open source and therefore freely available, running these PHP-based apps on a Windows IIS web server requires a bit of retrofitting.[7] Enter WampServer, an open source product that installs a PHP-apps-ready platform consisting of Apache web server, MySQL database, PHP, plus several helpful GUI-based utilities. WampServer can be installed on virtually any version of Windows, either desktop or server. With an active user community, industrial-grade training programs and a large installed base, WampServer is one of the world's most popular Apache-MySQL-PHP distributions.

3.1.2 Relevance of Programming Language

HTML is the programming language that powers the web. And like any language, once you master it, you can begin to create your own content, whether that's simple websites or complex web applications. Using HTML, you create user interface for web applications and mobile applications. HTML was published as a W3C recommendation.[8]

PHP was designed specifically for web application development. The web developers have to explore ways to keep the visitors engaged by increasing the website’s loading speed. PHP 7 comes with a just in time (JIT) engine that enhances PHP code execution speed significantly and helps programmers to speed up the web application. PHP works seamlessly with major operating systems, databases and web servers. They can simply make changes to the existing code and modify the command functions to add new features or functionality to the website. [9]

Python is a powerful and object-oriented high-level programming language. It has very simple easy-to-use syntax. It works on cross-platform operating systems and can be used across to develop a wide range of applications including those intended for image processing, text processing, web, and enterprise level using scientific, numeric and data from the network. [10]

3.2 REQUIREMENT ANALYSIS

3.2.1 Scope and Boundary

The growth and change in technology at a rapid rate is having a huge impact in healthcare field. It has been very helpful for doctor's and other healthcare related employees in providing effective treatment to patients. One of the main reasons technology is having a lot of influence is because the vast data that is being used in healthcare industry. The patient data, medical records, sensor readings and many more. Hence security is a must in order to protect the data that being is used. Any change or breach of data might have a huge impact on the patients. This is where our project can be used. All these data must be encrypted and must be only accessible to authorized people. All this activities of securing the data can be done by using cryptography. Hence we use light weight cryptography algorithm in order to secure the data.

The users of our software being mainly the doctors and related staff the portals must be easy to understand. It also needs to be speed in terms of processing the data , encrypting , storing and retrieving as well as accurate .

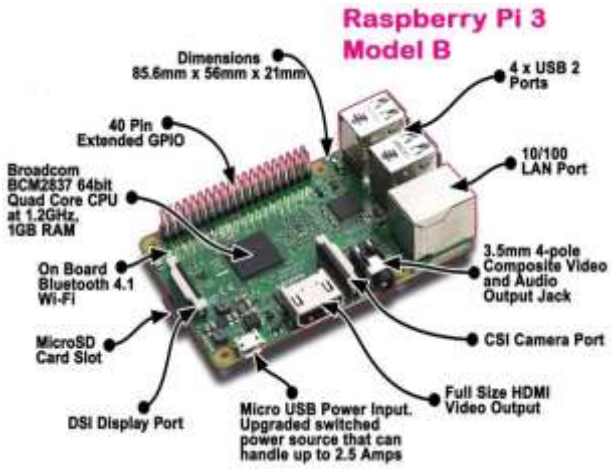
3.3 FUNCTIONAL REQUIREMENTS

3.3.1 Software Requirements:

- Software: 1. PyCharm
  2. VNC Viewer
  3. Putty SSH Client
  4. WinSCP
  5. SD card formatter
- HTML
- CSS
- JAVASCRIPT
- MY SQL
- PYTHON
- APACHE SERVER

3.3.2 Hardware Requirements:

- Operating system: Windows 7 and above.
- RAM: 4GB and above.
- Processor: Intel® Core (TM)2 duo CPU T6500.
- Processor speed: 2.67 GHz.
- CPU: 64-bit operating system.
- **Raspberry Pie 3**



CPU: Broadcom BCM2837 SOC 64-bit quad-core ARM Cortex A53 (ARMv8 CPU) with 512KB shared L2 cache.

Memory: Provided with 1 GB of RAM

Wi-Fi Support: 802.11n Wireless LAN

Bluetooth: Supports Bluetooth 4.1 Bluetooth Low Energy (BLE)

It has 4 USB ,1 HDMI Port,1 Ethernet, CSI, DSI and GPIO Ports. It has a 3.5 mm audio jack.

- **DHT11 Temperature sensor**

Operating Voltage: 3.5V to 5.5V

Operating current: 0.3mA (measuring) 60uA (standby)

Output: Serial data

Temperature Range: 0°C to 50°C

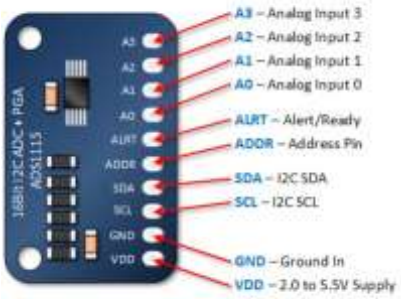
Resolution: 16-bit

Accuracy: ±1°C and ±1%

- **Pulse rate sensor**

Operating Voltage: +5V or +3.3V
Current Consumption: 4mA

- **ADS115 ADC module**



3.4 NON-FUNCTIONAL REQUIREMENTS:

In systems engineering and requirements engineering, a non-functional requirement (NFR) is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. Non-functional requirements are conditions under which the system must be able to function and the quality the system must have. It defines how a system is supposed to be.

- Performance
    - With ideal condition website response should be fast and error free.
    - Encryption and decryption speed should not decrease with time and load.

- Flexibility:
  - This website will be easy to learn and use.
  - Is able to encrypt and decrypt any kind of data related to healthcare without affecting the performance.
- User-friendly:
  - The users should be able to understand the functionality or working of the software easily.
  - The website's multiple features should be self-explanatory.
- Response Time:
  - The data uploaded by the staff or the doctor must be visible in the patients account without any problem and must be accurate within the time limit.
- Understandability:
  - All users can learn to operate the website because of its simplicity.

CHAPTER 4

SOFTWARE APPROACH

4.1 ABOUT WAMP

WAMP is an acronym formed from the initials of the operating system Microsoft Windows and the main components of the package: Apache**,** MySQL & PHP. Apache is the most popular open source web server, MySQL is the most popular open-source database, used by huge number of websites around the world and PHP is a widely used general-purpose server-side scripting language designed to produce dynamic web pages. By combining these components into a single installation package, Wamp Server allows users to set up a server locally on their Windows machine to create dynamic web applications with Apache, PHP and the MySQL database in the same development conditions as on the production server. One of the great benefits of Wamp Server is that it allows you to develop, upgrade components, perform any web development task and carefully test everything offline first, which reduces the risks of creating problems on the live server.[11]

4.2 PYTHON

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python was designed to be highly readable which uses English keywords frequently whereas other languages use punctuation and it has fewer syntactical constructions than other languages. Python is a general-purpose language, which means it can be used to build just about anything, which will be made easy with the right tools/libraries. Professionally, Python is great for backend web development, data analysis, artificial intelligence, and scientific computing. Many developers have also used Python to build productivity tools, games, and desktop apps, so there are plenty of resources to help you learn how to do those as well. PHP is now the most famous server-side scripting language that runs on a web server. It gives you an enhanced flexibility to make dynamic web pages and application. Below are some points that highlight the importance of PHP development in the web development industry.[12] It is open source and the resources are also open source which makes it really cheap to work on. PHP has a short learning curve which means it doesn’t take long to learn the language. The language is highly efficient and error detection is also easier in this language. PHP processes the data very fast and is among

the fastest languages available. Because of its high usability, it is training and acquiring talent is risk-free.

4.3 PHP

PHP is now the most famous server-side scripting language that runs on a web server. It gives you an enhanced flexibility to make dynamic web pages and application. Below are some points that highlight the importance of PHP development in the web development industry.

For a web developer, following are the importance of PHP development:

- It is open source and the resources are also open source which makes it really cheap to work on.
- PHP has a short learning curve which means it doesn't take long to learn the language.
- The language is highly efficient and error detection is also easier in this language.
- PHP processes the data very fast and is among the fastest languages available.
- Because of its high usability, it is training and acquiring talent is risk-free.

4.4 About Algorithm

Symmetric key block cipher using lightweight cryptography

Existing algorithm:

In recent years, small computing devices like embedded devices, wireless sensors, RFID tags (Radio Frequency Identification), Internet of Things (IoT) devices are increasing rapidly. They are expected to generate massive amount of sensitive data for controlling and monitoring purposes. But their resources and capabilities are limited. Those also work with valuable private data thus making security of those devices of paramount importance. Therefore, a secure encryption algorithm should be there to protect those vulnerable devices. Conventional encryption ciphers like RSA or AES are computationally expensive; require large memory but hinder performances of those devices. Simple encryption techniques, on the other hand are easy to crack, compromising security. In this paper a secure and efficient lightweight cryptographic algorithm for small computing devices has been proposed. It is a symmetric key block cipher, employing custom substitution-permutation (SP) network and a modified Feistel architecture.

Lightweight cryptography is a sub-category in the field of cryptography that intends to provide security solutions for resource-constrained devices. Many conventional cryptographic algorithms, was optimized for desktop and server environments. Optimization in terms of security, performance and resource requirements makes those algorithms difficult or impossible to implement in resource constrained devices. Even if they can be implemented, they hinder the performance on the small devices. Lightweight cryptography aims at wide variety of hardware and software spectrum in which an algorithm can be implemented. Highly resource-constrained devices are at the very end of the spectrum that has very limited processing capabilities and memory. Lightweight cryptography is principally motivated for those.

Proposed algorithm:

The proposed algorithm is a symmetric key block cipher. It constitutes 64-bit key. In any symmetric key algorithm the Some mathematical functions define each round to create confusion and diffusion. Increasing number of rounds will ensure better security but will increase the consumption of the device. A typical cryptographic algorithm usually consists of on average 10 to 20 rounds so that the encryption process is strong enough. But the proposed algorithm restricted to only five rounds. The algorithm utilizes the Feistel network. It creates sufficient confusion and diffusion of data so that attacks can be confronted.

CHAPTER 5
SYSTEM DESIGN

5.1 HIGH LEVEL DESIGN ARCHITECHTURE

The software contains two portals, one for the staff/doctors to access the patient's information and another known as the diagnosis portal where the sensor's reading is taken and encrypted. The encrypted data is then stored on to the database. This information is decrypted and is then accessed in the patient information portal.

Data Flow Diagram

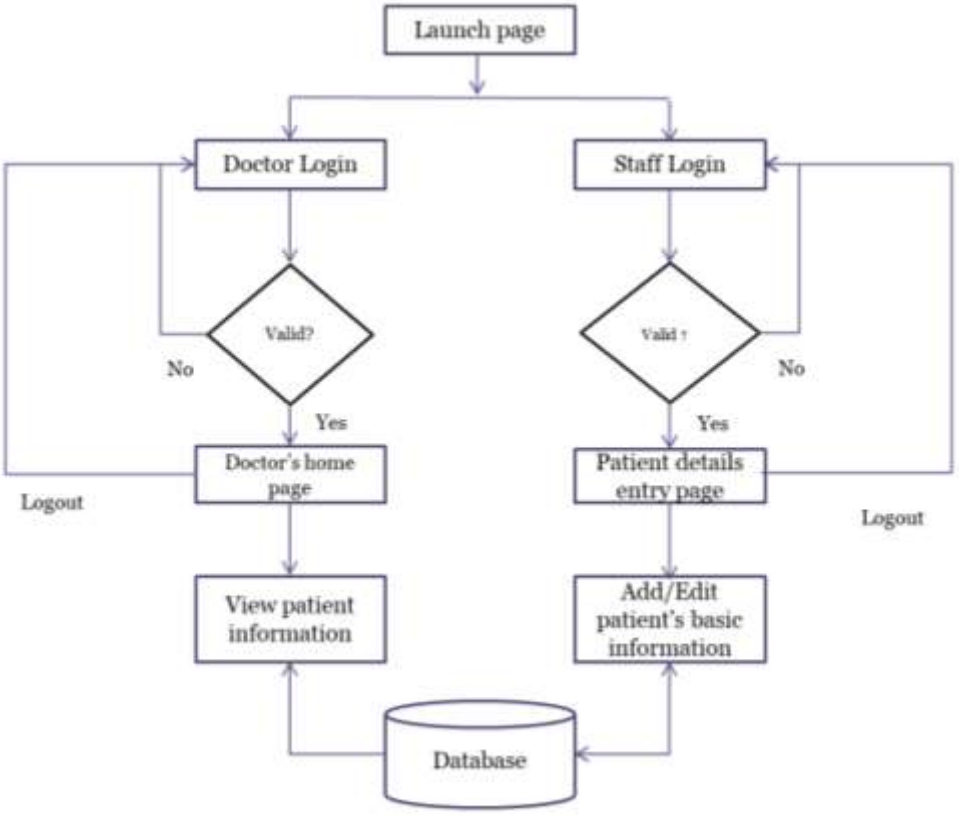


Figure 5.1 Dataflow diagram of Patient information portal

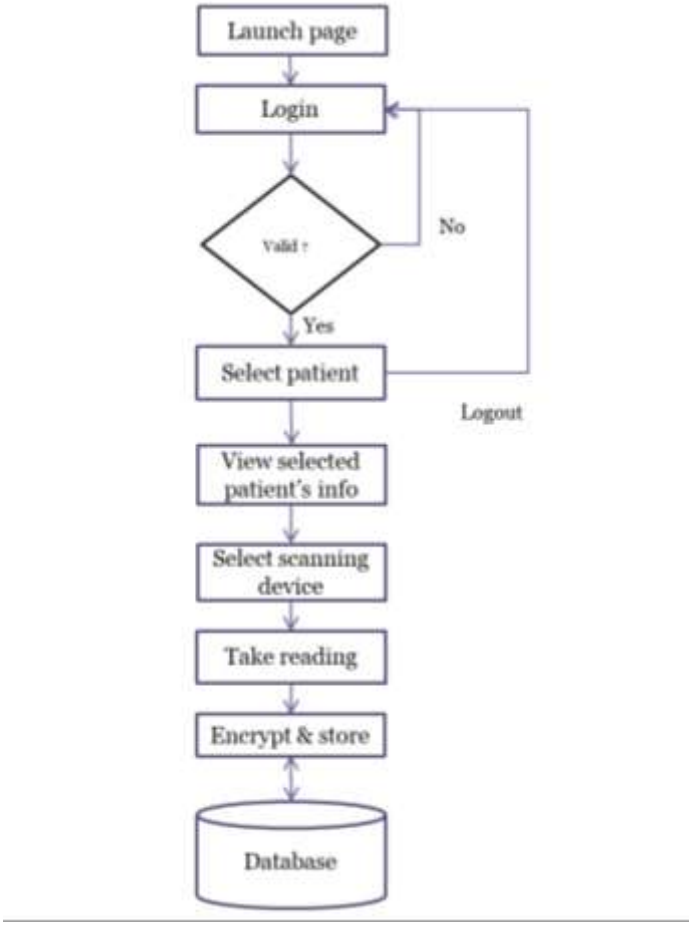


Figure 5.2 Dataflow diagram of diagnosis portal

5.2 LOW LEVEL DESIGN ARCHITECHTURE

5.2.1 Sequence Diagram /DFD

A sequence diagram shows object interaction arranged in time sequence. It describes interactions among classes in terms of an exchange of messages over time. It is also called as event diagram. A sequence diagram is a good way to visualize and validate various run time scenarios. These can help to predict how a system will behave and to discover responsibilities a class may need to have in the process of modelling the new system. Messages are arrows that represent communication between the objects. Lifelines are vertical dashed lines that indicate the object presence over time.

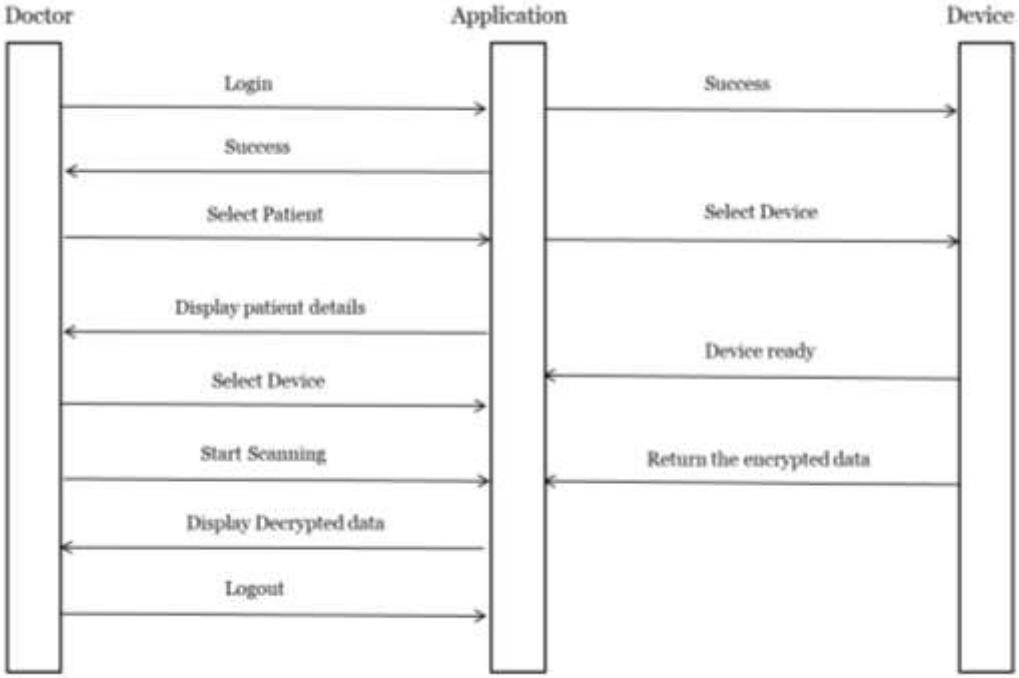


Figure 5.3 Sequence diagram of patient information portal

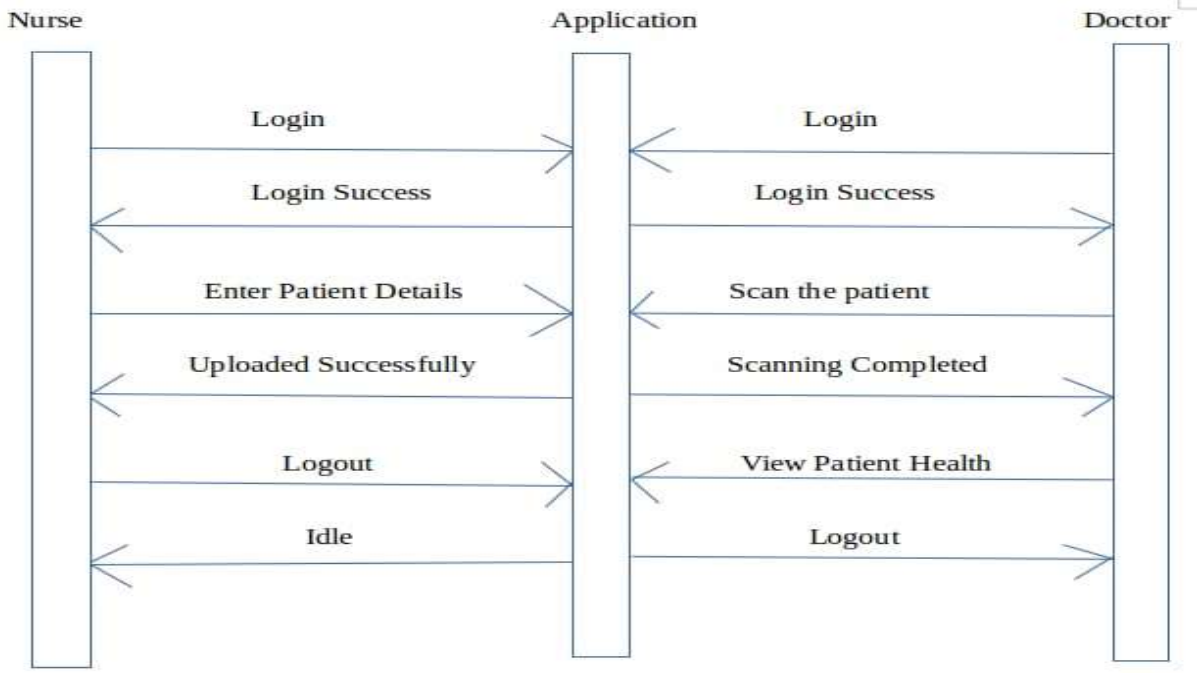


Figure 5. Sequence diagram of diagnosis portal

5.2.2 Activity Diagram

Activity diagram is another important diagram in UML to describe the dynamic aspects of the system. Activity diagram is basically a flowchart to represent the flow from one activity

to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc. Activity diagrams are not only used for visualizing the dynamic nature of a system, but they are also used to construct the executable system by using forward and reverse engineering techniques.

5.2.3 Use case Diagram

A use case diagram is a dynamic or behaviour diagram in UML. Use case diagrams model the functionality of a system using actors and use cases. Use cases are a set of actions, services, and functions that the system needs to perform.

CHAPTER 6

SYSTEM IMPLEMENTATION

6.1 SOFTWARE APPROACH

6.1.1 Design of User Interface

Any product or web application is dynamic and interactive elements that are directly linked to users and impact the business' tasks and productivity. A web application has to be designed at the comfort level and ease of use with the end user in mind. If a web application is not easily understandable, the efforts go in vain. Maintaining consistency and uniformity in all pages and same goes with styling, is very important. Getting familiarized to the interface is time taking, hence maintaining consistency in elements like style, layout, color and font makes it easier and appealing to the user. [15]

User Interface (UI) Design focuses on anticipating what users might need to do and ensuring that the interface has elements that are easy to access, understand, and use to facilitate those actions. UI brings together concepts from interaction design, visual design, and information architecture.

6.2 HARDWARE APPROACH

6.2.1 Raspberry Pie

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python. All the sensors are connected to Raspberry pie.

6.2.2 DHT11–Temperature Sensor

The DHT11 is a commonly used Temperature sensor. The sensor comes with a dedicated NTC to measure temperature and an 8-bit microcontroller to output the values of temperature as serial data. The sensor is also factory calibrated and hence easy to interface with other microcontrollers.

6.2.3 Pulse rate sensor

Pulse Sensor is a well-designed plug-and-play heart-rate sensor which clips onto a

fingertip or earlobe. It operates at +5V or +3.3V and the current consumption is 4mA. It has an inbuilt amplification and noise cancellation circuit.

The sensor has two sides, on one side the LED is placed along with an ambient light sensor and on the other side we have some circuitry. This circuitry is responsible for the amplification and noise cancellation work. The LED on the front side of the sensor is placed over a vein in our human body. This can either be our fingertip or our ear tips, but it should be placed directly on top of a vein.

The LED emits light which will fall on the vein directly. The veins will have blood flow inside them only when the heart is pumping, so if we monitor the flow of blood, we can monitor the heart beats as well. If the flow of blood is detected then the ambient light sensor will pick up more light since they will be reflected by the blood, this minor change in the received light is analyzed over time to determine our heart beats.

6.3 MODULES

The software designed has two portals, one for the staff and doctors to enter update and retrieve the patient information. The second portal is the diagnosis portal on which the patients reading from the sensors are taken by the staff. The reading taken through sensors are then uploaded to the database after encrypting it. These readings are retrieved when require by the doctors or staff.

6.3.1 Logging into the website as Doctor and Staff

Step 1: User will be provided with three options, namely staff and doctor.

Case A: If the selected user is Doctor or staff

Case I: If the doctor or staff is already registered, he has to enter his username and password to login.

Case II: If the doctor or staff enters incorrect mail id and password, log in will be failed.

Doctors can view about the patient. The staff can register the information about new patients and also can enter the information from the sensors.

6.3.2 Key Generation and Algorithm Implementation

The algorithm consists of two parts:

a) Key Scheduling

b) Encryption Process

Key Scheduling:

Key is the most fundamental component in the process of encryption and decryption. The entire security of the data is dependent on the key. The secrecy of the data will be lost if an attacker happens to know the key. Therefore, the revelation of the key should be as difficult as possible. The Feistel network used here consists of five rounds each requiring five unique keys for the encryption/decryption purpose.

The proposed algorithm requires a 64-bit key. A 64-bit of data can be encrypted or decrypted using that key. In order to guard against exhaustive search attack, the length of the first key must be large enough so that it becomes difficult for the enemy to perform key searching attacks. We use a key generation algorithm for generating the 5 keys.

Key Generation Algorithm:

In this algorithm list, split_list, shuffle_list, temp_list, key_list and new_list are the temporary lists. Key1, key2, key3, key4 and key5 are the 5 keys obtained at the of the algorithm.

step 1: Start

step 2: Initialize

list[0]=first_character_of_name

list[1]=fist_character_of_dob

j=0

for i=2 to 13 do

list[i]=aadhar[j]

j++

list[14]=last_character_of_name

list[15]=second_character_of_dob

step 3: for each element in list

convert the element to ascii

step 4: for each element in list

convert the element into hexadecimal number

if hexadecimal number is alphanumeric at 1 st or 15th position

replace list[0] with 00

replace list[14] with 99

step 5: j=0

for each item in list

split_list[j++]=item[0]

split_list[j++]=item[1]

step 6: j=0

for i=0 to 4

shuffle_list[j++]=split_list[i]

shuffle_list[j++]=split_list[i+4]

shuffle_list[j++]=split_list[i+8]

shuffle_list[j++]=split_list[i+12]

shuffle_list[j++]=split_list[i+16]

shuffle_list[j++]=split_list[i+20]

shuffle_list[j++]=split_list[i+24]

shuffle_list[j++]=split_list[i+28]

step 7: for each item in shuffle_list

convert item into binary

split the binary to individual digits and make list of those digits

append the above obtained list to temp_list

step 8: for each item in temp_list //LFSR function

for i=0 to 4

xor_result=item[0] XOR item[3]

left shift the elements in item by position 1

replace the 4^{th} positon of item by xor_result

append the item to new_list

step 9: for each item in new_list

merge the elements in item into string

convert the obtained string to integer and convert to decimal

append obtained decimal to key_list

step 10: j=0

for i=0 to 8

if length(key_list[j])=1

key1[i]=key_list[j]

key2[i]=key_list[j+8]

key3[i]=key_list[j+16]

key4[i]=key_list[j+24]

else

temp1=key_list[j]

temp2=key_list[j+8]

temp3=key_list[j+16]

temp4=key_list[j+24]

key1[i]=temp1[0]

key2[i]=temp2[1]

key3[i]=temp3[0]

key4[i]=temp4[1]

step 11: shuffle key1 and key2

shuffle key3 and key4

step 12: key5[0]=key1[0]

key5[1]=key1[7]

key5[2]=key2[0]

key5[3]=key2[7]

key5[4]=key3[0]

key5[5]=key3[7]

key5[6]=key4[0]

key5[7]=key4[7]

step 13: stop

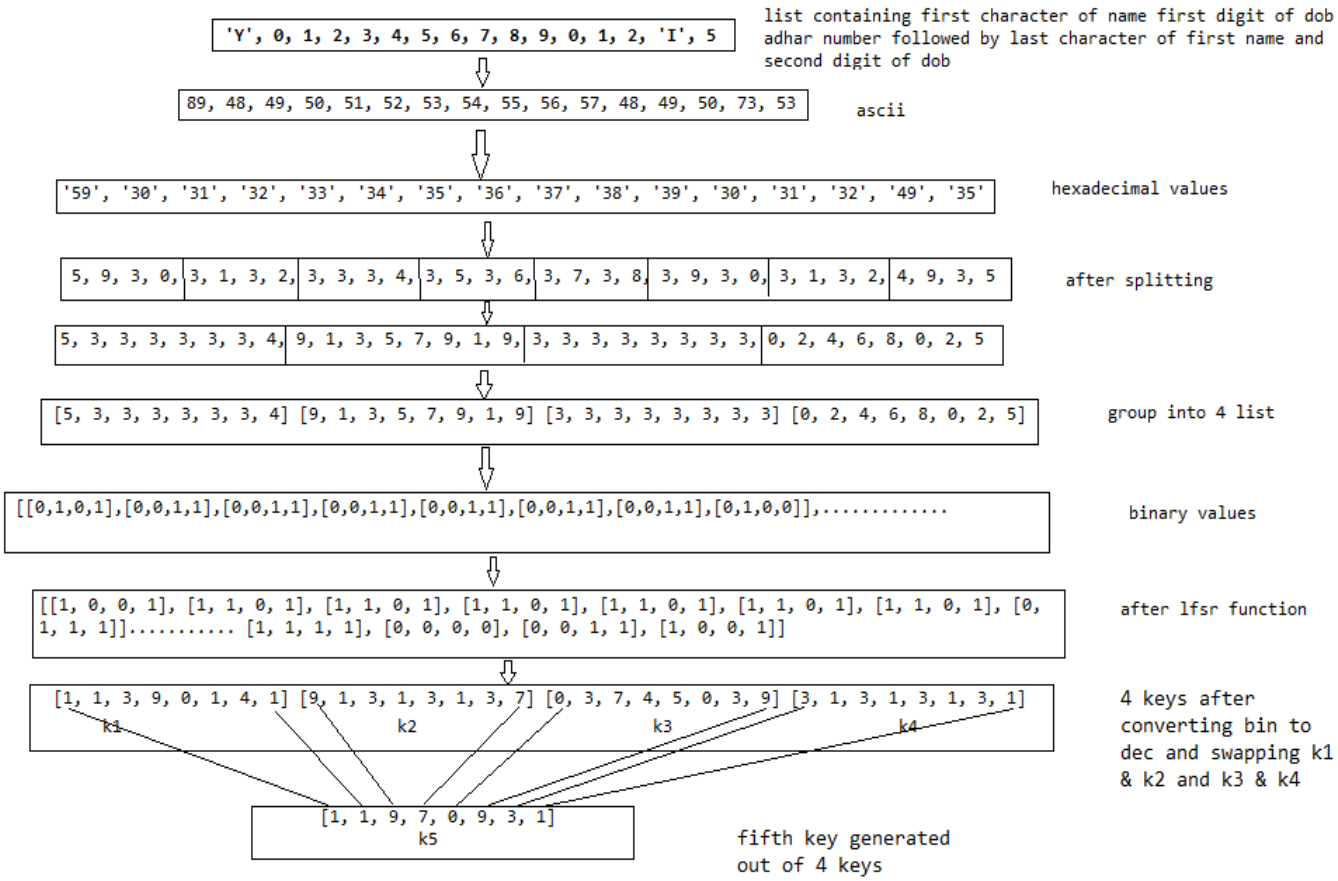


Figure 6.1 Generation of keys

Encryption:

The encryption process encrypts a 64-bit block of data in five rounds using five unique keys generated in the key expansion block. To create considerable confusion and diffusion this process is composed of some shifting, swapping, substitution, XOR, XNOR operations.

Step 1:

64 bit plain text is first divided into four segments of 16 bits.

P1(0-15), P2(16-31), P3(32-47) and P4(48-63).

Step 2 :

P1 = P1 XNOR K1

P4 = P4 XNOR K1

Step 3:

P1 = GFunction(P1)

P4 = GFunction(P4)

Step 4:

Temp1 = P1 XOR P3

Temp2 = P2 XOR P4

P2 = Temp1

P3 = Temp2

Step 5:

Swap P1 and P2

Swap P3 and P4

Step 6:

Repeat step 2 to step 5 with remaining keys K2, K3, K4 and K5

Step 6:

Merge P1, P2, P3, P4 to get 64 bit cipher text

The results of the final round are concatenated to obtain Cipher Text (Ct). The encryption process consists of five rounds and uses Feistel architecture. The data block is of 64-bit. The 64-bit data is divided into four 16-bit data. Each round utilizes one key; first round uses first key, second round uses second key and so on. Each key is used twice. In each round the innovated G-function is also used twice. This considerably reduces processing cycles. GFunction stores and returns the 16 bit data.

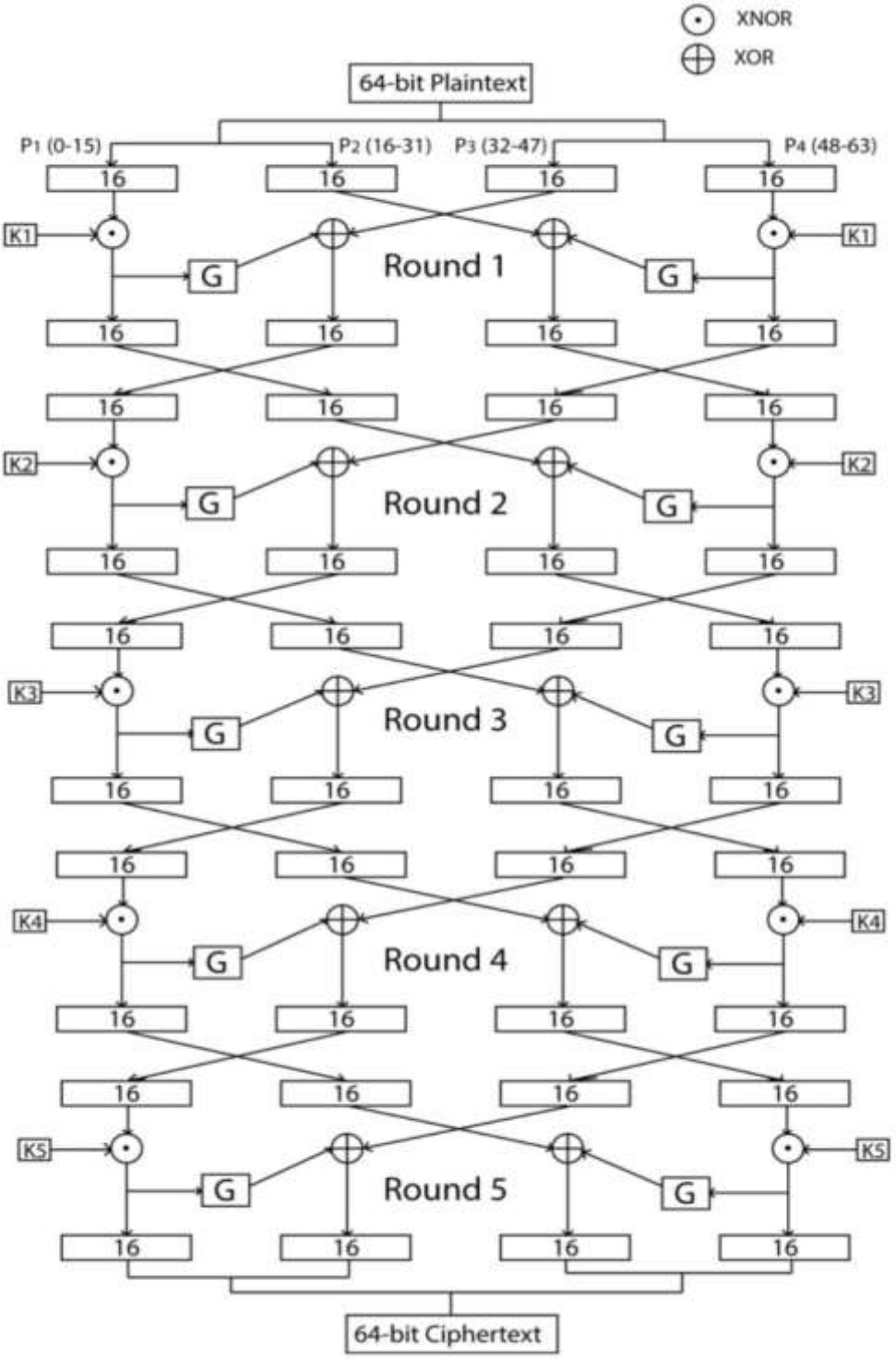


Figure 6.2 64 bit cipher text generation

CHAPTER 7

SYSTEM TESTING

7.1 INTRODUCTION

Software testing is a process used to identify the correctness, completeness and quality of the developed software. Testing is the process of questioning a product in order to evaluate it, where the questions are things the tester tries to do with the product and the product answers with its behaviour in reaction to probing of the tester.

Testing phase is performed after coding to detect all the errors and provide quality assurance and ensure reliability of the software. Testing is vital to the success of the system. During testing, the software to be tested is executed with a set of test cases, and the behaviour of the system for the test cases is evaluated to determine if the system is performing as expected. Clearly the success of testing in revealing errors depends critically on the test cases. [16]

7.2 UNIT TESTING

Unit Testing is a level of software testing where individual units/ components of a software are tested. The purpose is to validate that each unit of the software performs as designed. A unit is the smallest testable part of any software. It usually has one or a few inputs and usually a single output. In procedural programming, a unit may be an individual program, function, procedure, etc. In object-oriented programming, the smallest unit is a method, which may belong to a base/ super class, abstract class or derived/ child class. (Some treat a module of an application as a unit. This is to be discouraged as there will probably be many individual units within that module.) Unit testing frameworks, drivers, stubs, and mock/ fake objects are used to assist in unit testing.

The benefits of Unit Testing are:

- Unit testing increases confidence in changing/ maintaining code. If good unit tests are written and if they are run every time any code is changed, we will be able to promptly catch any defects introduced due to the change. Also, if codes are already made less interdependent to make unit testing possible, the unintended impact of changes to any code is less.

- Codes are more reusable. In order to make unit testing possible, codes need to be modular. This means that codes are easier to reuse.
- Development is faster. If you do not have unit testing in place, you write your code and perform that fuzzy 'developer test' (You set some breakpoints, fire up the GUI, provide a few inputs that hopefully hit your code and hope that you are all set.) But, if you have unit testing in place, you write the test, write the code and run the test. Writing tests takes time but the time is compensated by the less amount of time it takes to run the tests; You need not fire up the GUI and provide all those inputs. And, of course, unit tests are more reliable than 'developer tests'. Development is faster in the long run too. The effort required to find and fix defects found during unit testing is very less in comparison to the effort required to fix defects found during system testing or acceptance testing.
- The cost of fixing a defect detected during unit testing is lesser in comparison to that of defects detected at higher levels. Compare the cost (time, effort, destruction, humiliation) of a defect detected during acceptance testing or when the software is live.
- Debugging is easy. When a test fails, only the latest changes need to be debugged. With testing at higher levels, changes made over the span of several days/weeks/months need to be scanned.
- Codes are more reliable. I think there is no need to explain this to a sane person.

7.3 INTEGRATION TESTING

Integration Testing is a level of software testing where individual units are combined and tested as a group. The purpose of this level of testing is to expose faults in the interaction between integrated units. Test drivers and test stubs are used to assist in Integration Testing.

Definitions of integration testing are

Integration Testing**:**

- Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems.

Component Integration Testing**:**

- Testing performed to expose defects in the interfaces and interaction between integrated components.

System Integration Testing**:**

- Testing the integration of systems and packages; testing interfaces to external organizations (e.g. Electronic Data Interchange, Internet).

CHAPTER 8

RESULTS AND DISCUSSSIONS

8.1 USER INTERFACE

There are two portals that are being used in our project. One is the patient information portal and the other is the diagnosis portal.

Here are the various operations that could be done in the patient information portal.

Figure 8.1 Welcome page

Figure 8.2 Login Page

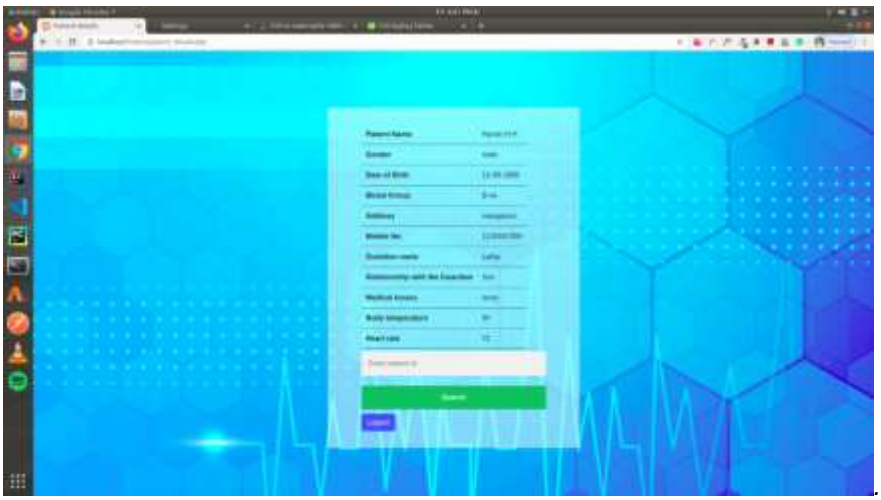


Figure 8.3 Patient Information

Figure 8.4 Patient Registration

Figure 8.5 Update patient details

The following are the operations that can be done on the diagnosis portal.

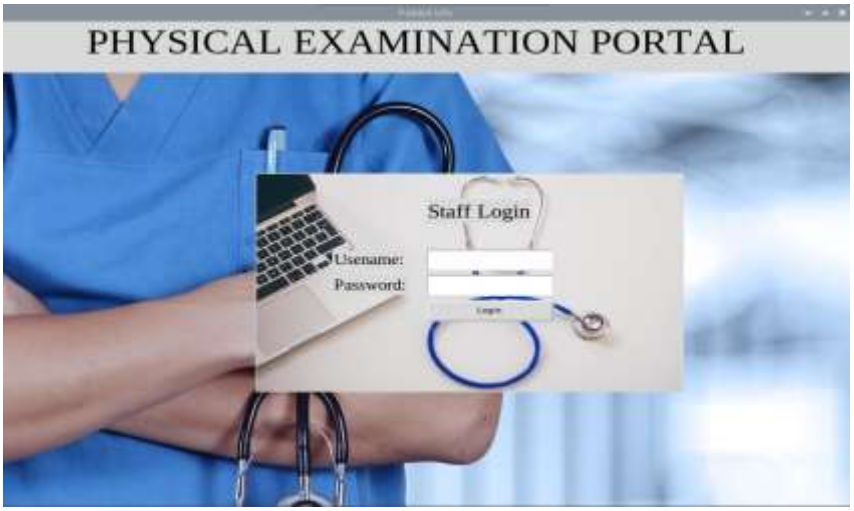


Figure 8.6 Staff Login portal

Figure 8.7 Patient Id to access his/her information

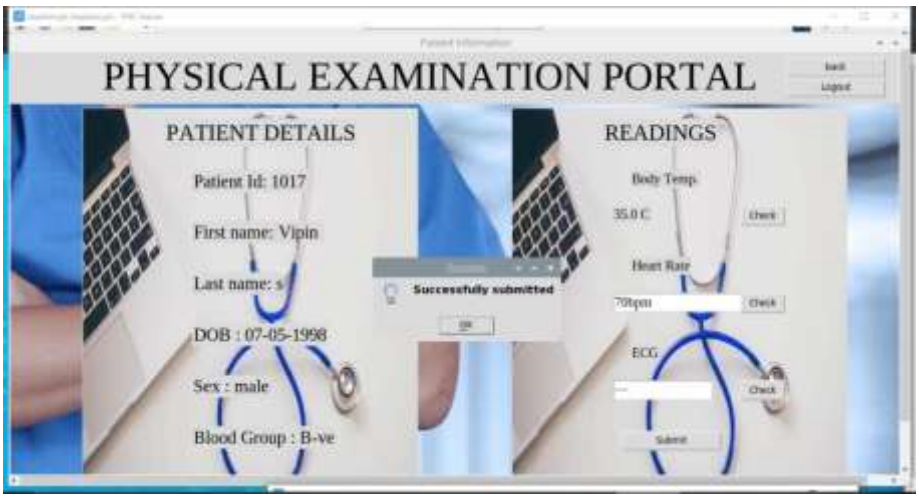


Figure 8.8 Patient Details and Readings

id	bodytemp	heartrate	ecg
1011	2691	6ddd	3bb6b67c
1012	c4fa9efa8da4	c7ad	7073e3a6
1013	1f9296db9f89	9a21ff1d	f88e94fa
1017	c4fa9efa8da4	9d5be9a39d18	7073e3a6

Figure 8.9 Snapshot of encrypted readings

8.2 DISCUSSIONS

The system that we have developed has multiple features that benefits the user. Further we want to focus more on making the device have an output with a higher and better accuracy, hence improving the overall performance of the system. We would also like to add more features to our system , like an option where the user's emergency contact and the hospital closest to his current location gets an alert message with all the readings and his current state. This can come in handy when usually when the patient has higher risk.

CHAPTER 9

CONCLUSION AND FUTURE WORK

9.1 CONCLUSION

The security of healthcare data has always been barrier due to low processing and data requirements of the healthcare devices. We have used a symmetric lightweight cryptography algorithm as its meets the necessary processing and memory requirements which are needed for healthcare devices you function efficiently . The project is successful at building a portable secure means of storing the patient's information. This project implements several realistic lightweight encryption algorithms suitable for IOT medical systems. The project implements a cryptographic algorithm resulting in fair analysis in terms of memory utilization and speed. The project attains a secure healthcare system considering the balance between the optimal requirement and the future threats.

We have made the use of sensors to collect medical data from the patient's body acquiring its transmission to the Healthcare system securely. We have ensured trust and data secrecy from the starting throughout the medical treatment to prevent any unauthorized access or unneeded interruption. In this project, we have designed a software in a such a way that it satisfies the requirements of doctors who use the data and the staff who upload the data into the storage units. The front end is developed by using Web Technologies like HTML and styling is done using CSS, bootstrap, with doctor and staff access.

The PHP is the backend for all the operations. The software also provides multiple additional features for the users which makes their interaction with the software flexible.

In this project we have generated a key which makes the encryption highly secure using the lightweight cryptography algorithm. The project also helps in making the hardware part i.e interfacing the sensors with the system more reliable and fast. Hence through this project we have successfully overcome the major problems and attained a secure Healthcare system.

9.1 FUTURE WORK

The system that we have currently developed has multiple features that benefits the user. Further we want to focus more on making the device have an output with a higher and better accuracy, hence improving the overall performance of the system. We would also

like to add more features to our system, like an option where the user's emergency contact and the hospital closest to his current location gets an alert message with all the readings and his current state. This can come in handy when usually when the patient has higher risk.

REFERENCES

[1] https://www.w3schools.com/about/

[2] https://blog.coursera.org/about/

[3] http://www.exforsys.com/tutorials/php/wamp-server.html

[4] https://www.lynda.com/HTML-tutorials/HTML-Essential-Training/170427-2.html

[5] https://medium.com/@mindfiresolutions.usa/how-relevant-is-php-for-web-developers-in-2017-66d8fca75f9f

[6] https://www.tutorialspoint.com/python/python_overview.htm

[7] https://techterms.com/definition/wamp

[8] https://www.upwork.com/hiring/development/server-side-scripting-back-end-web-development-technology/

[9] https://www.pythonforengineers.com/natural-language-processing-and-sentiment-analysis-with-python/

[10]https://www.pythonforengineers.com/natural-language-processing-and-sentiment-analysis-with-python/

[11] https://www.interaction-design.org/literature/topics/ui-design

[12]https://www.ministryoftesting.com/dojo/lessons/30-things-every-new-software-tester-should-learn

[13]https://www.researchgate.net/publication/257948587_A_survey_paper_on_e-learning_based_learning_management_Systems_LMS

[14]http://shodhganga.inflibnet.ac.in/bitstream/10603/34521/6/06_chapter1.pdf

[15] https://www.economicsnetwork.ac.uk/cheer/ch18/manochehr.pdf