

# **HOSPITAL MANAGEMENT SYSTEM WITH PATIENT MONITORING**

Sam Abraham Joshy (20BCE0986)  
Keerthi Sanjana A(20BCE2687)  
Riza Gaffoor(20BCE2395)  
Advaith Chandra Srivastav (20BCE0983)  
Sanjitha Rajesh (20BCE2541)

A report submitted for the J component of

CSE3501

Information Security Analysis and Audit

Supervisor: Dr. Ruby D



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering  
Vellore Institute of Technology, Vellore

## Declaration

This report has been prepared on the basis of my own work, And no other published or unpublished source materials have been used, these have been acknowledged.

Student Names:

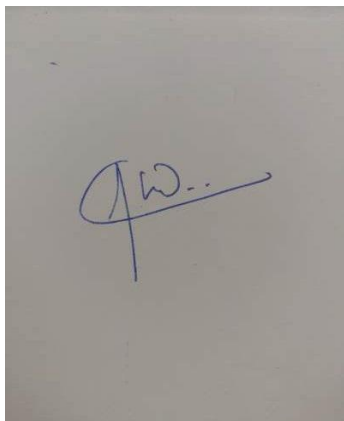
Sam Abraham Joshy (20BCE0986)

Keerthi Sanjana A(20BCE2687)

Riza Gaffoor(20BCE2395)

Advaith Chandra Srivastav (20BCE0983)

Sanjitha Rajesh (20BCE2541)

A handwritten signature in blue ink on a light gray background. The signature is stylized, starting with a large 'A' followed by 'W...' and a long horizontal stroke.

Signature

Date of Submission: 11/04/2023

# Table of Contents

Abstract. ....	4
Chapter 1: Introduction .....	5
Chapter 2: Literature Survey .....	8
Chapter 3: System Model .....	15
Chapter 4: Implementation .....	20
Chapter 5: Results and Discussions .....	23
Chapter 6: Conclusion & Future Scope .....	24
References.....	2

## **Abstract:**

Healthcare organizations must secure their websites and IoT systems due to the growing use of technology. This project examines hospital websites that use IoT technology and their vulnerabilities and attacks.

Understanding and analyzing cyber security threats and attacks on a hospital website with IoT technology is the goal. This will cover the website's technologies and social impact. Firewalls, intrusion detection, encryption algorithms, access control, and security protocols will be used in the project. Machine learning methods will also identify system threats and attacks. Technology in healthcare has made patient data security and privacy essential. A hospital website security breach can expose confidential patient data and damage patient trust.

This project will identify and mitigate cyber security vulnerabilities in a hospital website that uses IoT technology. The project also examines the social impact of such attacks and the importance of cyber security in healthcare.

# 1) Introduction

As technology continues to play a larger role in the healthcare industry, healthcare organisations must prioritise the security of their websites and IoT systems against potential cyber security threats and attacks. The goal of this project is to investigate the vulnerabilities in hospital websites that use IoT technology, as well as the various types of attacks that can be launched against such systems. The project's goal in conducting this analysis is to identify and address potential security gaps, as well as to provide recommendations for improving the overall security posture of hospital websites that use IoT technology.

Security is critical in hospital administration because hospitals store and manage highly sensitive data, such as patient health information and medical records. Any compromise of this information can have serious ramifications, including identity theft, insurance fraud, and even medical malpractice. The hospital management system must be safe and secure, with all necessary safeguards in place to protect against potential threats.

Patient privacy is a major concern in hospital administration. Patients rely on healthcare providers to safeguard their personal and medical information, and it is the hospital's responsibility to do so. To prevent access, it is critical to have secure methods of communication, including secure channels for data transfer and storage, such as encryption.

Physical security of medical equipment and devices is another critical aspect of hospital security. Medical devices are frequently costly and valuable, and they contain sensitive information. Unauthorized access to these devices can pose a significant security risk, so hospitals must take precautions to keep them secure.

Cybersecurity threats are also a major concern in hospital administration. Malware, viruses, and other types of cyberattacks can jeopardize patient data security, with serious consequences. To protect against these types of threats, hospitals must implement cybersecurity protocols such as regular software updates and antivirus software.

Finally, the significance of security in hospital administration cannot be overstated. Patient data and medical device security are critical to the proper operation of healthcare systems, and hospitals must take steps to ensure that appropriate safeguards are in place to protect against potential threats.

The project aims to display patients' heart rates in every room, which is an important aspect of monitoring patients' health in hospitals. The project also includes key pair encryption to protect

data transfer to ensure the security and privacy of patient data. Key pair encryption is a secure method of communication that encrypts and decrypts data using two keys, a public key and a private key. This ensures that the data transfer is secure and that the patient's health data is not compromised. The project uses this encryption technology to provide a secure and reliable way to display patient health data, which is an important aspect of hospital management.

WBAN protocols are used to connect medical devices to a network, allowing patient health data to be transferred to a central system. These protocols are important because they ensure that medical devices can communicate securely and reliably with one another, allowing for accurate and timely data transfer.

WBAN protocols typically operate at 2.4 GHz and employ low-power wireless technologies such as Bluetooth Low Energy (BLE), Zigbee, or IEEE 802.15.6. WBAN protocols are notable for their ability to support multiple devices in close proximity. This is important in medical settings where multiple medical devices may be used to monitor a patient's health at the same time. WBAN protocols can also support a variety of sensor types, such as temperature sensors, ECG sensors, and accelerometers. Another important feature of WBAN protocols is their ability to support various levels of security. Because patient health data is extremely sensitive, WBAN procedures include security features such as authentication, encryption, and access control. This safeguards the data against unauthorized access and modification.

In the application, socket programming is used to simulate real-time data transfer. This is important because it ensures that the data displayed is current and accurate. Socket programming is a technique used to establish a connection between two devices over a network in order to allow real-time data transfer. Socket programming can be used in the project to simulate real-time data transfer between medical devices that measure patients' heart rates and the hospital management system.

The project establishes a connection between the devices and the system using socket programming, allowing for the real-time transfer of heart rate data. When a new reading is taken, the devices can be configured to send data to the server, which can then process and display the data to the healthcare provider in real-time. This real-time data transfer enables healthcare providers to detect and respond to any abnormalities in the patient's heart rate.

The website in the project is built with HTML, CSS, and JavaScript, and the backend is built with PHP. Socket programming is used in the PHP code to allow for real-time data transfer between devices and the server. Socket programming is a powerful tool that can be used to simulate real-time data transfer between medical devices and the hospital management system. The server is configured to listen for incoming data from the devices, and the data is processed and displayed on the website in real-time. By incorporating this technique into the project, we

provide healthcare providers with a dependable and efficient method of monitoring patients' heart rates.

A Python script is used in the project to connect to the same SQL database that the hospital management system uses. This enables the Python script to perform database read and write queries, allowing it to access and manipulate patient data. The Python script can retrieve heart rate data from the database, perform calculations, and generate patient health reports. It can also be used to add new readings and other patient information, such as medication records and appointment schedules, to the database.

The Python script can seamlessly integrate with the system and share data with other project components by using the same SQL database as the hospital management system. This ensures that healthcare providers have access to accurate and up-to-date patient data, allowing them to make informed decisions about patient care. The Python script is crucial to the project because it connects to the SQL database and performs read and write queries. This allows it to access and manipulate patient data, which is critical for effective patient care management. The project ensure that healthcare providers have access to the data they need to provide high-quality care to patients by integrating the Python script with the hospital management system.

## 2) Literature Survey

Sl.No	Name of the transaction/journal/conference with year	Major technologies used	Results/Outcome of their research	Drawbacks if any
1	Load control and load balancing in a shared database management system	The proposed system effectively balances the load on the shared database, resulting in improved performance and reduced downtime.	The system may require significant computational resources and may not be suitable for smaller systems.	The system may require significant computational resources and may not be suitable for smaller systems.
2	IEEE Website Attacks and its vulnerabilities	Web security, network protocols, cryptography.	The paper presents an overview of common website attacks and vulnerabilities and discusses current methods for mitigating these threats.	The mitigation techniques may require significant resources and may not be effective against new and evolving threats.
3	Cybersecurity	Network security, cryptography, machine learning	The paper provides a comprehensive overview of the field of cybersecurity and discusses various techniques and technologies used to secure digital systems and networks.	Some security techniques may have limitations and may not be effective against new and evolving threats
4	An impact review on internet of things attacks	Internet of things, network security, cryptography	The paper provides a review of the various attacks that can impact internet of things (IoT) systems and their potential consequences.	Some security solutions may not be practical for resource-constrained IoT devices and may require significant resources to implement.
5	Research of Web Resources Protection Based on Digital Watermarking and Digital Signature	Digital watermarking, digital signature, web security	The paper presents a study on using digital watermarking and digital signature to protect web resources. The research evaluates the effectiveness and limitations of these techniques for web resource protection.	Some digital watermarking and signature techniques may have limitations in terms of data size, processing time, and robustness.



6	Internet of Things: Security vulnerabilities and challenges	Internet of Things (IoT), network security, cryptography	The paper presents a study on the security vulnerabilities and challenges faced by the Internet of Things. The study looks at the different security risks that IoT devices and networks face and suggests ways to reduce these risks.	The implementation of security measures for IoT devices may require significant resources and time.
---	---	--	--	---

### 1. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks

Authors: Mohamed Abomhara and Geir M. Kjøien

Published in 2015

This study introduced security issues and risks to the IoT, focusing on confidentiality, privacy, and entity trust. It also discussed cyber threats, which include people, motives, and capabilities fueled by cyberspace. It was found that threats coming from intelligence agencies and criminal gangs are more challenging to counter than those coming from lone hackers, due to individual attacks having less severe effects while their targets may be less predictable. The article also attempted to categorize various threat types.

### 2. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics

Authors: Yang Lu, Li Da Xu

Published in 2019

The Internet of Things (IoT) is an emerging technology that has changed the way people, intelligent objects, smart devices, information, and data are connected on a global scale. It is a secure network for people, software/hardware, processes, and things, providing a higher level of interoperability, confidentiality, scalability, accessibility, integrity, and availability.

### 3. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components

Authors: Jose Fran Ruiz; Rajesh Harjani; Antonio Mana; Vasily Desnitsky; Igor Kottenko; Andrey Chechulin

Published in 2012

This research provides an integrated methodology for designing embedded systems with increased security. It uses a modelling tool called Domain Security Metamodel (DSM) to

create a threat model that details the threats and attacks that affect certain security features in particular domains. The Security Framework for Security Aspects (for systems development) and the Intruder Model (for DSM development) make up the methodology.

#### **4. Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System**

Authors: Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson  
Published in 2016

This research presents a neural network-based approach to intrusion detection, one that distinguishes between benign and malicious patterns in a network of Internet-connected devices. A supervised ANN called a multi-level perceptron is trained, and then its ability to withstand Distributed Denial of Service (DDoS) attacks is measured. Data from several IoT network nodes is collected, analysed, and distributed denial of service attacks are detected using the ANN approach. It had high true and false positive rates and was effective in recognising a variety of assault types.

#### **5. Network Security: Threat Model, Attacks, and IDS Using Machine Learning**

Authors: Divya Kapil; Nidhi Mehra; Atika Gupta; Sudhanshu Maurya; Anupriya Sharma  
Published in 2021

This research effort presents threat models for multiple networking layers. The NSL KDD dataset is used for the experimental investigation, and the findings for TPR, precision FPR, F-measure, and recall parameters are provided for Nave Bayes, Random forest, and J 48 classification algorithms. The process of creating a reliable system is demanding and requires additional security personnel as well as all potential risks. A system or Framework must be examined for malicious behaviour or strategy violations.

#### **6. Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach**

Authors: Farhan Ullah; Hamad Naeem; Sohail Jabbar; Shehzad Khalid; Muhammad Ahsan Latif; Fadi Al-turjman; Leonardo Mostarda  
Published in 2019

This research uses a combination of deep learning algorithms to detect malware-infected files and fake software across an IoT network. The TensorFlow deep neural network is used to filter the noisy data and hone in on the significance of each

token in terms of source code plagiarism. Color image visualisation is used to identify malware characteristics, which are subsequently used to train a deep convolutional neural network. The results of the experiments demonstrate that the combination technique yields the best classified results.

## **7. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study**

Authors: Mamoon Humayun, Mahmood Niazi, Noor Zaman

Published on January 2020

For the purpose of identifying and analysing typical cyber security vulnerabilities, this study identified and examined 78 primary studies. To demonstrate the publication venue, country of publication, and important targeted infrastructures and applications, data was combined and evaluated. The findings demonstrated that the security strategies previously discussed only addressed security in general, and that the solutions proposed in these research required more empirical verification and practical application.

## **8. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks**

Authors: Mohamed Abomhara and Geir M. Kjøien

Published on January 2015

Devices connected to the Internet of Things (IoT) are quickly becoming commonplace, and their success has not gone unnoticed. IoT cyberattacks are nothing new, but since IoT will be so pervasive in the lives and communities, cyber defence must be taken seriously. In this study, threat types are classified, and IoT device and service intruders and attacks are examined and described.

## **9. Cyber sity: Study on Attack, Threat, Vulnerability**

Authors: TUSHAR P. PARIKH, DR. ASHOK R. PATEL

Published on June 2017

Cyber infrastructure, such as hardware and software systems, networks, enterprise networks, intranets, and the usage of cyber intrusions, are the focus of this investigation into assault, threat, and vulnerability. It describes the surge in cybercrime, the factors that contribute to it, and the value of cyber security. Preventative actions and potential answers are suggested.

#### **10. Cyber Security Attacks, Threats, and Vulnerabilities**

Authors: Dr. Mahesh Sharma, Dr. Seema Nath Jain

Published on May 2022

This investigation aims to understand the significance of network invasions and cyber-theft, its role in community infiltration and cyber theft, and the reasons for the rise in cybercrime. It also provides preventative measures and practical remedies to reduce the impact of cyber attacks.

#### **11. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments**

Published on November 2021

This study seeks to analyze the difficulties, shortcomings, and strengths of the suggested approaches as well as evaluate and thoroughly review the standard advancements in the field of cyber security. The history of early-generation cyber-security techniques are explored along with standard security frameworks. New developments and emerging trends are presented. The thorough review study is anticipated to be beneficial for IT and cyber security researchers.

#### **12. A Survey on Internet of Things: Security and Privacy Issues**

Authors: J. Sathish Kumar, Dhiren R. Patel

Published on 2014

This paper introduces the Internet of Things (IoT), which provides the ability to recognise and link physical things located all over the world into a single system. Serious concerns are being expressed as a result of IoTs regarding access to personal information pertaining to devices and individual privacy. The security risks and privacy issues posed by IoT are summarised in this survey.

#### **13. Development of a Low-Power Heart Rate Monitor Device for Observation of Heart Rate Variability**

Authors: Haziq Kamarul Azman; Abd Hafiz Qayyum Abd Talib; Kushsairy Kadir

Published in: 2019

A new concept in heart rate variability acquisition was presented by modifying the IPFM model, implemented as a low-power solution, and captured similar profile as with the

gold standard with good performance ( $MSE = 1.73 \times 10^{-4}$ , Pearson correlation 0.99). Study of the effect of acquisition resolution showed that variability profile can be captured with good performance for a range of frequency.

#### **14. Comparison between Noninvasive Heart Rate Monitoring Systems using GSM Module and ESP8266 Wi-Fi Module**

Authors: Anadi Ranjan Barai; Md Rysul Kibria Badhon; Fatematuz Zhora; Md. Rakib Rahman

Published in: 2019

ESP8266 Wi-Fi module-based heart rate monitoring allows doctors to prevent heart attacks, while GSM-based modules just give SMS alerts for tachycardia or bradycardia. Both gadgets have limits. Both systems' pulse sensor photomasks are not lightproof. Therefore measurement can be somewhat off. Microprocessors are quieter than Arduino. ESP8266 Wi-Fi module is more versatile, accurate, and cheaper.

#### **15. IoT Based Health Monitoring System**

Authors: Gowtham S; Venkatesh L; Rajendra Varaprasad B; Diwakar SS; Aarthi N

Published in 2021

The proposed system is a remote health monitoring system that allows doctors to manage patients from one place and patients to wear a lightweight device to monitor their own health. The data is logged to a database and accessible by both doctors and patients from their respective web portals. The adoption of the system in mass scale in due course of time could make it necessary and affordable.

#### **16. SHANE – Smart HeartRate Analysis and Notification System for Emergencies**

Author: T. Venkat Narayana Rao; Gadige Vishal Sai; Panyala Harsha Vardhan Reddy; Sai Harsha Bandarupally; Chukka Nikhil

Published in 2021

SHANE helps identify sudden abnormality in a person's resting heart rate with real-time data gathered from SMART Hospitals, APIs, etc. It focuses on reducing the number of health issues caused by Cardio Vascular Diseases. Future scope includes using other sensors, machine learning to identify trends in SMV values, and design to improve user experience. The system performs with an accuracy of 93%.

#### **17. Strengthening Database Security with Capture the Flag Exercises**

Authors:Ruben Hubert; Anna Bánáti; László Erdődi; Rita Fleiner  
Published on: 2022

Two co-working participants discovered that it was possible to upload php files to the system by exploiting an unrestricted file upload vulnerability, which arose from a profile photo upload functionality in the administrative section of the application. They uploaded a web shell and launched further attacks on the system from there..

#### **18. Alphanumeric Database Security through Digital Watermarking**

Authors:Akshata A. Churi; Vinayak D. Shinde  
Published on: 2020

Digital watermarking techniques have been used for a long time, but they are limited to a limited set of characters. The proposed system is applicable to both numerical and non-numerical databases and will apply an optimal watermark in a shorter amount of time and preserve the original database quality. It will verify the watermark and get the original data from the database faster than existing techniques.

#### **19. Load control and load balancing in a shared database management system**

The proposed system does a good job of balancing the load on the shared database, which means it will work better and have less downtime. The system may need a lot of computing power and may not work well with smaller systems. The system may need a lot of computing power and may not work well with smaller systems.

#### **20. Cybersecurity**

Network security, cryptography, and machine learning The paper give a broad overview of the field of cybersecurity and talks about the different methods and technologies used to protect digital systems and networks. Some security techniques may have limitations and may not be effective against new and evolving threats

#### **21. Research of Web Resources Protection Based on Digital Watermarking and Digital Signature**

Digital watermarking, digital signatures, and web security. The paper presents a study on using digital watermarking and digital signatures to protect web resources. The research evaluates the effectiveness and limitations of these techniques for web resource protection. Some digital watermarking and signature techniques may have limitations in terms of data size, processing time, and robustness.

## **Gaps In Literature Survey:**

Based on the wide range of research papers from different fields, it is clear that there are many gaps in the existing literature that need to be filled. One thing that all of the papers have in common is the need for better methods and rules to protect data security and privacy in the face of more cyber attacks. Also, there doesn't seem to be much standardization in the fields of machine learning and database management, which can make it harder to make systems that work well and are reliable. Another gap is the need for more robust and reliable wireless body area network (WBAN) protocols that can help collect and send healthcare data with little interference. The project need to switch to encryption algorithms that can't be broken by a quantum computer because the ones we use now can be. Overall, these gaps show that more research and development is needed in these fields to solve the problems that exist right now.

### 3) System Model

#### Overview

The hospital management system has a website as a UI to display all the details coming from the database. The website shows the details of all the patients in the hospital with their respective Room numbers, Heart rate, and Personal information.

The heart rates are read from the database using a script that sends an XML HTTP request to a PHP file to read the heart rates every 1 second. The heart rate system is a combination of 2 python scripts acting as a sender and a receiver. All data is transported using socket programming and TCP protocols. The sender encrypts the data and the receiver decrypts it and appends it to the database.

#### Overall Architecture Diagram

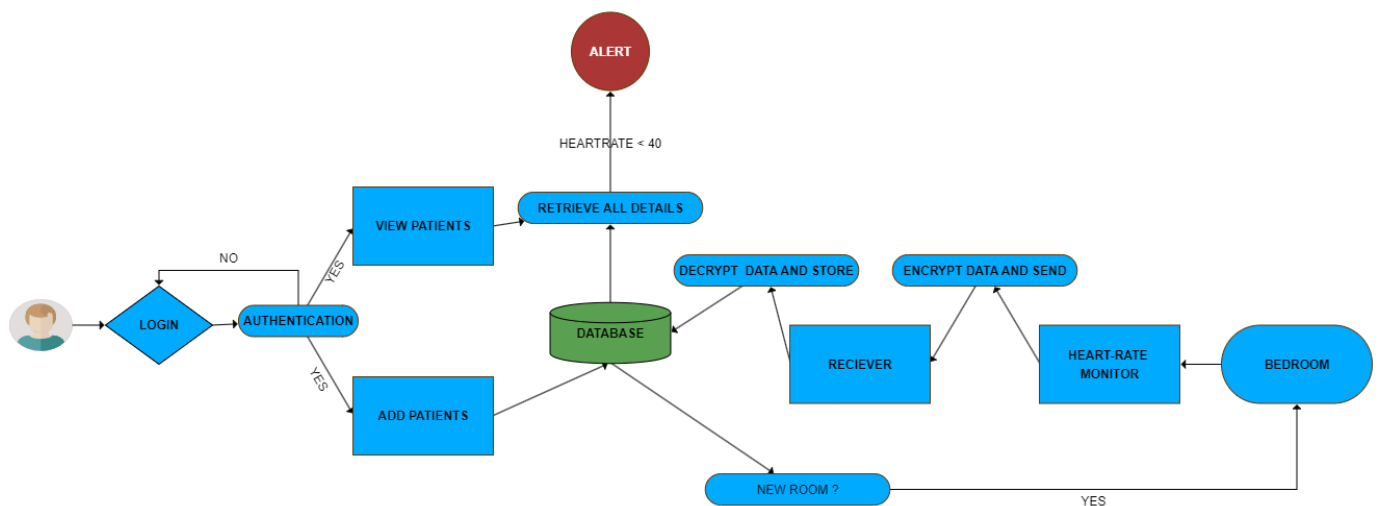


Fig. 3.1: Architectural Diagram, describing the steps of the system.



## Subsystem and Modules

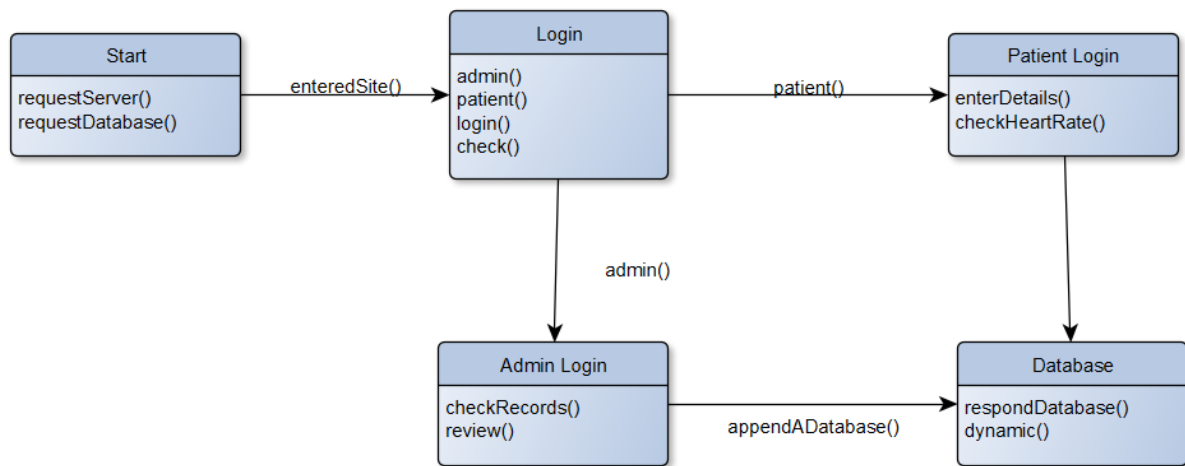
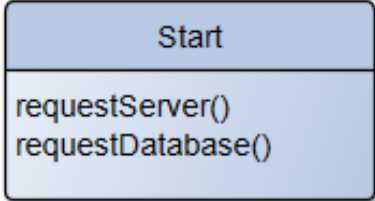
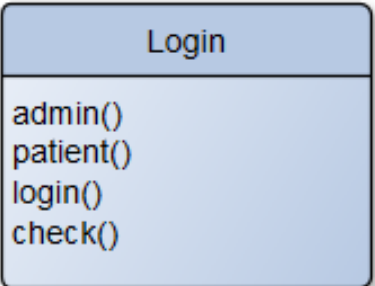
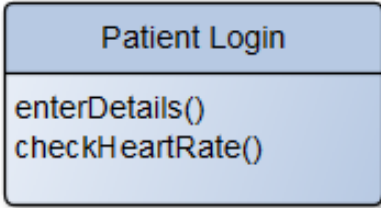
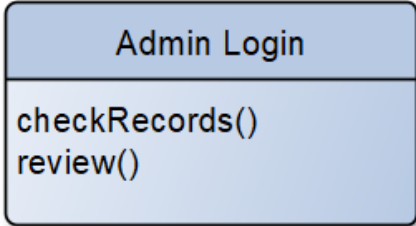
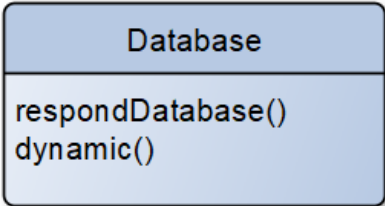


Fig. 3.2: State Transition Diagram, describing the steps of the system.

### 3.1 Module 1 (Website)

 <p>Fig. 3.2.1: Module 1 - Start.</p>	<h4>3.1 Start</h4> <p>The requestServer() function could be a custom function that initiates such requests to a server. The requestDatabase() function could be a custom function that interacts with a database server to retrieve or modify data.</p>
 <p>Fig. 3.2.2: Module 2 - Login. tv</p>	<h4>3.2 Login</h4> <p>admin() function could be used to authenticate users with administrative privileges, manage system configurations, or perform maintenance.</p> <p>patient() function could be used to create, read, update, or delete patient records, store medical histories or treatment plans, or generate reports about patient data</p> <p>login() function could present a login page or form to users, validate their credentials</p> <p>check() function could be used to validate user</p>

	input in a form, ensuring that a file or database record meets certain criteria.
 <p>Fig. 3.2.3: Module 3 - Patient Login.</p>	<p><b>3.3 Patient Login</b></p> <p>enterDetails() function could be used to collect information about a patient's personal details, and medical history</p> <p>checkHeartRate() function could analyze heart rate readings collected from a wearable device or medical equipment to identify irregularities</p>
 <p>Fig. 3.2.4: Module 4 - Admin Login.</p>	<p><b>3.4 Admin Login</b></p> <p>checkRecords() function could be used to validate the completeness or accuracy of patient records, financial transactions, or inventory data.</p> <p>review() function could be used to analyze the usability, security, or performance of an application or feature.</p>
 <p>Fig. 3.2.5: Module 5 - Database.</p>	<p><b>3.5 Database</b></p> <p>respondDatabase() function could be used to parse or transform data retrieved from a database.</p> <p>dynamic() variable type could be used to represent values that can change type or value during runtime</p>

### 3.2) Module 2 (Heart Rate Monitor)

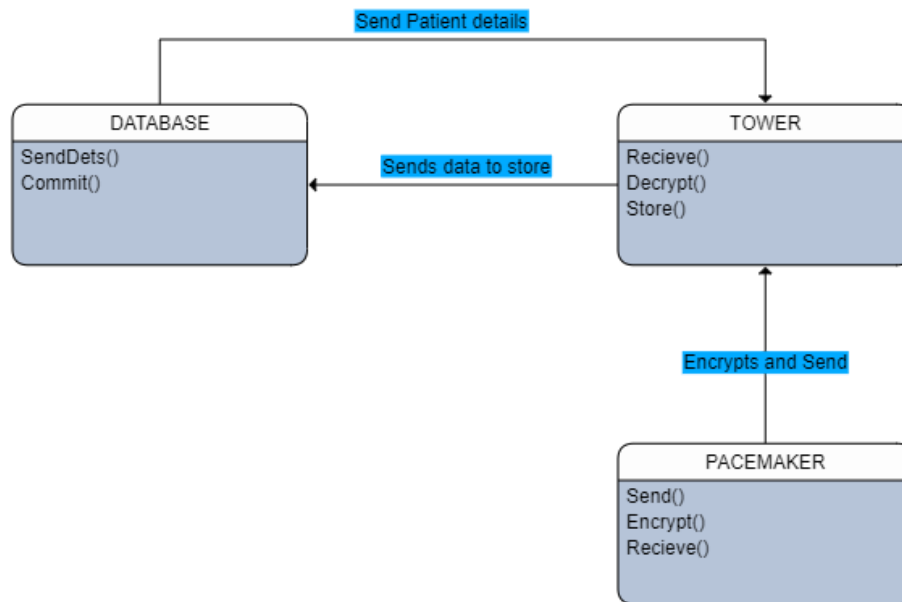


Fig 3.2.0 State transition Diagram of Module 2

<p>Fig. 3.2.1: Module 3.2.1 - Pacemaker.</p>	<p><b>3.2.1)Pacemaker</b></p> <p>Send() function could be used to manage data transmission between a pacemaker device and a receiver.</p> <p>Receive() function could be used to collect data from a pacemaker device</p> <p>Encrypt() function encrypts the heartrate data received.</p>
<p>Fig. 3.2.1: Module 3.2.1 - Pacemaker.</p>	<p><b>3.2.2)Tower</b></p> <p>Recieve() function receives the encrypted data from the pacemaker</p> <p>Decrypt() function decrypts the encrypted message and stores it in a variable</p> <p>Store() function is an SQL command function to store the data in the databases</p>

<div data-bbox="315 296 683 499"><p>DATABASE</p><p>SendDets() Commit()</p></div> <p data-bbox="310 527 691 554">Fig. 3.2.1: Module 3.2.1 - Database.</p>	<p data-bbox="824 289 1057 325"><b>3.2.3)Database</b></p> <p data-bbox="824 331 1421 506">SendDets() function sends the room and patient details to the tower to create a new instance for the heartrate generation</p> <p data-bbox="824 512 1421 596">Commit() function saves the data received from the tower</p>

## 4) IMPLEMENTATION

Source Code:

Website

```
if (parseInt(row['Heart_Rate']) < 80) {
    tableRow.style.backgroundColor = 'red';
}
// add the row to the table body
document.getElementById('table-body').appendChild(tableRow);
});
} else {
    console.log('Request failed. Status:', this.status);
}
};
xhr.send();
}, 10);
}

getData();
</script>
<tbody id="table-body">

</tbody>
</table>
<br>
</div>
<div class="tab-pane fade" id="add-pat" role="tabpanel" aria-labelledby="list-pat-list">

<div class="col-md-8">
</div>
<form action="addpatient.php" method="POST">
<div class="label-group">
<label for="room_no">Room Number</label>
<label for="fname">First Name</label>
</div>
<div class="input-group">
<input type="text" id="room_no" name="room_no" required>
<input type="text" id="fname" name="fname" required>
</div>
<div class="label-group">
<label for="lname">Last Name</label>
<label for="email">Email</label>
</div>
</div>
```

The website provides the user interface for the nurse station to view and monitor the patients from a single location.

## Pacemaker.py

```
device.py > ...
1  import socket
2  from datetime import datetime
3  import random
4  import time
5  from cryptography.fernet import Fernet
6  import mysql.connector
7  mydb = mysql.connector.connect(
8      host="localhost",
9      user="root",
10     password="",
11     database="myhmsdb"
12 )
13
14
15 def collectpid():
16     mycursor = mydb.cursor()
17     mycursor.execute("SELECT pid FROM patreg")
18     pid_list = [row[0] for row in mycursor.fetchall()]
19     return pid_list
20
21
22 def encrypt(message, key):
23     f = Fernet(key)
24
25     encrypted_message = f.encrypt(message.encode())
26     return encrypted_message
27
28 device_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
29 device_socket.connect(('localhost', 8888))
30 while True:
31     patient_list = collectpid()
32     patientid = random.choice(patient_list)
33     value = random.randint(40, 100)
34     message = encrypt(str(patientid)+"", "+str(value)+"", "+str(datetime.timestamp(
35         datetime.now()))", 'iVvNNUzoA2fEM_b-02z9W8XvskMXkw_cMMJ51YGTzn0=')
36     device_socket.send(message)
37     time.sleep(0.3)
38
39 # Close the socket connection
40 device_socket.close()
```

This is the python script to generate the heartrate values and send them to the tower using a TCP protocol. The Heartrates are encrypted using a key.

## Tower.py

```
tower.py > updater
1  import socket
2  from datetime import datetime
3  import time
4  from cryptography.fernet import Fernet
5  import mysql.connector
6  mydb = mysql.connector.connect(
7      host="localhost",
8      user="root",
9      password="",
10     database="myhmsdb"
11 )
12 def decrypt(encrypted_message, key):
13     f = Fernet(key)
14     decrypted_message = f.decrypt(encrypted_message)
15     return decrypted_message.decode()
16 def updater(rate,pid):
17     mycursor = mydb.cursor()
18     sql = "UPDATE patreg SET Heart_Rate = '"+str(rate)+"' WHERE pid = '"+str(pid)+"'"
19     mycursor.execute(sql)
20     mydb.commit()
21 receiver_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
22 receiver_socket.bind(('localhost', 8888))
23 receiver_socket.listen(1)
24 print("Waiting for device to connect...")
25 device_socket, device_address = receiver_socket.accept()
26 print("Device connected:", device_address)
27 while True:
28     message = device_socket.recv(1024)
29     values = decrypt(message.decode(), 'iVvNNUzoA2fEM_b-02z9W8XvskMXkw_cMMJ51YGTZn0=').split(',')
30     updater(values[1],values[0])
31     time.sleep(0.3)
32     dt = datetime.now()
33     ts = datetime.timestamp(dt)
34
35     print(ts)
36 device_socket.close()
37 receiver_socket.close()
38
```

This is the python script to receive the heart rates from the device. The decrypt function decrypts the data using the same key used in the device.py

## 5) RESULTS AND DISCUSSIONS

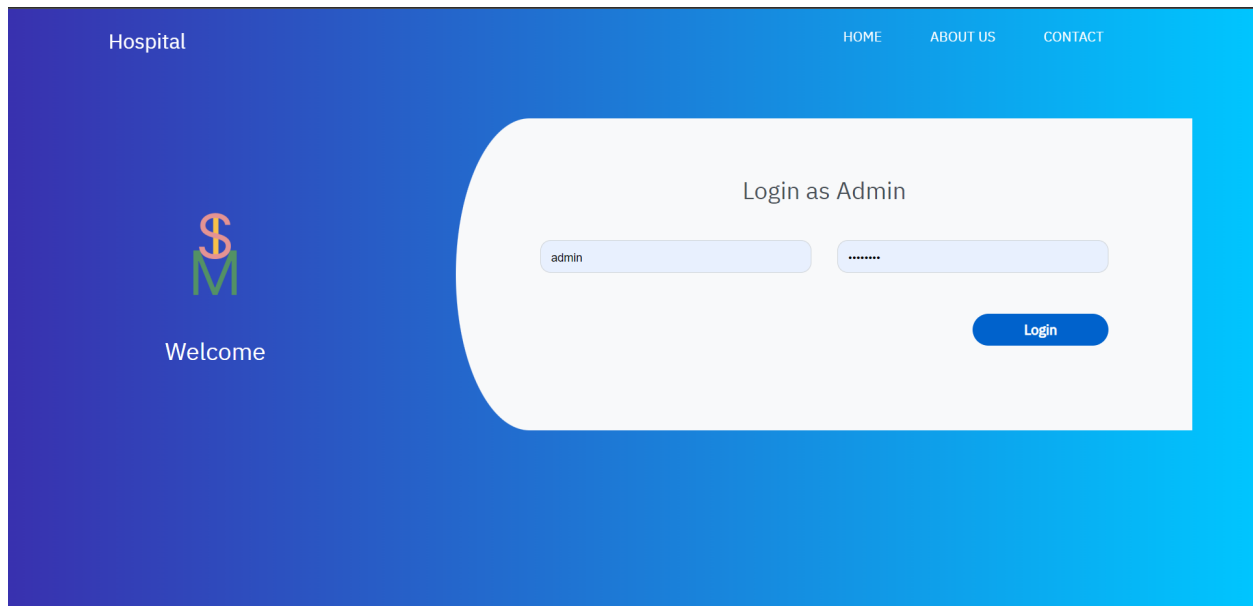
System print of all the values shared from the device to the tower in the terminal

```
PROBLEMS 11 OUTPUT DEBUG CONSOLE TERMINAL COMMENTS

Traceback (most recent call last):
  File "C:\wamp64\www\Pacemaker_hospital_monitor\device.py", line 28, in <module>
    device_socket.connect(('localhost', 8888))
ConnectionRefusedError: [WinError 10061] No connection could be made because the target machine actively refused

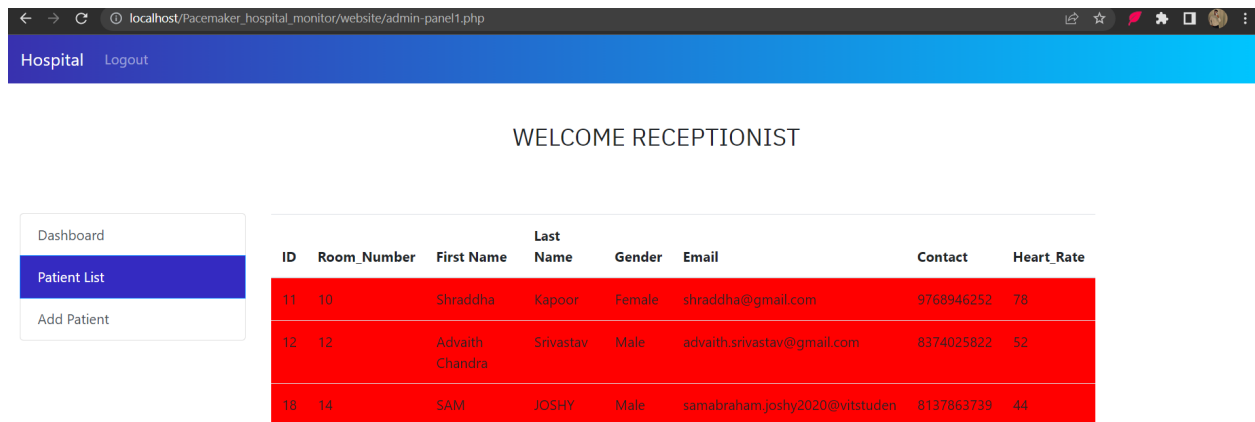
C:\wamp64\www\Pacemaker_hospital_monitor>python tower.py
Waiting for device to connect...
1680456527.953745
1680456528.264599
1680456528.574225
1680456528.884551
1680456529.196044
1680456529.508317
1680456529.820635
1680456530.134717
1680456530.447981
1680456530.757303
1680456531.070421
1680456531.381356
```

Landing page of the website



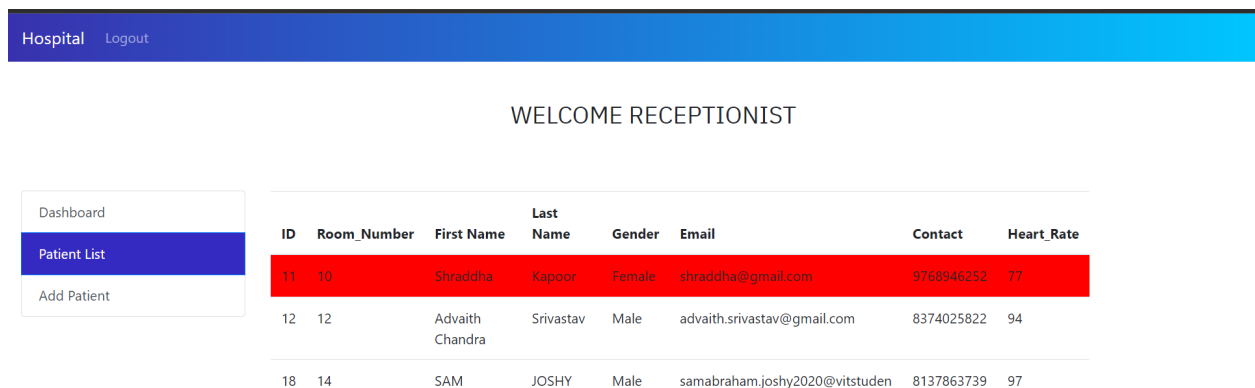


Website shows the details of the patients with respective patients and it gets updated every 1 second. All the patients are highlighted in red because their heartrates are below a certain level



ID	Room_Number	First Name	Last Name	Gender	Email	Contact	Heart_Rate
11	10	Shradha	Kapoor	Female	shraddha@gmail.com	9768946252	78
12	12	Advaith Chandra	Srivastav	Male	advaith.srivastav@gmail.com	8374025822	52
18	14	SAM	JOSH Y	Male	samabraham.joshy2020@vitstuden	8137863739	44

This screenshot below again shows that only if the patient's heart rate falls below a certain level it is highlighted as red.



ID	Room_Number	First Name	Last Name	Gender	Email	Contact	Heart_Rate
11	10	Shradha	Kapoor	Female	shraddha@gmail.com	9768946252	77
12	12	Advaith Chandra	Srivastav	Male	advaith.srivastav@gmail.com	8374025822	94
18	14	SAM	JOSH Y	Male	samabraham.joshy2020@vitstuden	8137863739	97

## **6) CONCLUSION & FUTURE SCOPE**

In conclusion, consumers and medical professionals in need of precise and dependable heart rate data will find the heart rate monitoring system with a website and its security measures to be an excellent solution. The device provides continuous monitoring of heart rate, allowing users to immediately identify and address any anomalies. Users may track their progress and make educated decisions regarding their health thanks to the website's convenient access to heart rate data. The system protects users' privacy and security with high-level safeguards like encryption and user authentication. In sum, the work in this project marks a major technological leap in heart rate monitoring, which has the potential to enhance health outcomes for people all around the world.

## References:

1. Reuter, A. (1986, February). Load control and load balancing in a shared database management system. In 1986 IEEE Second International Conference on Data Engineering (pp. 188-197). IEEE.
2. Rodríguez, G. E., Torres, J., & Benavides, E. (2022, April). XSS2DENT, Detecting Cross-Site Scripting Attacks (XSS) Vulnerabilities: A Case Study. In *Applied Technologies: Third International Conference, ICAT 2021, Quito, Ecuador, October 27–29, 2021, Proceedings* (pp. 365-380). Cham: Springer International Publishing.
3. Amin, M. R., & Bhowmik, T. (2022, August). Existing Vulnerability Information in Security Requirements Elicitation. In 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW) (pp. 220-225). IEEE.
4. Gamundani, A. M. (2015, May). An impact review on internet of things attacks. In 2015 international conference on emerging trends in networks and computer communications (ETNCC) (pp. 114-118). IEEE.
5. He, C. (2016, September). Research of web resources protection based on digital watermarking and digital signature. In 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS) (pp. 294-297). IEEE.
6. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.
7. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
8. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103-2115.
9. Ruiz, J. F., Harjani, R., Mana, A., Desnitsky, V., Kotenko, I., & Chechulin, A. (2012, February). A methodology for the analysis and modeling of security threats and attacks for systems of embedded components. In 2012 20th Euromicro International Conference on Parallel, Distributed and Network-based Processing (pp. 261-268). IEEE.

10. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.
11. Kapil, D., Mehra, N., Gupta, A., Maurya, S., & Sharma, A. (2021, March). Network security: threat model, attacks, and IDS using machine learning. In 2021 international conference on artificial intelligence and smart systems (ICAIS) (pp. 203-208). IEEE.
12. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE access, 7, 124379-124389.
13. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.
14. Abomhara, M., & Kjøien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.
15. Parikh, T. P., & Patel, A. R. (2017). Cyber security: Study on attack, threat, vulnerability. Int. J. Res. Mod. Eng. Emerg. Technol, 5, 1-7.
16. Ghazal, T. M., Afifi, M. A. M., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technology, 63(1s).
17. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
18. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).
19. Azman, H. K., & Kadir, K. (2019, August). Development of a Low-Power Heart Rate Monitor Device for Observation of Heart Rate Variability. In 2019 IEEE International Conference on Smart Instrumentation, Measurement and Application (ICSIMA) (pp. 1-4). IEEE.

20. Barai, A. R., Badhon, M. R. K., Zhora, F., & Rahman, M. R. (2019, December). Comparison between Noninvasive Heart Rate Monitoring Systems using GSM Module and ESP8266 Wi-Fi Module. In 2019 3rd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE) (pp. 45-48). IEEE.
21. Valsalan, P., Baomar, T. A. B., & Baabood, A. H. O. (2020). IoT based health monitoring system. *Journal of critical reviews*, 7(4), 739-743.
22. Rao, T. V. N., Sai, G. V., Reddy, P. H. V., Bandarupally, S. H., & Nikhil, C. (2021, November). SHANE–Smart HeartRate Analysis and Notification System for Emergencies. In 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 1104-1107). IEEE.
23. Hubert, R., Bánáti, A., Erdődi, L., & Fleiner, R. (2022, August). Strengthening Database Security with Capture the Flag Exercises. In 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES) (pp. 000137-000142). IEEE.
24. Churi, A. A., & Shinde, V. D. (2020, February). Alphanumeric Database Security through Digital Watermarking. In 2020 International Conference on Convergence to Digital World-Quo Vadis (ICCDW) (pp. 1-4). IEEE.