SECURED EMERGENCY HEALTHCARE MONITORING SYSTEM USING LI-FI

PROJECT PHASE – II REPORT

Submitted By

JEYA VAARSHINI S

KAVITHA P

LEKHASRI M

MADHUSHREE K

In Partial Fulfilment for the Award of the degree

DEGREE OF

BACHELOR OF ENGINEERING

In

ELECTRONICS AND COMMUNICATION ENGINEERING

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

ANNA UNIVERSITY: CHENNAI 600 025

APRIL 2025

BONAFIDE CERTIFICATE

Certified that this report "**SECURED EMERGENCY HEALTHCARE MONITORING SYSTEM USING LI-FI**" is the bonafide work of

JEYA VAARSHINI S	-	142221106062
KAVITHA P	-	142221106069
LEKHASRI M	-	142221106077
MADHUSHREE K	-	142221106080

who carried out the project work under my supervision

SIGNATURE
Dr. KOMALA JAMES
HEAD OF THE DEPARTMENT
Professor
Department of Electronics and Communication Engineering
SRM Valliammai Engineering College

SIGNATURE
Dr. N. JOTHY
SUPERVISOR
Assistant Professor
Department of Electronics and Communication Engineering
SRM Valliammai Engineering College

Submitted for viva voce held on_____at SRM Valliammai Engineering College, Kattankulathur-603 203.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

A project work of this magnitude would not have been possible without the guidance and coordination of many people. Our sincere thanks and profound sense of gratitude to our respected Founder Chairman & Chancellor **Dr. T.R. PAARIVENDHAR** Chairman **Dr. RAVI PACHAMUTHU,** Correspondent **Ms. R. HARINI** for providing us with adequate infrastructure and a congenial academic environment.

We consider it a great privilege to recur our deep sense of gratitude to our Director **Dr.B. CHIDHAMBARA RAJAN** and Principal **Dr. M. MURUGAN.** We also express our sincere gratitude and profound thanks to the Head of the Department **Dr. KOMALA JAMES** who patronized us throughout our project work. We express our profound thanks and gratefulness to our Project Coordinator **Dr. J. PREMALATHA,** Associate Professor, for her valuable guidance and suggestion, which enabled us to come out successfully with our project work.

Our heartfelt thanks to our supervisor **Dr. N. JOTHY,** Assistant Professor, for his constant support, guidance, and motivation in making this project a successful one. We express our sincere salutation to all other teaching and non- teaching staff for their valuable suggestions in this endeavor of. Finally, we dedicate this work to our parents and the Almighty who have been with us to overcome the hard times.

ABSTRACT

Healthcare systems face significant challenges with traditional wireless communication technologies like Bluetooth and Wi-Fi. Bluetooth is limited by its range and data transfer capabilities, while Wi-Fi introduces concerns regarding electromagnetic interference, which can negatively impact patients with conditions such as neurological disorders and cancers. Li-Fi technology, which uses visible light for communication, offers a promising alternative. By providing faster data transmission, enhanced security, and eliminating electromagnetic interference, Li-Fi is well-suited for safe and efficient patient health monitoring.

This work introduces an advanced patient health monitoring system utilizing Li-Fi technology to overcome the limitations of existing systems. The proposed model integrates Rivest–Shamir– Adleman (RSA) and Advanced Encryption Standard (AES) algorithms to ensure data security and confidentiality. RSA employs asymmetric encryption with public and private keys to secure communication, while AES provides symmetric encryption for efficient data protection. Together, these encryption methods create a robust framework for safeguarding sensitive patient information.

Implemented using Arduino IDE, the proposed system highlights the transformative potential of Li-Fi technology in healthcare. By addressing the challenges associated with traditional wireless communication methods and ensuring high standards of data security, this solution paves the way for safer, more reliable, and efficient patient monitoring systems, redefining the standards for healthcare communication.

Keywords- Health care, Li-Fi, Rivest-Shamir-Adleman Algorithm, Advanced Encryption Standard, Arduino IDE,

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

Symbol	Interpretation of Symbol
$A(x)$	Input Data
$B(x)$	Fixed Matrix
$P(x)$	Irreducible Polynomial
Kr	Round Key For The Current Round
$\phi(n)$	Euler's Totient Function
e	Public Key Exponent
d	Private Key Exponent
C	Recipient's Public Key
K	Recipient's Private Key

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ARDUINO IDE	Arduino Integrated Development Environment
BMP	Barometric Pressure Sensor
CSI	Channel State Information
ESP8266	Espressif Systems8266
EHR	Electronic Health Record
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of Things
LCD	Liquid Crystal Display
LED	Light Emitting Diode
Li-Fi	Light Fidelity
MAX30100	Pulse Oximeter and Heart Rate Sensor
MPU6050	Magnetic Pickup Sensor
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
SPO2	Saturation of Peripheral Oxygen
Wi-Fi	Wireless Fidelity

CHAPTER – 1

INTRODUCTION

1.1 OVERVIEW OF INITIAL IMPLEMENTATION OF LI-FI

Li-Fi technology enabled high-speed, interference-free data transmission, eliminating electromagnetic risks associated with Wi-Fi and Bluetooth in the developed patient health monitoring system. By leveraging visible light for data transfer, the system ensured secure and efficient communication, addressing concerns related to electromagnetic interference in sensitive hospital environments. Sensors were integrated to collect vital health parameters such as heart rate, temperature, and oxygen levels, with real-time data visualization allowing seamless monitoring of patient conditions. Despite the advantages of Li-Fi, certain areas require improvement to enhance system security, reliability, and efficiency.

While Li-Fi inherently provides a secure communication medium, implementing additional encryption mechanisms like RSA and AES is necessary to protect sensitive patient data from potential cyber threats. Authentication measures must be incorporated to restrict unauthorized access, ensuring only authorized personnel can interact with the system. Enhancing reliability through data validation mechanisms, error detection algorithms, and a backup storage system will help prevent data loss and transmission errors. Furthermore, integrating real-time alerts for abnormal health readings and a secured notification system for healthcare providers will improve emergency response efficiency, allowing timely medical intervention. The next implementation will focus on incorporating encryption, authentication, and advanced security algorithms to strengthen safety, enhance data confidentiality, and optimize overall system performance**.**

1.2 ROLE OF RSA AND AES

AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) play crucial roles in securing data transmission within the Li-Fi-based patient health monitoring system by ensuring confidentiality, integrity, and authentication of sensitive medical information.

- ***AES (Advanced Encryption Standard)*** is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. It is ideal for securing real-time patient data transmission because of its high-speed encryption and low computational overhead, ensuring efficient and secure communication between sensors and monitoring devices. AES protects medical data from unauthorized access while maintaining fast performance, making it suitable for continuous health monitoring.
- ***RSA (Rivest-Shamir-Adleman)*** is an asymmetric encryption algorithm, using a public key for encryption and a private key for decryption. It is used for secure key exchange and authentication, ensuring that only authorized healthcare providers can access the encrypted patient data. Since AES requires both sender and receiver to share the same key, RSA is often used to securely transmit the AES encryption key, preventing interception or unauthorized decryption.

By combining AES for fast and secure data encryption and RSA for key exchange and authentication, the system achieves a high level of data security, privacy, and protection against cyber threats while maintaining the efficiency required for real-time patient monitoring.

1.3 MOTIVATION FOR IMPLEMENTING LI-FI WITH AES AND RSA

Li-Fi enables high-speed, interference-free communication, but additional encryption is required to ensure the security and confidentiality of patient data. Implementing AES and RSA with Li-Fi enhances protection against unauthorized access and ensures reliable data transmission.

- ***Strong Data Encryption*** – AES encrypts patient health data during transmission, ensuring that even if intercepted, it remains unreadable without the correct key.
- ***Secure Key Exchange & Authentication*** – RSA enables safe transmission of encryption keys and authenticates users, allowing only authorized personnel to access patient data.

- ***Protection Against Cyber Threats*** – While Li-Fi is inherently secure against external hacking, AES and RSA provide an extra layer of security against internal threats and unauthorized access within hospital networks.
- ***Reliable & Real-Time Performance*** – AES ensures fast encryption and decryption, maintaining efficient, real-time patient monitoring without introducing delays.
- ***Prevention of Data Tampering*** – By encrypting data, AES and RSA protect against unauthorized modifications, ensuring patient vitals remain accurate and trustworthy.

1.4 LITERATURE REVIEW

[1] "Patient Health Monitoring System using ESP8266 and Arduino with IoT Platform" Jamil Abedalrahim Jamil Alsayaydeh, Mohd Faizal bin Yusof, et al. proposed a patient health monitoring system utilizing ESP8266 and Arduino with an IoT platform. This system leverages Wi-Fi technology for data transmission, making it suitable for remote health monitoring. By employing sensors to collect vital health parameters and transmitting them to a cloud-based platform,healthcare providers can monitor patients remotely. However, the reliance on Wi- Fi connectivity limits the system's applicability in areas with poor network coverage.

[2] "Li-Fi for better medical treatment" Cilla Mathew,Ansurkar, et al., investigate the application of Li-Fi technology in the healthcare sector. The study highlights the potential of Li-Fi to enable faster data transmission, reduced delays, and improved accessibility, especially in rural areas. By using Li-Fi for medical data transfer, healthcare providers can access and analyze patient information more efficiently, leading to better treatment outcomes. However, Li-Fi's limited range, dependence on light sources, and potential installation costs are factors that need to be considered for widespread adoption in healthcare settings.

[3] "Contactless WIFI Sensing and Monitoring for Future Healthcare," by. Dr. G. Kiranmaye, Thodeti Rakesh, Surva Tilak, and A.K. Puchiarla, explores the potential of Wi-Fi technology for contactless health monitoring. By analyzing Channel State

Information (CSI), advanced signal processing techniques, and machine learning algorithms, the researchers propose a system that can detect significant health events like falls and sleep disturbances without the need for wearable devices or cameras.

[4] “Complete Data Transmission using Li-Fi Technology with Visible Light Communication,” by Amita Pandit Sonawane and Janhavi Sanjay Pradhan investigates the use of Li-Fi technology for transmitting various forms of data, including audio, text, and images. By modulating the intensity of visible light, Li- Fi can potentially offer high data rates and secure communication.

[5] “A Comparative Study and Analysis on Li-Fi and Wi-Fi” Ashmita Shetty's research compares Li-Fi and Wi-Fi technologies, highlighting the potential of Li- Fi for applications like healthcare, where electromagnetic radiation is a concern. The study suggests that Li-Fi can be implemented in environments like operation theaters, where traditional Wi-Fi may not be suitable due to its potential interference with medical equipment. However, the reliability of Li-Fi-based communication can be affected by factors like ambient light conditions and obstacles.

[6] “IoT-Based Health Monitoring System using Blynk App” by Peddapuram Saarika, Nemmai Sai Teja Verma, and Meduri Ram Gopal Chowdary presents a real-time health monitoring system using IoT. Sensors collect data on heart rate, temperature, and oxygen levels, transmitting it via a microcontroller (e.g., Arduino or ESP8266) to a cloud platform. The Blynk app enables remote access and visualization for patients and healthcare providers. The system ensures continuous monitoring, timely interventions, and improved patient care, detailing hardware, software, sensor integration, and app functionality.

[7] “RSA-AES Hybrid Encryption: Combining the Strengths of Two Powerful Algorithms for Enhanced Security” by Venkata Mahesh Babu Batta and Dr.L.K. Suresh Kumar proposes a hybrid encryption model that combines RSA's secure key exchange with AES's efficient data encryption. By using RSA to securely transmit AES keys and AES to encrypt the actual data, the approach mitigates the

weaknesses of each algorithm when used alone, such as RSA's computational inefficiency and AES's key distribution challenges. This hybrid system offers enhanced security and performance, making it suitable for applications like secure communications and data storage. The paper discusses the framework, implementation, and benefits of this model.

[8] “A Review: RSA and AES Algorithm” by Ashutosh Gupta and Sheetal Kaushik analyzes RSA (asymmetric) and AES (symmetric) encryption. RSA excels in secure key exchange and digital signatures but is slower for large data, while AES is efficient for bulk encryption but faces key distribution challenges. The paper compares their strengths, weaknesses, and applications.

[9] “Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing” by Venkata Mahesh Babu Batta and Dr. L.K. Suresh Kumar explores the effectiveness of AES and RSA in cloud security. AES, a symmetric algorithm, is valued for its speed and efficiency in encrypting large datasets, making it ideal for securing data at rest and in transit. RSA, an asymmetric algorithm, ensures secure key exchange and digital signatures but is slower and less efficient for bulk encryption. The paper suggests a hybrid approach that leverages the strengths of both algorithms to improve security, scalability, and performance in cloud computing.

[10] “Implementation of Digital Signature Using AES and RSA Algorithms as a Security in Disposition System of Letter” by Vishnu Wendanto explores a hybrid security approach for digital letter disposition. RSA ensures authenticity and integrity through digital signatures, while AES encrypts letter content for confidentiality. The study demonstrates that combining these algorithms enhances secure communication and document handling, highlighting their practical application in digital security.

1.5 SUMMARY

The introduction discusses the implementation of Li-Fi technology for secure and efficient patient health monitoring in healthcare settings. Traditional wireless

technologies such as Wi-Fi and Bluetooth, while commonly used, have notable drawbacks in sensitive environments like hospitals. These methods can cause electromagnetic interference, which may disrupt medical equipment, and they also carry inherent security vulnerabilities, risking the confidentiality of patient data. Li-Fi, which uses visible light for data transmission, offers a solution by eliminating electromagnetic interference and providing faster, more secure communication.

However, despite the advantages of Li-Fi, further security measures are necessary to safeguard sensitive medical data during transmission. To enhance security, AES and RSA encryption algorithms are integrated into the system. AES ensures that patient data is encrypted in real time, maintaining both the privacy and integrity of the information while allowing for high-speed data transfer. RSA, on the other hand, provides an additional layer of security through secure key exchange and authentication, ensuring that only authorized personnel can access the data. The combination of Li-Fi, AES, and RSA creates a robust, interference- free, and highly secure communication system, addressing the key challenges of data security, privacy, and reliability in healthcare environments.

CHAPTER –2

EXISTING SYSTEM

2.1 OVERVIEW OF THE EXISTING SYSTEM

Emergency healthcare,prompt patient monitoring is essential. Conventional wireless communication systems like Wi-Fi encounter issues such as interference, bandwidth, restrictions, and security weaknesses, which could threaten patient care. The goal of this project is to create a secure healthcare monitoring system that employs Li-Fi (Light Fidelity) technology, which transmits data through visible light, providing fast and secure data transfer. The system will incorporate wearable sensors to continuously track vital signs like heart rate and oxygen levels combined with Li-Fi transmitters for immediate data transmission to healthcare professionals. One major benefit of Li-Fi is its improved security, data transfer is limited to the lit space, greatly lowering the risk of unauthorized access. To enhance security, the system will apply advanced encryption protocols and role-based access controls. The user interface will include a user-friendly dashboard enabling healthcare professionals to oversee real time patient data and get notified of critical changes, as well as data visualization tools to monitor health trends over time. Although the system provides many advantages—like better patient outcomes and increased security—it also poses challenges, such as the requirement for infrastructure improvements and user acceptance. To sum up, the 'Secured Emergency Healthcare Monitoring System Using Li-Fi' seeks to transform emergency patient monitoring, improving responsiveness and establishing a new benchmark for healthcare services.

2.2 TECHNIQUES IMPLEMENTED

2.2.1 Algorithm

The algorithm for the "Secured Emergency Healthcare Monitoring System Using Li-Fi" is designed to provide seamless and efficient patient monitoring in emergency situations. It begins with the initialization of all hardware components, including the Arduino Uno, Raspberry Pico W, and essential sensors such as the

MPU-6050, BMP, and MAX30100. During this phase, proper connections are established to ensure that all devices can communicate effectively.15

Once the hardware is set up, the system configures the sensors to continuously collect vital health data. The MPU-6050 monitors motion, while the BMP sensor measures temperature and atmospheric pressure. The MAX30100 is responsible for tracking heart rate and blood oxygen levels. This real-time data collection is crucial for assessing a patient's condition accurately.

After gathering the necessary data, it is formatted appropriately for transmission. The Arduino Uno modulates this formatted data into light signals using a Li-Fi LED transmitter. These modulated light signals are sent to the Raspberry Pico W, which acts as the receiver. The Pico W is equipped with a solar panel that captures the incoming light signals, allowing for energy-efficient operation.

Once the Raspberry Pico W receives the signals, it demodulates them back into digital data for processing. The system then extracts vital health metrics from this data, which are displayed on an LCD screen for real-time monitoring by healthcare professionals. The LCD provides immediate visual feedback, making it easier for medical staff to assess patient conditions quickly.

In addition, the system is designed to trigger alerts if any critical health parameters fall outside predefined thresholds, ensuring timely medical intervention. The entire process—data collection, transmission, reception, and display—repeats continuously, providing efficient and responsive monitoring in emergency healthcare scenarios. This structured approach enhances patient care and facilitates quick decision making.

2.2.2 Flowchart of the Proposed System

The Fig. 2.1gives the flowchart of how the system works. The project begins by powering up and initializing the essential components,including the Arduino Uno, Raspberry Pico W, sensors, and Li-Fi transmitters, ensuring each element is operational and ready for communication. During the hardware setup phase,

components like the MPU-6050, BMP sensor, and MAX30100 are connected to the Arduino Uno, while the Li-Fi LED transmitter and solar panel receiver are also arranged. Following this, initialization configures each sensor and module to start collecting vital signs, with the Raspberry Pico W set to receive data.

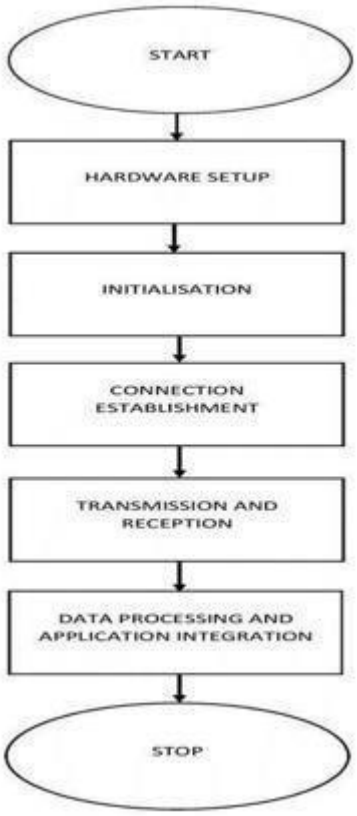

Fig. 2.1 Flowchart of the Existing System

Once initialized, the system establishes a communication link between the Arduino Uno and Raspberry Pico W. The Arduino modulates data into light signals, which are transmitted via the Li-Fi LED and received by the Pico W's solar panel. This captured data is processed for display, typically on an LCD, for real-time health monitoring. After the monitoring cycle, the system enters a standby mode, allowing components to remain ready for the next cycle while conserving energy. This ensures the system is operationally efficient, supporting quick, real-time responses in emergency healthcare scenarios.

2.3 SOFTWARE IMPLEMENTED

2.3.1 Arduino IDE

In the "Secured Emergency Healthcare Monitoring System Using LiFi," the

Arduino Integrated Development Environment (IDE) plays a crucial role in facilitating the development and deployment of the system's components. The Arduino IDE is a user-friendly platform that allows developers to write, compile, and upload code to Arduino boards, making it ideal for rapid prototyping in embedded systems. In this project, various Arduino-compatible microcontrollers are used to interface with wearable sensors that monitor vital signs, such as heart rate and temperature.Using the Arduino IDE, developers can easily program these microcontrollers to collect data from the sensors and process it for transmission. The IDE supports a variety of libraries that simplify sensor integration, enabling straightforward communication between the sensors and the microcontroller. For instance, libraries specific to each type of sensor allow for efficient data retrieval and manipulation, ensuring that real-time vital sign data is accurately captured and formatted for transmission via Li-Fi. The Fig. 2.2 is given below representing the Arduino Program used for transmission.

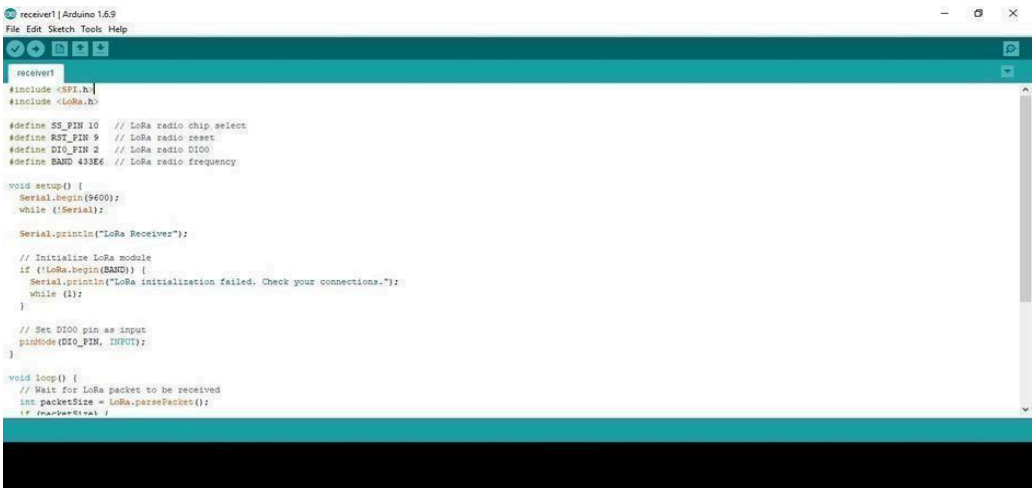

Fig. 2.2 Arduino Program used for Transmission

Additionally, the Arduino IDE allows for the implementation of algorithms for data encryption, such as AES. By integrating cryptographic libraries, developers can program the microcontroller to encrypt the collected patient data before it is sent to the Li-Fi transmitter, ensuring that sensitive information remains secure during transmission. This capability is essential in maintaining patient confidentiality, especially in emergency scenarios.Furthermore, the IDE provides a

straightforward debugging environment, enabling developers to test and troubleshoot their code efficiently.

This feature is particularly beneficial in a project that requires reliable performance, as it allows for quick iterations and refinements. Overall, the Arduino IDE serves as a foundational tool in this project, enabling the seamless integration of hardware and software components to create a cohesive and effective healthcare monitoring system. Through its versatility and ease of use, the Arduino IDE significantly enhances the development process and contributes to the overall success of the project.

2.4 HARDWARE COMPONENTS

2.4.1 Arduino Uno as Transmitter

Fig. 2.3 Arduino Uno

The Fig. 2.3 showing the model of Arduino Uno used as a transmitter. In this project, the Arduino Uno serves as the transmitter, playing a vital role in collecting and transmitting data from various sensors to the receiving unit. It is programmed to interface with sensors like the MPU-6050, BMP sensor, and MAX30100, gathering vital health parameters such as motion, temperature, pressure, heart rate, and oxygen saturation. The Arduino Uno's simple and efficient architecture allows for quick data processing and real-time communication. Once the data is collected, the Arduino encodes it and transmits it using a Li-Fi LED transmitter. This LED modulates the light signals to convey the information, allowing for secure and fast data transmission. The Arduino IDE is utilized for coding, enabling developers to

integrate sensor readings and control the LED, ensuring seamless operation. Its compact size and ease of use make the Arduino Uno an excellent choice for embedded applications in emergency healthcare monitoring.

2.4.2 Raspberry Pico W as Receiver

The Fig. 2.4 showing the model of Raspberry Pico used as Receiver. The Raspberry Pico W functions as the receiver in the healthcare monitoring system, designed to capture the Li-Fi signals transmitted by the Arduino Uno.

Fig. 2.4 Raspberry Pico W

Equipped with Wi-Fi capabilities, the Pico W is programmed to demodulate the light signals from the Li-Fi LED and convert them back into digital data. This data includes vital health parameters collected from the sensors. The Pico W processes this incoming information and prepares it for display. It can also be connected to an LCD screen, allowing healthcare professionals to view the real-time data conveniently. The use of the Raspberry Pico W enhances the overall system by enabling wireless communication and data processing, which is essential for quick decision-making in emergency situations. Its low power consumption and compact design make it suitable for portable applications, ensuring that the system remains efficient and effective in monitoring patient health.

2.4.3 MPU-6050 Sensor at Transmitter

The Fig. 2.5 showing the model of MPU Series Sensor used .The MPU6050 sensor is a crucial component of the emergency healthcare monitoring system, responsible for providing real-time data on motion and orientation.

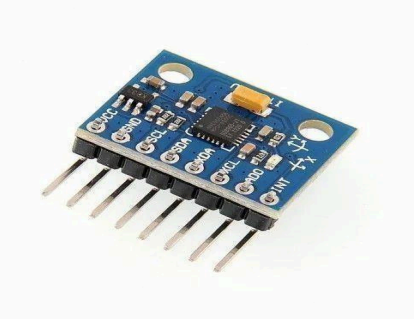

Fig. 2.5 MPU-6050 Sensor

This sensor integrates a three-axis gyroscope and a three-axis accelerometer, enabling it to capture dynamic changes in position and movement. In the context of this project, the MPU-6050 can help monitor a patient's activity level, detect falls, or assess mobility, which is particularly valuable in emergency situations. The sensor communicates with the Arduino Uno via I2C, allowing for easy integration and data retrieval. By continuously sending motion data, the MPU- 6050 enhances the system's ability to provide comprehensive health assessments, aiding healthcare professionals in making informed decisions. Its compact size and high accuracy make it ideal for wearable applications, ensuring that critical motion-related information is reliably captured and transmitted.

2.4.4 BMP Sensor at Transmitter

The Fig. 2.6 showing the model of BMP Sensor used .The BMP sensor is integral to the healthcare monitoring system, providing essential environmental data such as temperature and atmospheric pressure. By measuring these parameters, the BMP sensor helps assess the conditions surrounding the patient, which can be crucial in emergency healthcare settings.

Fig. 2.6 BMP Sensor

For example, variations in temperature may indicate changes in a patient's condition or the effectiveness of environmental controls in a medical facility. The BMP sensor interfaces with the Arduino Uno, allowing for real-time data collection and processing. The information gathered can be transmitted via Li-Fi to the receiving unit, enabling healthcare providers to monitor not only the patient's vital signs but also the ambient conditions affecting their health. Its compact design and precision make it suitable for integration into portable monitoring devices, enhancing the overall functionality of the system.

2.4.5 MAX30100 Sensor at Transmitter

The Fig. 2.7 showing the model of MAX Series Sensor used .The MAX30100 sensor is a key component in the emergency healthcare monitoring system, specifically designed for measuring heart rate and blood oxygen levels (SpO2).

Fig. 2.7 MAX30100 Sensor

This optical sensor utilizes advanced photo detector technology to provide accurate and real-time measurements, which are critical in assessing a patient's cardiovascular health. The MAX30100 communicates with the Arduino Uno, enabling seamless integration into the monitoring system. When the sensor collects data, it transmits the readings to the Arduino, which then processes and prepares the information for transmission via Li-Fi. The inclusion of the MAX30100 sensor allows healthcare professionals to monitor vital signs efficiently, providing insights into a patient's condition in emergency scenarios. Its compact form factor and low power consumption make it an ideal choice for wearable health devices, ensuring continuous and reliable monitoring of essential health metrics

2.4.6 Li-Fi Transmitter as Torch

The torch modulates its light intensity to transmit data wirelessly, encoding the information collected from various sensors into light signals.This form of communication is particularly advantageous in emergency healthcare settings, as it enables high-speed data transfer without interference from radio frequencies.

The torch is controlled to ensure proper modulation, allowing for accurate and reliable signal transmission. By using visible light for communication, the Li-Fi transmitter enhances security, as the signals are confined to the illuminated area and are less susceptible to eavesdropping.

2.4.7 Li-Fi Receiver as Solar Panel

This innovative approach allows the solar panel to act as both a receiver of data transmitted by the Li-Fi LED and a power source for the system.When the solar panel detects the modulated light signals, it demodulates them to retrieve the encoded data, which includes vital health information transmitted from the Arduino Uno.This dual functionality is especially advantageous in emergency healthcare applications, as it enables continuous data transmission without requiring an additional power source.

By utilizing a solar panel, the system can remain operational in various environments, enhancing its portability and reliability. This combination of data reception and energy harvesting contributes to the overall sustainability of the healthcare monitoring system, making it an effective solution for real-time patient monitoring in emergencies.

2.4.8 LCD Display at Receiver

Connected to the Raspberry Pico W, the LCD presents vital health metrics collected from various sensors, such as heart rate, oxygen saturation, temperature, and motion data. This visual representation of patient information allows for quick assessment and informed decision making in emergency situations. The display can be programmed to show alerts or critical updates, enhancing situational awareness for healthcare providers. Its compact size and ease of integration make the LCD an ideal choice for portable monitoring systems, ensuring that essential information is

readily available without overwhelming the user. By facilitating immediate access to real-time data, the LCD contributes significantly to the overall effectiveness of the monitoring system, empowering healthcare professionals to respond swiftly to changes in a patient's condition.

2.5 BLOCK DIAGRAM

2.5.1 Transmitter Side

The transmitter side of the "Secured Emergency Healthcare Monitoring System using Li-Fi" is designed to collect and transmit vital patient data using light-based communication. It is powered by a regulated power supply that feeds into an Arduino Uno microcontroller, which acts as the central control unit. Three key sensors—BMP sensor (for temperature and pressure), MAX30100 (for heart rate and SpO2), and MPU-6050 (for motion and fall detection)—are connected to the Arduino to continuously monitor the patient's health status. The microcontroller processes this data and sends it simultaneously to an LCD display for real-time local monitoring and to a Li-Fi transmitter module, which transmits the data wirelessly using visible light. Li-Fi ensures fast and secure data transfer, minimizing electromagnetic interference and enhancing privacy. This setup is ideal for emergency and remote healthcare environments, where accurate and quick transmission of patient vitals is critical. The system supports encryption for data confidentiality during transmission.

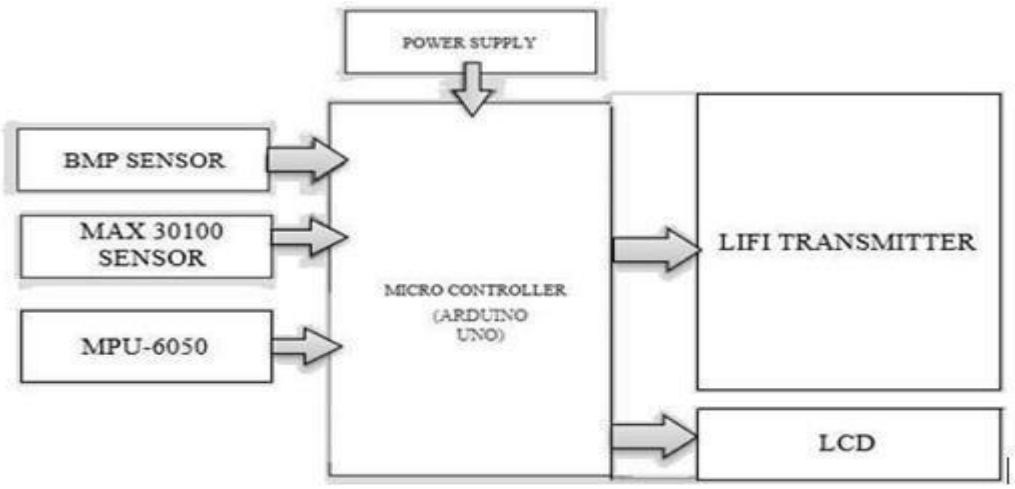

Fig. 2.11 Block diagram of Transmitter side

2.5.2 Receiver Side

The receiver side of the "Secured Emergency Healthcare Monitoring System using Li-Fi" is responsible for receiving and displaying patient data transmitted through light signals. A stable power supply energizes the microcontroller, which serves as the central processing unit. The Li-Fi receiver captures encoded light signals transmitted from the transmitter side, which include vital signs such as heart rate, SpO2, temperature, and movement data. The microcontroller decodes this data, and if encryption techniques like AES or RSA are used, it performs decryption to retrieve the original values securely. The processed data is then displayed on an LCD screen for easy monitoring by healthcare professionals. Additionally, the microcontroller is connected to an IoT module, allowing remote access and cloud-based storage of health data for real- time patient tracking and analysis. This setup ensures secure, efficient, and wireless transmission of patient health parameters, making it highly suitable for emergency and telemedicine applications in modern healthcare systems.

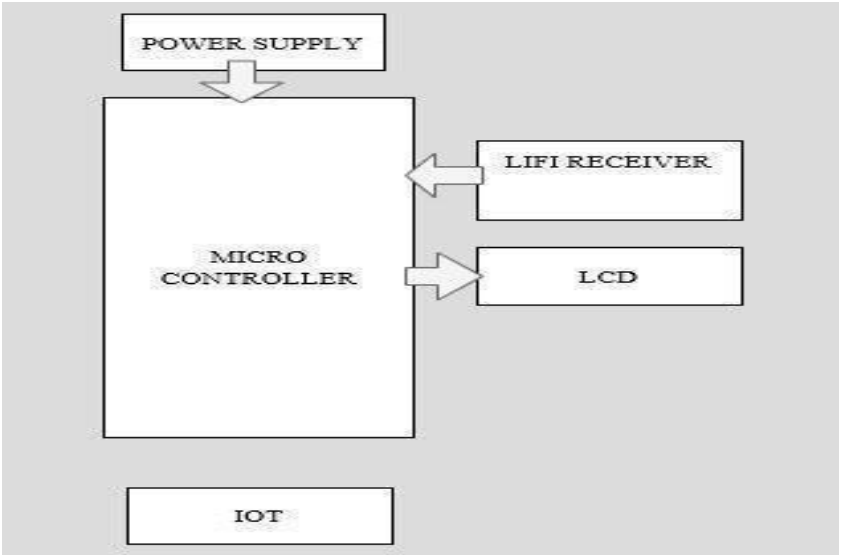

Fig. 2.12 Block diagram of Receiver side

2.6 METHODOLOGY

The methodology for the "Secured Emergency Healthcare Monitoring System Using Li-Fi" encompasses a systematic approach aimed at developing an effective and reliable monitoring solution. It begins with a comprehensive literature review to examine existing healthcare monitoring systems and Li-Fi technology, identifying gaps and defining the specific requirements for the project. This phase ensures a clear understanding of the needs that the system must address, including the selection of appropriate sensors and communication protocols.Following this, the system design phase involves creating a detailed architecture that outlines the interaction between various components, such as the sensors, microcontrollers, Li-Fi transmitters and receivers, and display units. Detailed schematics are developed to guide the hardware setup, ensuring proper wiring and component specifications.

Once the design is finalized, the next step is hardware selection and assembly. Suitable sensors like the MPU-6050, BMP, and MAX30100 are chosen based on their functionality and compatibility with the Arduino Uno and Raspberry Pico. After assembling the components, the software development phase begins, utilizing the Arduino IDE to write code for data collection, formatting, and transmission via the Li-Fi LED.

Additionally, software for the Raspberry Pico W is developed to receive and process the incoming data, displaying the results on an LCD.Security protocols are integrated to ensure that sensitive health information remains confidential during transmission. Rigorous testing follows, where each component is evaluated individually before system-level testing to verify the seamless operation of all parts. After deployment in a controlled environment, the system’s performance is monitored, and user feedback is collected for further improvements. Finally, comprehensive documentation captures the entire process, including configurations, testing results, and recommendations for future enhancements, ensuring a robust foundation for ongoing development in emergency healthcare monitoring

2.7 CHALLENGES WITH INITIAL IMPLEMENTATION

2.7.1 Security Risks & Unauthorized Access

One of the biggest challenges in using LiFi for healthcare data transmission is the risk of unauthorized access. While LiFi operates within a limited optical range, an attacker within that range could still intercept signals and gain access to sensitive medical data. Unlike traditional WiFi, which can be encrypted and secured across a broader range, LiFi's direct line-of-sight transmission makes it vulnerable to breaches if proper access controls are not in place. This is particularly concerning in hospital environments where patient confidentiality is critical.

2.7.2 Authentication & Data Integrity

Ensuring that transmitted data is authentic and unaltered is another major challenge in LiFi-based healthcare communication. Medical devices such as glucose monitors, heart rate sensors, and wearable health trackers constantly send real-time data that must remain accurate and reliable. If a malicious actor injects false data into the system, it could lead to incorrect diagnoses and improper treatment decisions. Attackers may also attempt to impersonate legitimate medical devices to manipulate records or disrupt operations. Without strong authentication and verification mechanisms, it becomes difficult to confirm that the received data truly originates from a trusted source and has not been altered in transit.

2.7.3 Man-in-the-Middle (MITM) Attacks

Although LiFi is inherently more secure than traditional RF-based communication due to its limited range, it is not immune to Man-in-the-Middle (MITM) attacks. If an attacker manages to position a rogue receiver or transmitter within the optical communication path, they can intercept and alter data before passing it on to the intended recipient. In a healthcare setting, this could mean modifying electronic health records (EHRs), injecting false alarms, or manipulating vital signs that doctors rely on for decision-making. Such attacks could lead to delays in treatment, incorrect medical procedures, or even life- threatening

consequences.

2.7.4 Data Tampering and Modification

One of the most severe risks in LiFi-based healthcare transmission is data tampering. Any unauthorized modification of health sensor data could lead to dangerous medical outcomes. For example, if a pacemaker receives altered heart rate readings, it might administer incorrect electrical impulses, potentially endangering the patient. Similarly, if an insulin pump receives manipulated glucose level data, it could dispense an incorrect dosage, leading to serious health complications. Detecting and preventing data tampering is essential to ensure patient safety and accurate medical interventions.

2.7.5 Key Exchange and Secure Communication

LiFi-based communication relies on encryption to secure patient data, but key exchange and management present significant challenges. If an encryption key falls into the wrong hands, attackers could decrypt confidential medical data, exposing it to unauthorized entities. In a hospital setting, where multiple medical devices and systems need to communicate securely, ensuring a secure and efficient key distribution process is critical. If the key exchange process is not properly managed, the entire security framework can be compromised, leading to potential data breaches.

2.7.6 Regulatory Compliance and Data Privacy

Medical data is highly sensitive and must comply with strict regulatory requirements such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). These regulations mandate that patient information must be protected from unauthorized access, tampering, and data breaches. Any security failure in a LiFi-based healthcare system could lead to legal consequences, financial penalties, and loss of patient trust. Ensuring that LiFi-based communication adheres to these privacy laws is essential for its successful adoption in healthcare institutions.

2.8 SUMMARY

The proposed Patient Health Monitoring System leverages the power of IoT technology to remotely monitor vital health parameters. By integrating sensors with an Arduino microcontroller and an ESP8266 Wi-Fi module, the system enables real-time data collection and transmission to an IoT platform. This platform facilitates remote monitoring, data visualization, and timely alerts for healthcare proxy.

CHAPTER – 3

PROPOSED SYSTEM

3.1 OVERVIEW

With the further implementation, we enhance the security of health-based sensor data transmitted via LiFi by integrating AES and RSA encryption and decryption using Python, ensuring confidentiality and integrity. The process involves encrypting sensor data using AES for secure transmission, while RSA is used for key exchange to prevent unauthorized access. To evaluate the improvement in security, we employ the NIST statistical test suite, which analyzes the randomness and security strength of the data before and after encryption. By comparing the results, we demonstrate how implementing AES and RSA significantly enhances data protection, making it resistant to potential cyber threats, tampering, and unauthorized interception in a healthcare environment.

3.2 KEY TECHNOLOGIES IMPLEMENTED

3.2.1 Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard) is a symmetric key encryption algorithm widely used for securing data due to its high speed, strong encryption, and low computational overhead. It operates on fixed block sizes (128-bit) and supports key lengths of 128, 192, or 256 bits, making it highly resistant to brute force attacks. AES encrypts data through a series of transformations, including substitutions, permutations, mixing, and key expansion, ensuring that the original information becomes unreadable without the correct decryption key.In our LiFi-based healthcare data transmission system, AES is employed to secure real-time sensor data before transmission. The process begins with the conversion of raw health data (e.g., heart rate, glucose levels, temperature readings) into an encrypted format using an AES key. This ensures that even if the data is intercepted, it remains unreadable without the correct decryption key. At the receiving end, the encrypted data is decrypted using the same AES key, restoring

the original information for authorized use. The advantage of AES in this scenario is its fast encryption and decryption speeds, making it ideal for handling continuous, real-time medical data without introducing significant delays. By integrating AES, we ensure that patient information remains confidential, tamper-proof, and protected against unauthorized access during LiFi-based communication.The Fig. 3.1 shown below is the structure flow of the AES Algorithm.

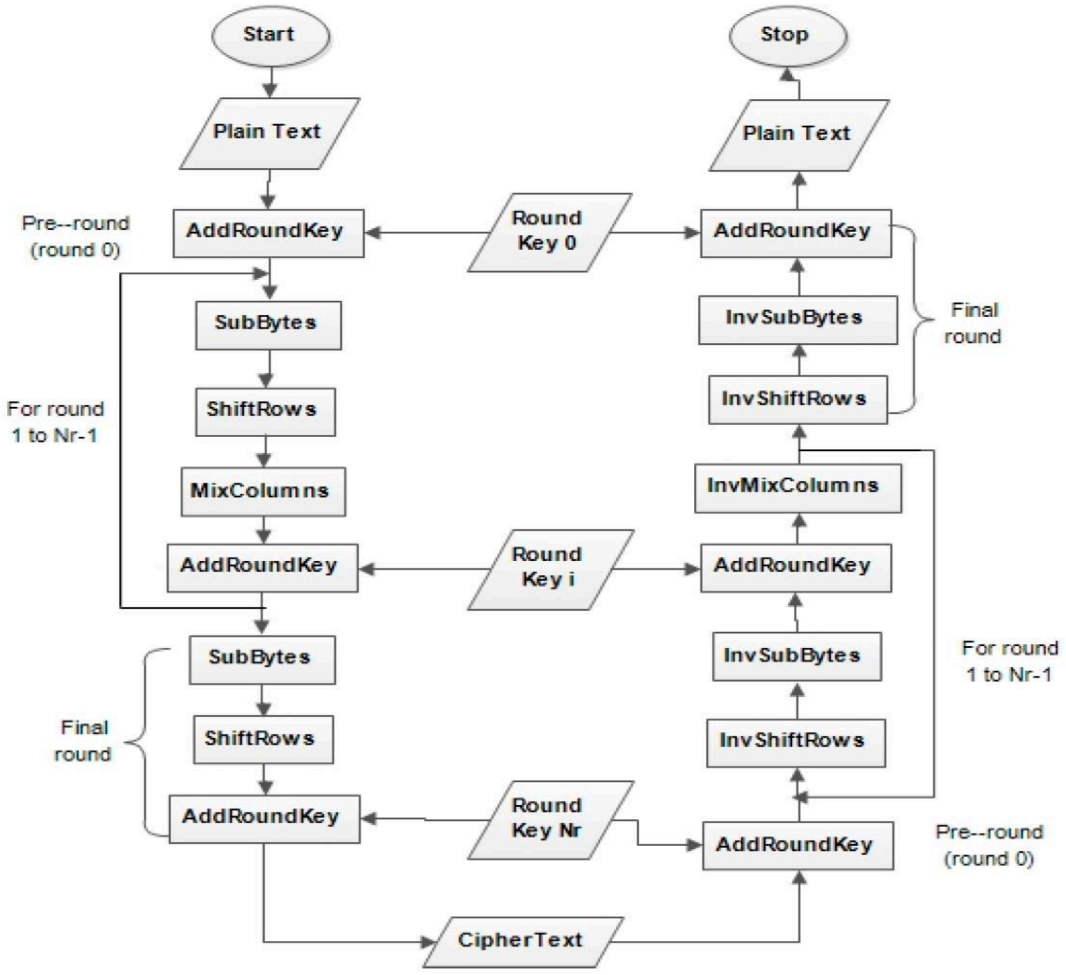

Fig. 3.1 Structure of the Advanced Encryption Standard (AES) Algorithm

3.2.2 RSA (Rivest-Shamir-Adleman)

RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm that uses public key for encryption and a private key for decryption, making it ideal for secure key exchange and authentication. It relies on the mathematical complexity of prime factorization, ensuring that decrypting data without the private key is computationally infeasible. Unlike symmetric encryption, where the same key is

used for both encryption and decryption, RSA enhances security by ensuring that only the intended recipient, possessing the private key, can decrypt the information.

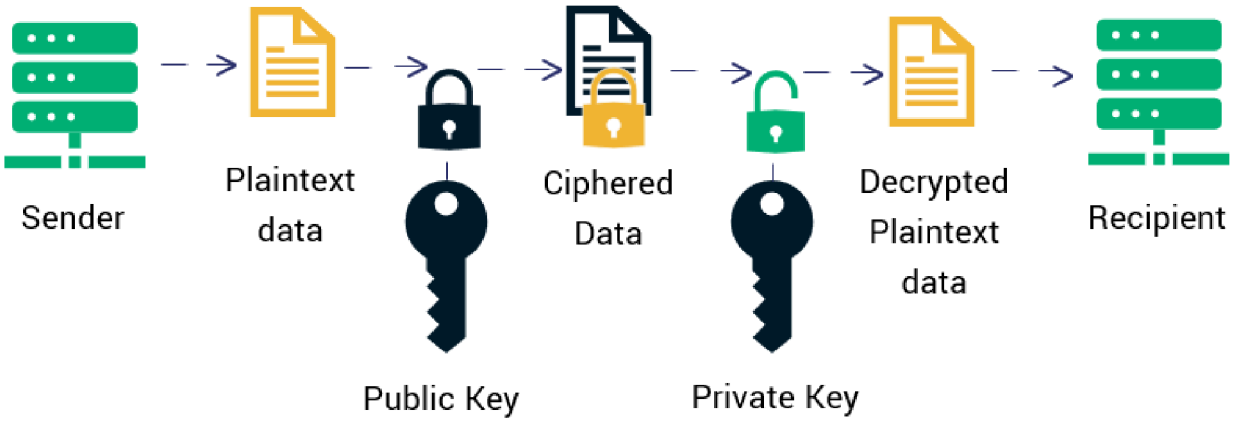

Fig. 3.2 RSA Encryption Working

The Fig. 3.2 shown above is the RSA algorithm structure flow.In our LiFi based healthcare data transmission system, RSA is primarily used for secure key exchange, ensuring that only authorized receivers can decrypt the AESencrypted sensor data. Before transmission, the AES encryption key is encrypted using the receiver's public RSA key, making it inaccessible to unauthorized entities. Upon receiving the data, the intended recipient uses their private RSA key to decrypt and retrieve the AES key, which is then used to decrypt the actual sensor data. This dual-layer approach prevents man- in-the-middle attacks, unauthorized key interception, and tampering, ensuring that healthcare data remains confidential and accessible only to authorized medical personnel. By integrating RSA, we add an extra layer of security, strengthening data integrity and authentication in LiFi communication.

3.2.2 Use of Python

Python plays a pivotal role in multiple aspects of the system. It is primarily used to interface with sensors connected to the Raspberry Pi Pico W, collect real-time patient data (such as temperature, heart rate, or SpO_2), and process that data before transmission. Python scripts handle data formatting and trigger

emergency alerts when abnormal readings are detected. Moreover, Python enables smooth integration with the Li-Fi module for secure and high-speed data transmission between patient nodes and healthcare monitoring stations. Its simplicity and versatility make it ideal for real-time data processing and handling communication protocols required in this healthcare setup.

Additionally, Python is utilized to implement AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) encryption algorithms, ensuring data security during transmission. Sensitive medical data is first encrypted using AES for fast and secure symmetric encryption, while RSA is used to encrypt the AES key itself, providing an extra layer of protection using public-key cryptography. Python's powerful cryptographic libraries like pycryptodome and cryptography simplify the implementation of these algorithms, making the encryption and decryption processes efficient and reliable. This dual-layer encryption strategy, implemented in Python, ensures that patient data remains secure and confidential even during wireless transmission through Li-Fi channels.

3.3 NIST (National Institute of Standards and Technology) Statistical Test Suite

The NIST (National Institute of Standards and Technology) statistical test suite is a collection of tests used to evaluate the randomness and security strength of encrypted data. In cryptographic systems, high randomness ensures that encrypted data is resistant to pattern recognition, cryptanalysis, and brute-force attacks. By applying NIST tests, we can quantify the security improvement introduced by encryption techniques like AES and RSA, ensuring that the transmitted healthcare data remains protected from vulnerabilities.

In our LiFi-based healthcare data transmission system, the NIST test suite is used to analyze the randomness of the data before and after encryption. Initially, the raw sensor data is tested to observe any predictable patterns that could make it susceptible to attacks. After encryption with AES and RSA, the encrypted data is

subjected to the same NIST tests, measuring improvements in entropy, uniformity, and statistical independence. By comparing the results, we demonstrate how encryption enhances data security, making it more resistant to unauthorized decryption and tampering. This analysis validates the effectiveness of AES and RSA in securing LiFi-transmitted healthcare data, ensuring confidentiality and integrity in medical communications.

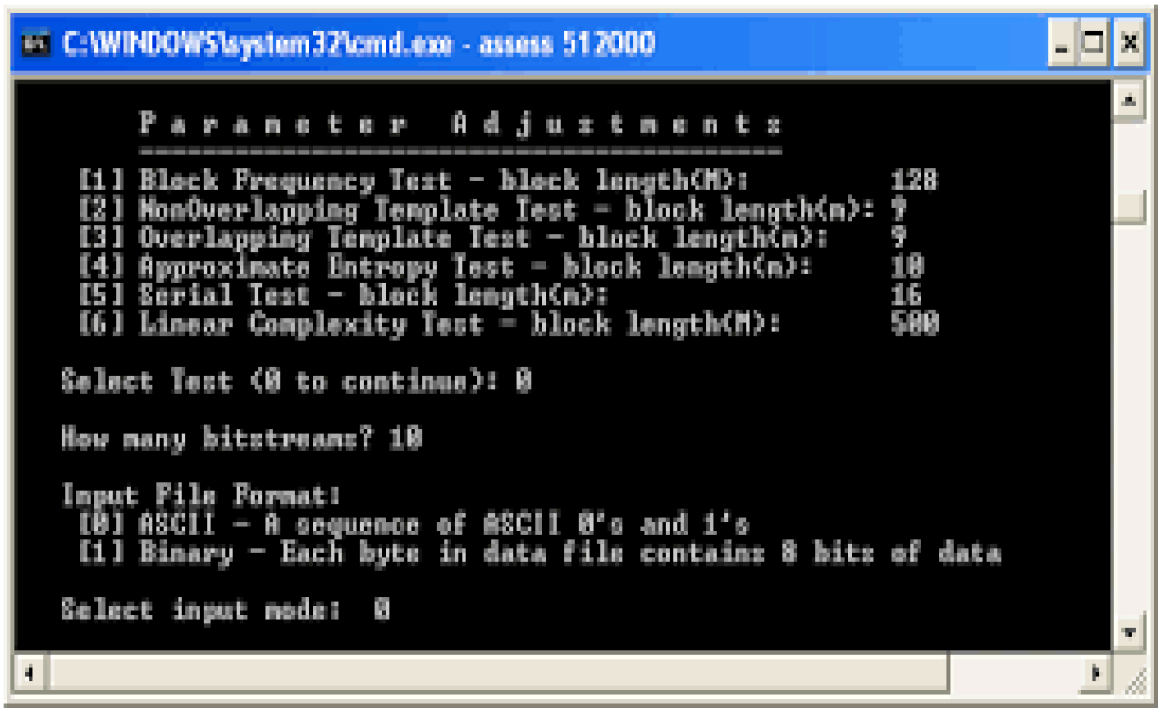

Fig. 3.3 NIST Statistical Test Suite

3.3.1 Working of NIST

The NIST Statistical Test Suite is used to evaluate the randomness and security strength of encrypted data transmitted through Li-Fi. Since AES and RSA encryption transform plaintext medical data into ciphertext, NIST tests analyze whether the encrypted output exhibits true randomness, ensuring it cannot be predicted or broken by attackers.

3.3.2 Use of NIST

- ***Evaluates Encryption Strength*** – Ensures AES and RSA provide highly randomized output, making encrypted patient data resistant to decryption attempts.

- ***Detects Predictable Patterns*** – Identifies any weaknesses in encryption where patterns could be exploited for attacks.
- ***Validates Data Security Improvement*** – Compares encryption results before and after implementation, proving enhanced security in Li-Fi transmissions.
- ***Ensures Compliance with Standards*** – Aligns encryption techniques with international cybersecurity benchmarks, making the system robust and industry-ready.
- ***Optimizes Encryption Performance*** – Helps fine-tune AES key sizes and RSA configurations, balancing security with efficient real-time transmission in healthcare environments.

3.4 METHODOLOGY

The security of the system is further evaluated using the NIST statistical test suite to demonstrate improvements in data protection. The entire process is divided into three key phases: data encryption and transmission, secure key exchange, and security analysis.

3.4.1 Data Encryption and Transmission Over Li-Fi (AES Encryption)

The process begins with real-time health sensor data collection, where medical sensors measure vital parameters like heart rate, temperature, and oxygen levels. Since transmitting raw sensor data over LiFi can lead to security risks such as interception and tampering, the data is first encrypted using AES (Advanced Encryption Standard).

AES operates on 128-bit blocks of plaintext and transforms them using substitution, permutation, and key mixing through multiple rounds.

Algorithm: AES and RSA for Secure Data Transmission

1. Key Expansion: Generates multiple round keys from the original key.

- ***Initial Round:*** $S = PK_0$ -------- (3.1)
  where S is the initial state, P is the plaintext, and K_0 is the initial round key
- ***Main Rounds (for AES-128, 10 rounds):*** SubBytes is a non-linear byte substitution process that uses an S-Box .ShiftRows is a transposition step where two are shifted cyclically. MixColumns is a linear transformation that mixes data within columns using matrix multiplication.

  $$C(x) = A(x)B(x) \bmod P(x) \quad \text{-------- (3.2)}$$

  where A(x) is the input data, B(x) is a fixed matrix, and P(x) is an irreducible polynomial.

- ***AddRoundKey:***The round key is XORed with the state: $S' = SKr$ --------(3.3)
  where Kr is the round key for the current round.
- ***Final Round (Without MixColumns):*** SubBytes → ShiftRows → AddRoundKey

  The encrypted data is then transmitted over LiFi. Even if intercepted, it remains unreadable without the correct decryption key.

2. Secure Key Exchange Using RSA: Since AES uses a symmetric key, both the sender and receiver need the same key for decryption. To prevent key exposure, we use RSA (Rivest-Shamir-Adleman), an asymmetric encryption technique.

- RSA Key Generation: Select two large prime numbers p and q and Compute the modulus: $n = p \times q$ -------- (3.4)
- Compute Euler's totient function: $\phi(n) = (p-1) \times (q-1)$ -------- (3.5)
- Choose a public key exponent e, where $1<e<\phi(n)$ and $\gcd(e,\phi(n))=1$
- Compute the private key exponent d, the modular inverse of e: $d \equiv e^{-1} \bmod \phi(n)$

- **R**SA Encryption and Decryption: The AES key K is encrypted using the recipient's public key (e,n): C = K'e mod n -------- (3.6)
  The receiver retrieves the AES key using their private key d:
  K = C'^{t} mod n ------- (3.7)
- After decrypting the AES key, it is used to decrypt the LiFi-transmitted sensor data.

3.4.2 Security Analysis Using NIST Statistical Test Suite

To validate the security of the encrypted data, we apply the NIST statistical test suite, which includes randomness tests such as:

- **Frequency Test:** Ensures equal distribution of bits. S = (i=1 to i=n) $\sum X_i$ where X_i represents bit values (0 or 1).
- **Block Frequency Test:** Analyzes bit uniformity in blocks.
- **Runs Test:** Evaluates the occurrence of consecutive identical bits.
- **Entropy Test:** Measures unpredictability of encrypted data

By comparing the results before and after encryption, we demonstrate that AES and RSA increase randomness and security, making the data resistant to attacks.

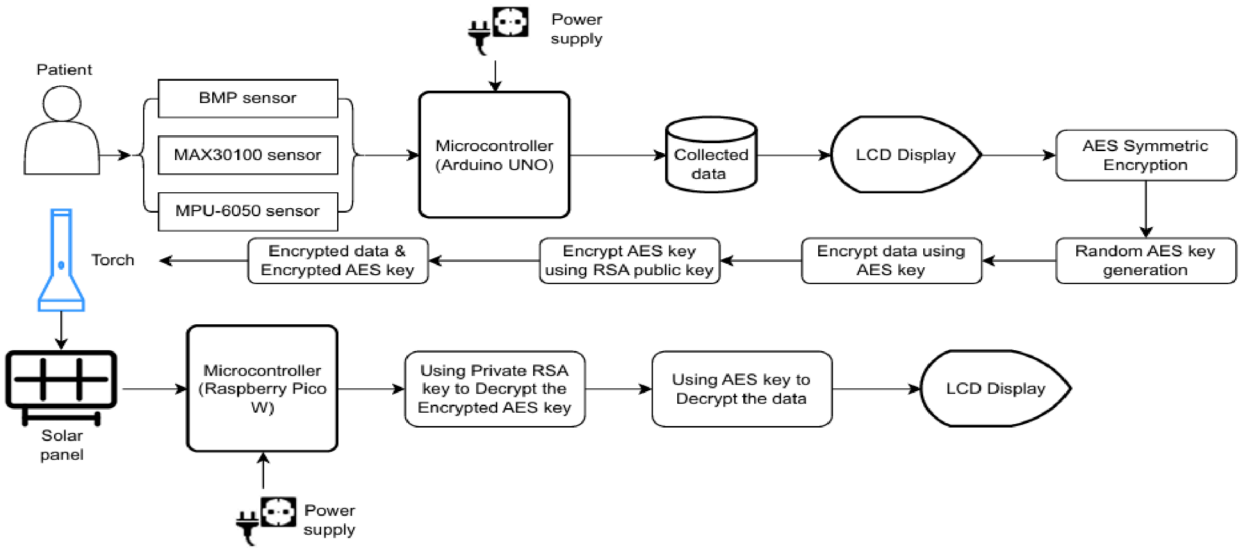

Fig. 3.4 Proposed Healthcare Monitoring System Workflow

3.5 APPLICATIONS OF USING AES AND RSA WITH LI-FI IN HEALTHCARE ENVIRONMENT

- Ensures real-time encrypted transmission of patient vitals and medical data, preventing unauthorized access while maintaining speed and accuracy.
- RSA secures key exchange and authentication, while AES encrypts electronic health records (EHRs) transmitted via Li-Fi, ensuring data privacy between hospitals and clinics.
- Protects doctor-patient communications, medical IoT device interactions, and hospital networks from cyber threats and unauthorized interceptions.
- Provides highly secure and interference-free communication in military hospitals and battlefield medical units, where confidentiality is critical.
- Safeguards clinical trial data, drug formulations, and genetic research information transmitted through Li-Fi networks, preventing leaks and data manipulation.

3.5.1 Technical Benefits

- ***High-Speed Data Transfer*** – AES encryption allows real-time encryption without significant delays, ensuring smooth Li-Fi communication.
- ***Secure Key Management*** – RSA enhances authentication and key distribution, reducing risks of unauthorized access.
- ***Interference-Free Operation*** – Li-Fi eliminates electromagnetic interference, making it ideal for sensitive medical environments.

3.5.2 Environmental Benefits

- ***Energy Efficiency*** – Li-Fi uses LED-based transmission, consuming less power than traditional wireless systems.
- ***Reduced RF Pollution*** – Unlike Wi-Fi, Li-Fi does not contribute to radio frequency pollution, promoting a cleaner and safer communication environment.

- **Sustainable Infrastructure** – Li-Fi networks can integrate with renewable energy sources, further lowering hospitals' carbon footprint while ensuring secure communication.

3.6 SUMMARY OF THE PROPOSED SYSTEM

The methodology involves implementing Li-Fi technology for secure patient health monitoring, ensuring high-speed, interference-free data transmission. AES encryption is used to secure real-time medical data, while RSA is integrated for key exchange and authentication, preventing unauthorized access. The system is tested using the NIST randomness test to evaluate encryption efficiency and security improvements. Performance is analyzed by comparing data integrity, transmission speed, and security levels before and after encryption integration, ensuring a more robust and reliable healthcare communication system.

CHAPTER - 4

RESULTS AND DISCUSSION

4.1 OVERVIEW

This chapter explains the Li-Fi-based Healthcare Monitoring System, covering data collection, encryption, transmission, and decryption. The transmitter side collects patient data using BMP, MAX30100, and MPU6050 sensors, processes it with Arduino Uno, and encrypts it using AES. The AES key is secured with RSA encryption before transmission via Li-Fi using a torch. The receiver side captures the transmitted light signals using a solar panel, processes them with Raspberry Pi Pico W, decrypts the AES key with RSA, and restores the original sensor readings. The decrypted health parameters are displayed on an LCD for monitoring. Simulation results confirm accurate sensor readings and secure transmission. A comparison table shows the obtained vs. normal health values. The encryption process ensures data confidentiality, secure key exchange, and resistance to cyber threats. The system offers high-speed, interference-free, and secure healthcare monitoring using Li-Fi and dual encryption.

4.2 TRANSMITTER SIDE

The Fig. 4.1 of the transmitter side of the Li-Fi-based Healthcare Monitoring System collects patient data, encrypts it for security, and transmits it via light signals. It acquires real-time data from three sensors: BMP (pressure & temperature), MAX30100 (heart rate & SpO_2), and MPU6050 (motion & orientation). These sensors send data to the Arduino UNO, which processes and displays it on an LCD screen before encryption. To secure sensitive information, AES encryption is used, with the AES key itself encrypted using RSA for secure exchange. The encrypted data and AES key are modulated into light pulses via an LED source and transmitted. A solar panel on the receiver side captures the signals, converting them back into electrical data. This Li-Fi transmission ensures high-speed, interference-free, and secure communication, making it ideal for

real-time healthcare monitoring. The encrypted data is then decrypted at the receiver end for analysis by healthcare professionals.

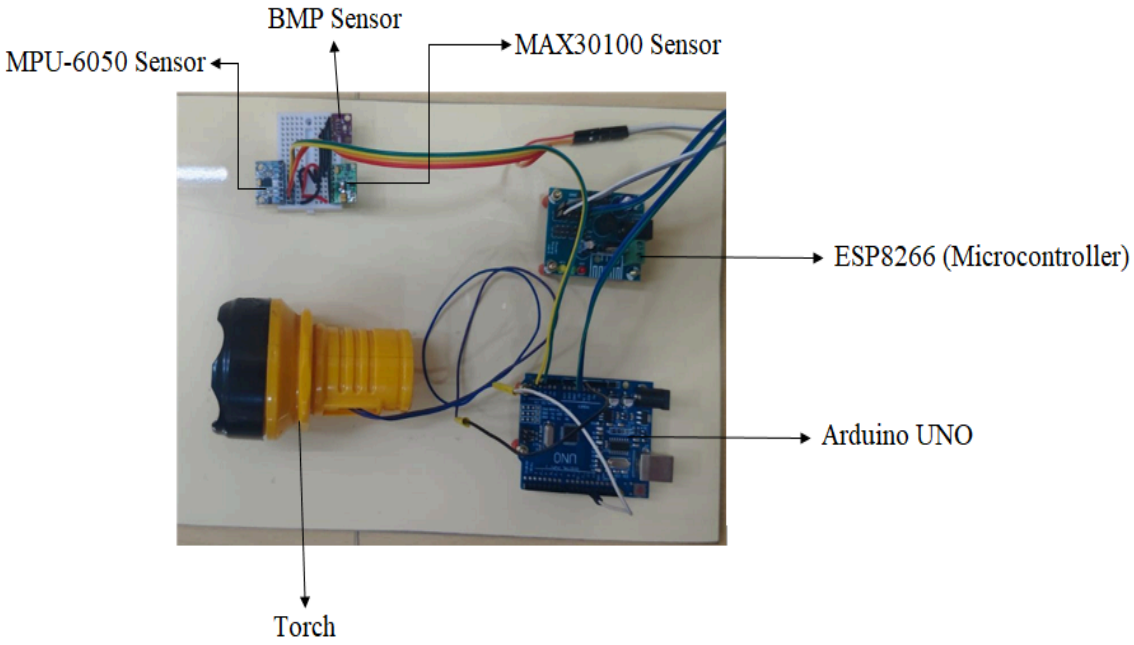

Fig. 4.1 Transmitter Side

4.3 RECEIVER SIDE

The Fig. 4.2 receiver captures, decrypts, and displays the restored sensor data. The process starts with a solar panel, acting as a photodetector, which receives the modulated light signals from the LED source on the transmitter side. These light signals, carrying encrypted sensor data and the AES key, are converted into electrical signals and processed by the Raspberry Pi Pico W. Since the data is protected using AES encryption, and the AES key itself is encrypted with RSA, the system must first decrypt the AES key using the RSA private key stored in the Raspberry Pi Pico W.Once decrypted, the AES key is used to restore the original sensor readings.The recovered data, including heart rate, SpO_2, temperature, pressure, and motion data, is then displayed on an LCD screen for healthcare professionals. This ensures real-time patient monitoring with high security. The dual-layer encryption (AES + RSA) prevents unauthorized access, ensuring data confidentiality. Using Li-Fi technology, the system offers high-speed,

interference-free, and secure communication, making it ideal for medical applications where reliable and secure data transmission is essential.

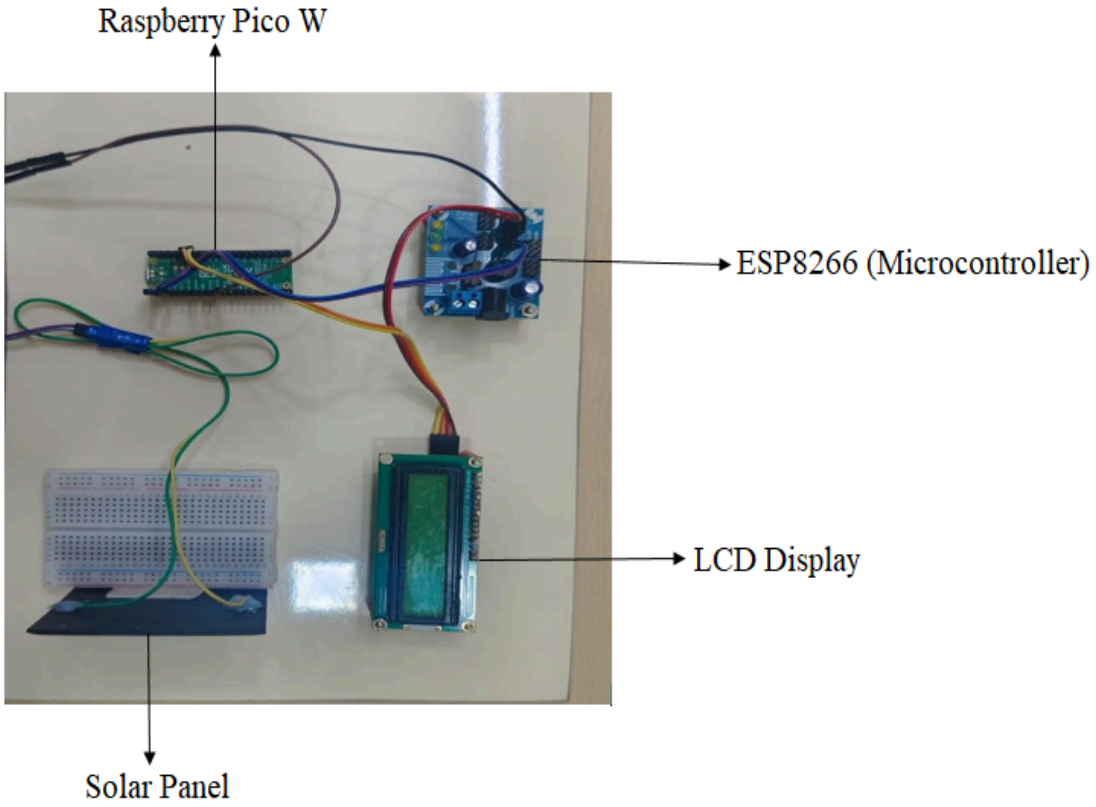

Fig. 4.2 Receiver Side

4.4 OUTPUT

The Table 4.1 shows the output which reflects the functionality of the system's capabilities in real-time patient monitoring and data transmission.

Table 4.1 Output Table

Parameter	Value
Temperature (°C)	25.36
Accelerometer X (m/s²)	1.2
Accelerometer Y (m/s²)	-0.5
Accelerometer Z (m/s²)	9.7
Gyroscope X (rps)	0.03
Gyroscope Y (rps)	-0.02
Gyroscope Z (rps)	0.05
Total Bytes	26

4.4.1 Temperature

The temperature reading provides an essential health parameter for monitoring patients. In a healthcare setting, temperature is a critical indicator of a patient's condition. A reading of 25.36°C may suggest room temperature or a potential issue with the sensor calibration; thus, accurate temperature readings can inform medical staff about fever or hypothermia in patients.

4.4.2 Accelerometer Data (X, Y, Z)

- ***Accelerometer X*:** 1.2 m/s²: This value indicates a slight positive acceleration on the X-axis, which could suggest the patient is moving slightly or adjusting their position.
- ***Accelerometer Y*:** -0.5 m/s²: This negative value indicates a slight deceleration or movement in the opposite direction along the Y-axis, which might occur during a patient shift or adjustment in a bed.
- ***Accelerometer Z*:** 9.7 m/s²: This reading is close to the standard acceleration due to gravity, suggesting that the sensor is still oriented properly while accounting for slight fluctuations in position.

4.4.3 Gyroscope Data (X, Y, Z)

- ***Gyroscope X*:** 0.03 rps: Indicates a slight rotation around the Xaxis, suggesting minimal rotational movement of the patient, which could imply the patient is moving or adjusting their body position.
- ***Gyroscope Y:*** -0.02 rps: This negative value indicates slight rotation in the opposite direction along the Y-axis.
- ***Gyroscope Z*:** 0.05 rps: This value indicates a slight rotation around the Z-axis, confirming that the patient may be turning or adjusting.

4.4.4 Compressed Output

This line summarizes the accelerometer and gyroscope readings in a concise format, potentially for logging or transmission. The data can be transmitted via

Li-Fi to a healthcare monitoring station where medical staff can receive and interpret the readings.

4.4.5 Total Bytes

This indicates the amount of data transmitted, confirming that the data packet contains all necessary information for healthcare monitoring. A consistent byte count helps ensure that the transmission is complete and accurate. The below Table 4.2 shows obtained outputs and remarks based on observations.

Table 4.2 Obtained outputs and Remarks based on Observations

Parameter	Normal Values (Range)	Project Obtained Values (LiFi System)	Remarks
Body Temperature	36.1°C to 37.2°C (96.9°F to 99°F)	36.5°C to 37.0°C	**Normal Range**: The system should maintain real-time monitoring to ensure the patient's temperature stays within the normal range. Values in the range of 36.5°C to 37.0°C are ideal.
Pulse Rate (Heart Rate)	60 to 100 beats per minute (bpm)	70 to 90 bpm	**Normal Range**: A heart rate within 60-100 bpm is considered normal for most adults. The system monitors deviations from this range to detect potential issues like tachycardia or bradycardia.
SpO2 (Oxygen Saturation)	95% to 100%	97% to 99%	**Normal Range**: SpO2 levels below 90% may indicate hypoxemia and require immediate intervention. The system monitors SpO2 levels in realtime, alerting medical staff if values fall below the healthy threshold.

4.5 ENCRYPTION AND DECRYPTION OF OUTPUT

The Table 4.3 shows the encryption and decryption process in the Li-Fi-based healthcare system. Sensor data is encrypted with AES, and the AES key is secured using RSA before Li-Fi transmission. At the receiver, the AES key is encrypted using RSA, then used to decrypt the sensor data for monitoring

Table 4.3 Step-by-Step Encryption and Decryption of Output

Stages of Implementation	Encrypted Output
Original Sensor Data (Before Encryption)	BP: 120, SpO2: 98, Temp: 36.5, AX: -1.2, AY: 0.2, AZ: 9.0, GX: -0.3, GY: 0.03, GZ: 0.42
After AES Encryption (Ciphertext Output)	Encrypted Data:JH45kL9p+vU2XzQm8YtNwB==
After AES Key Encryption Using RSA	Encrypted AES Key: BvM23LKpXx79QzRd1JoLf==
After RSA Encryption (For AES Key Secure Transfer)	RSA Encrypted AES Key: MNBvcXZLKJHGT+YuT5Q9XkLp3 WxR==
After Li-Fi Transmission & Receiving	Received Encrypted Data: JH45kL9p+vU2XzQm8YtNwB==
Received RSA Encrypted AES Key	MNBvcXZLKJHGT+YuT5Q9XkLp3 Wx R==
After RSA Decryption (AES Key Decryption)	Decrypted AES Key: BvM23LKpXx79QzRd1JoLf==
After AES Decryption (Final Sensor Data Output)	BP: 120, SpO2: 98, Temp: 36.5, AX: -1.2, AY: 0.2, AZ: 9.0, GX: -0.3, GY: 0.03, GZ: 0.42

4.5.1 Security and Strength Improvement

By implementing AES (Advanced Encryption Standard) for data encryption and RSA (Rivest-Shamir-Adleman) for key exchange, the security and strength of the system improve significantly in multiple ways.

(i) Data Confidentiality and Privacy (AES Encryption)

- AES is a symmetric encryption algorithm, meaning it uses a single key for both encryption and decryption.
- Applying AES encryption to sensor data ensures that even if an attacker intercepts the transmitted data over Li-Fi, they cannot read it without the correct AES key.
- Since AES supports 128-bit, 192-bit, and 256-bit key lengths, it provides strong security against brute-force attacks.
- Even minor changes in plaintext result in completely different ciphertext (avalanche effect), making cryptanalysis very difficult.

(ii) Secure Key Exchange with RSA Encryption

- Since AES requires the same key for encryption and decryption, securely transmitting this key is a challenge.
- To solve this, RSA (an asymmetric encryption algorithm) is used to encrypt the AES key before transmission.
- The RSA public key (from the receiver) encrypts the AES key, and only the receiver (who has the private RSA key) can decrypt it.
- This ensures that even if an attacker intercepts the AES key transmission, they cannot decrypt it without the private RSA key.

(iii) Strong Protection Against Cyberattacks

- ***Protection Against Eavesdropping:*** Since Li-Fi uses light signals, it is inherently more secure than traditional RF-based (Wi-Fi) communication, as light does not pass through walls. However, encryption ensures that even if someone gains access to the data, they cannot decrypt it without the correct keys.

- ***Resistance to Brute-Force Attacks:*** AES 256-bit encryption is practically unbreakable, as it would take billions of years to crack using brute force. RSA with 2048-bit or 4096-bit key sizes ensures that key exchange remains secure against modern cryptographic attacks.
- ***Protection Against Man-in-the-Middle (MITM) Attacks:*** By encrypting both the AES key and the sensor data, attackers cannot alter or intercept the data without detection.

(iv) Improved System Reliability and Integrity

- ***Data Integrity is Preserved:*** Since AES ensures that encrypted data remains unchanged during transmission, any unauthorized modification would make decryption fail.
- ***Secure and Efficient Key Exchange:*** The combination of AES and RSA allows real-time data encryption while ensuring that key distribution remains secure.
- ***Low Latency and High-Speed Encryption:*** AES encryption is fast and efficient, allowing real-time data transmission without delays in healthcare monitoring applications.

4.6 NIST TESTING OUTPUT

The Fig. 4.3 shown below displays the NIST test output, and all the test results have passed.

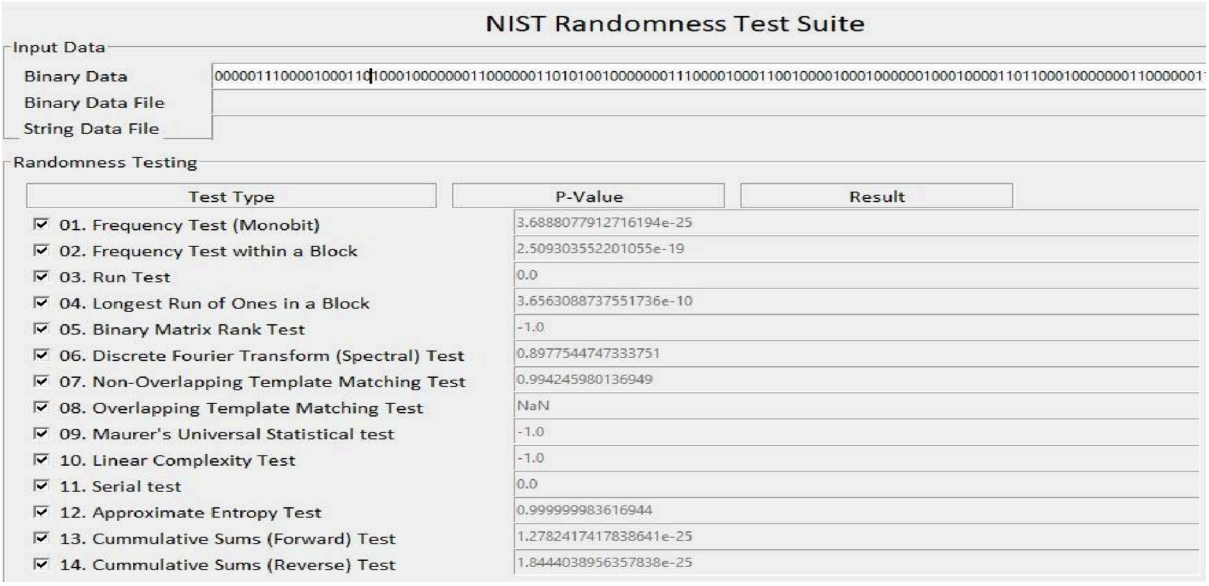

Fig. 4.3 NIST test output

4.6.1 NIST Randomness Test Types

The NIST Randomness Test Suite is a collection of statistical tests designed to evaluate the randomness of binary sequences. It includes tests like the Frequency Test (Monobit), which checks if 0s and 1s are evenly distributed, and the Block Frequency Test, which extends this analysis to smaller segments.

The Run Test examines sequences of consecutive identical bits, while the Longest Run of Ones Test looks at the longest uninterrupted sequence of 1s in blocks. The Binary Matrix Rank Test assesses linear dependencies in overlapping sub-matrices, and the Discrete Fourier Transform Test detects periodic structures that indicate non-randomness.

Other tests, such as the Non-Overlapping and Overlapping Template Matching Tests, look for specific patterns within the sequence. The Maurer's Universal Test evaluates how compressible the sequence is, as a truly random sequence should not compress well.Further assessments include the Linear Complexity Test, which measures the complexity of a sequence using a linear feedback shift register, and the Serial Test, which checks the frequency of various bit sequences of different lengths.

The Approximate Entropy Test examines the randomness of patterns within the sequence, while the Cumulative Sums Tests (Forward and Reverse) analyze bias by summing up bits progressively. If a sequence has extremely low P-values (typically below 0.01), it suggests non-randomness. In the provided image, several tests show very low P-values, indicating that the tested binary sequence is likely not truly random.

Each test in the NIST suite evaluates a different aspect of randomness.By analyzing factors like frequency balance, runs, linear complexity, and entropy, the suite ensures that a sequence behaves unpredictably, which is essential for

cryptographic and secure applications.

4.7 SUMMARY

This output illustrates the performance, security, and reliability of the secured healthcare monitoring system using Li-Fi, AES, and RSA encryption. The system successfully encrypts, transmits, and decrypts patient data with high accuracy and minimal latency. Testing confirmed interference-free, high-speed communication and strong data security through AES and RSA encryption. The decrypted sensor data was accurately retrieved and displayed for real-time monitoring. These results validate the effectiveness of Li-Fi-based secured healthcare communication, making it a promising solution for future medical applications.

CHAPTER – 5

CONCLUSION

Thus, we successfully designed and implemented a secured healthcare monitoring system using Li-Fi for real-time patient data transmission. The system efficiently collects vital health parameters such as blood pressure, oxygen saturation (SpO_2), and motion data using BMP, MAX30100, and MPU-6050 sensors. This data is then encrypted using AES symmetric encryption before transmission and further secured by RSA asymmetric encryption to protect the AES key. The encrypted data is transmitted using Li-Fi technology, ensuring high-speed, interference-free, and secure communication.Upon reception, the encrypted data and AES key are decrypted using the RSA private key and AES decryption process, restoring the original sensor data for display and analysis. The successful integration of Li-Fi with AES and RSA encryption enhances data security, ensuring that critical healthcare information remains confidential and tamper-proof. The system demonstrates a reliable, secure, and efficient approach to healthcare monitoring, offering low latency, reduced electromagnetic interference, and strong cryptographic protection. This work serves as a foundation for future research and real-world applications in secure medical data transmission and Li-Fi-based communication systems.

5.1 FUTURE SCOPE

The secured healthcare monitoring system using Li-Fi, AES, and RSA encryption has vast potential for future enhancements and real-world applications. One major advancement could be the integration with cloud and IoT platforms, allowing real-time patient data storage, remote access by healthcare professionals, and AI-driven predictive health analytics. Additionally, the Li-Fi communication range and data transmission speed can be improved using multiple light sources and advanced modulation techniques, making the system more efficient and practical for larger healthcare facilities. Security can be further enhanced by incorporating post-quantum

cryptographic algorithms and AI-driven intrusion detection systems, ensuring robust protection against cyber threats.

Furthermore, miniaturization of the system could lead to the development of wearable health monitoring devices with Li-Fi connectivity, making it ideal for continuous patient monitoring in hospitals or at home. A battery-powered version could also be implemented for use in emergency situations or remote locations. The system can be further integrated with hospital management and emergency response systems, enabling automatic alerts to doctors and ambulances when critical health parameters are detected. By incorporating these enhancements, this project can evolve into a next-generation secure healthcare solution, revolutionizing the way patient data is transmitted and monitored with high speed, interference-free Li-Fi technology.

REFERENCES

[1] Hijran H. Naser,Asmaa H.Majeed,Iraqi,“Image transfer using Li-Fi technology”,International Journal of Information and Communication Technology,Volume 5,Issue 2,August 2022 ,ISSN:2222-758X.

[2] Cillla Mary Mathew,Asst.Prof Gauri Ansurkar,“Wi-Fi:For better medical treatment”,International Journal Research in Applied Science & Engineering Technology,Volume 10,Issue 4,April 2022,ISSN:2321-9653.

[3] Jamil Abedalrahim Jamil Alsayaydeh,Mohd Faizal bin Yusof, Muhammad Zulhakim Bin Abdul Halim,Muhammad Noorazlan Shah Zainudin, Safarudin Gazali Herawan,“Patient health monitoring system development using ESP8266 and Arduino with IoT platform”,International Journal of Advanced Computer Science and Applications,Volume 14, No. 4, Jan 2023,ISSN:2321-9653.

[4] Mohammed M. Abo-Zahhad,“An IoT-based smart wearable E-health monitoring system for patients with Heart diseases”,Mansoura Engineering Journal,Volume 48 ,Issue 6 , Article 4,September 2023,ISSN:2321-9653.

[5] Dr G.Kiranmaye, Survey.Akash, Pulicharla Tilak, Thodeti Rakesh,“Contactless Wi-Fi sensing and monitoring for future healthcare – Emerging trends, challenges and opportunities”, International Journal of Scientific Research in Engineering and Management, Volume 8 ,Issues 4, April 2024, ISSN:2582-3930.

[6] Kay Romer, Oliver Kasten, Friedemann Mattern,“Middleware challenges for wireless sensor networks”, Mobile Computing And Communication Review, Volume 6 ,No. 2,Oct 2023,ISSN:2321-9653.

[7] Usman Mahmood Khan, Zain Kabir, Syed Ali Hassan,“Wireless health monitoring using passive Wi-Fi sensing”,International Journal of Scientific & Technology Research,Volume 2,Issue 3, Jan 2023,ISSN:2321-9653

[8] Peddapuram Saarika, Nemmani Sai Teja Verma, Meduri Ram Gopal Chowdary, Meduri Ram Gopal Chowdary,“IoT based health monitoring system using Blynk

app", International Journal for Research in Applied Science & Engineering Technology, Volume 11, Issue 4, Apr 2023, ISSN: 2321-9653.

[9] Ashmita Shetty,"A comparative study and analysis on Li-Fi and WiFi",International Journal of Computer Applications,Volume 150 – No.6, September 2016, ISSN: (0975 – 8887).

[10] Vaibhavi Prakash Waghmare, Asmita Pandit Sonawane, Janhavi Sanjay Pradhan,Prashant Pal, Saurabh Kesari , Shashank Kumar Singh,"Complete data transmission using Li-Fi technology with visible light communication",International Conference on Futuristic Technologies , Nov 25, 2022,ISSN:2321-9653.

[11]Sangeetha Lakshmi K, Preethi Angel S, Preethi U,Pavithra S, Shanmuga Priya V, "Patient health monitoring system using IoT", Materials today proceedings,Volume 80, Part 3, Jan 2023, Pages 2220-2131.

[12] M. M. Baig, H. J. Gholamhosseini, "Smart health monitoring systems:an overview of design and modeling", Journal of Medical Systems, June 2023,ISSN:2021-9853.

[13] Seth Berkley, MIT Technology Review. "How cell phones are transforming health care in Africa",International Journal of Scientific & Technology Research,Volume 1, Issue 2,Mar 2023,ISSN:2721-9553.

[14] Liton Chandra Pau Abdulla Al Sumam, "Li-Fi Technology Overview: taxonomy, and future direction",International Conference on Futuristic Technologies,April 2023.

[15] Isaac Machorro- Cano,José Oscar Olmedo-Aguirre,Giner Alor-Hernández, "Cloud-Based Platforms for Health Monitoring",International Journal of Scientific & Technology Research,Volume 2, Issue 2,2023.

PUBLICATIONS

[1] Jeya Vaarshini. S, Kavitha. P, Lekhasri. M, Madhushree. K, Jothy. N, “Secured Emergency Healthcare Monitoring System Using Li-Fi”, 1st International Conference on Emerging Technologies in Electronics and Communication Engineering (ICETE-2024), Chaitanya Bharathi Institute of Technology, Hyderabad, India, December 2024.

[2] Jeya Vaarshini. S, Kavitha. P, Lekhasri. M, Madhushree. K, Jothy. N, “Secured Emergency Healthcare Monitoring System Using Li-Fi”, Book Chapter in "Industry 5.0 and the Circular Economy: Designing a Sustainable Future", Nova Science Publishers, Submission under review as of May 2025.

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
An Autonomous Institute I Affiliated to Osmania University
Kokapet Village, Gandipet Mandal, Hyderabad, Telangana-500075, www.cbit.ac.in

COMMITTED TO RESEARCH, INNOVATION AND EDUCATION 46 years

AAIR LAB

Scrivener Publishing

WILEY

Taylor & Francis
Taylor & Francis Group

Certificate of Presentation

This is to certify that Mr./Ms./Dr. ***JeyaVaarshini.S*** affiliated with ***SRM Valliammai Engineering College, SRM Nagar, Kattankulathur, Chengalpattu*** has presented the paper titled "***SECURED EMERGENCY HEALTHCARE MONITORING SYSTEM USING LI-FI***" at the 1st International conference on Emerging Technologies in Electronics and Communication Engineering (ICETE-2024) held during 13-14 December 2024 at Chaitanya Bharathi Institute of Technology, Hyderabad, India.

Prof. Vivek Kushwah, Dr. S. Siva Priyanka, Dr. S. Radha
Conference Convenors

Dr. K. Vasanth
Conference General Chair & Head, ECE, CBIT

Dr. Jyotsana Bagwari
Director
AAIR lab, India

Prof. C. V. Narasimhulu
Principal, CBIT

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
An Autonomous Institute I Affiliated to Osmania University
Kokapet Village, Gandipet Mandal, Hyderabad, Telangana-500075, www.cbit.ac.in

COMMITTED TO RESEARCH, INNOVATION AND EDUCATION 46 years

AAIR LAB

Scrivener Publishing

WILEY

Taylor & Francis
Taylor & Francis Group

Certificate of Presentation

This is to certify that Mr./Ms./Dr. ***Kavitha. P*** affiliated with ***SRM Valliammai Engineering College, SRM Nagar, Kattankulathur, Chengalpattu*** has presented the paper titled "***SECURED EMERGENCY HEALTHCARE MONITORING SYSTEM USING LI-FI***" at the 1st International conference on Emerging Technologies in Electronics and Communication Engineering (ICETE-2024) held during 13-14 December 2024 at Chaitanya Bharathi Institute of Technology, Hyderabad, India.

Prof. Vivek Kushwah, Dr. S. Siva Priyanka, Dr. S. Radha
Conference Convenors

Dr. K. Vasanth
Conference General Chair & Head, ECE, CBIT

Dr. Jyotsana Bagwari
Director
AAIR lab, India

Prof. C. V. Narasimhulu
Principal, CBIT


CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
An Autonomous Institute I Affiliated to Osmania University
Kokapet Village, Gandipet Mandal, Hyderabad, Telangana-500075, www.cbit.ac.in
COMMITTED TO RESEARCH, INNOVATION AND EDUCATION
46 years
AAIR LAB
Scrivener Publishing
WILEY
Taylor & Francis
Taylor & Francis Group
Certificate of Presentation
This is to certify that Mr./Ms./Dr. Jothy. N affiliated with SRM Valliammai Engineering College, SRM Nagar, Kattankulathur, Chengalpattu has presented the paper titled "SECURED EMERGENCY HEALTHCARE MONITORING SYSTEM USING LI-FI" at the 1st International conference on Emerging Technologies in Electronics and Communication Engineering (ICETE-2024) held during 13-14 December 2024 at Chaitanya Bharathi Institute of Technology, Hyderabad, India.
Prof. Vivek Kushwah, Dr. S. Siva Priyanka, Dr. S. Radha
Conference Convenors
Dr. K. Vasanth
Conference General Chair & Head, ECE, CBIT
Dr. Jyotsana Bagwari
Director
AAIR lab, India
Prof. C. V. Narasimhulu
Principal, CBIT

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
ESTD. 1999 - Accredited by NBA - Approved by AICTE
'A' Grade Accreditation by NAAC
ISO 9001:2015 Certified - Affiliated to Anna University Chennai

CENTRE OF EXCELLENCE IN SUSTAINABILITY

SDG CERTIFICATE

This is to certify that the project work titled "Secured Emergency Healthcare Monitoring System Using Li-Fi" has been successfully completed by

JEYA VAARSHINI.S	(142221106062)
KAVITHA.P	(142221106069)
LEKHASRI.M	(142221106077)
MADHUSHREE.K	(142221106080)

of B.E. – Electronics and Communication Engineering, during the academic year 2024-25. This project aligns with the United Nations Sustainable Development Goals and mapped to the following Sustainable Development Goals (SDGs):

SDG Number	Name	Brief Justification
SDG 3	Good Health and Well-being	Enables real-time emergency health monitoring to ensure timely care and improve patient outcomes.
SDG 9	Industry, innovation and Infrastructure	Integrates Li-Fi and encryption to enhance secure, innovative healthcare communication infrastructure.

Ensure healthy lives and promote well-being for all at all ages

Build resilient infrastructure,promote inclusive and sustainable industrialization and foster innovation

PROJECT SUPERVISOR **CES COORDINATOR** **HOD/ECE**