

AI Driven Health Monitoring System With Secure Transmission

*A Project Report Submitted in the
Partial Fulfillment of the Requirements for
the Award of the Degree of*

BACHELOR OF TECHNOLOGY

IN

Computer Science And Engineering

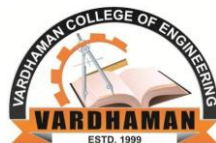
Submitted by

A. Akshaya	22881A05K4
Ch. Sreekumari	22881A05L7
Deepak Kashid	22881A05L9

SUPERVISOR

G. Prasada Reddy

Assissant Professor

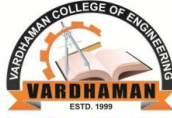


Department of Computer Science Engineering

VARDHAMAN COLLEGE OF ENGINEERING, HYDERABAD

An Autonomous Institute, Affiliated to JNTUH

May, 2021



VARDHAMAN COLLEGE OF ENGINEERING, HYDERABAD

An Autonomous Institute, Affiliated to JNTUH

Department of Computer Science And Engineering

CERTIFICATE

This is to certify that the project titled **AI Driven Health Monitoring System With Secure Transmission** is carried out by

A. Akshaya	22881A05N4
Ch. Sreekumari	22881A05L7
Deepak Kashid	22881A05L9

in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science And Engineering** during the year 2025-26.

Signature of the Supervisor
G. Prasada Reddy
Assissant Professor

Signature of the HOD
Dr.Ramesh Karnati
Professor and Head, CSE

Kacharam (V), Shamshabad (M), Ranga Reddy (Dist.)-501218, Hyderabad, T.S.
Ph: 08413-253335, 253201, Fax: 08413-253482, www.vardhaman.org

Acknowledgement

The satisfaction that accompanies the successful completion of the task would be put incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

We wish to express our deep sense of gratitude to **G. Prasada Reddy**, Guide and Project Supervisor, Department of Computer Science And Engineering, Vardhaman College of Engineering, for his able guidance and useful suggestions, which helped us in completing the project in time.

We are particularly thankful to **Dr.Ramesh Karnati**, the Head of the Department, Department of Computer Science And Engineering, his guidance, intense support and encouragement, which helped us to mould our project into a successful one.

We show gratitude to our honorable Principal **Dr. J.V.R. Ravindra**, for providing all facilities and support.

We avail this opportunity to express our deep sense of gratitude and heartfelt thanks to **Dr. Teegala Vijender Reddy**, Chairman and **Sri Teegala Upender Reddy**, Secretary of VCE, for providing a congenial atmosphere to complete this project successfully.

We also thank all the staff members of Electronics and Communication Engineering department for their valuable support and generous advice. Finally thanks to all our friends and family members for their continuous support and enthusiastic help.

A. Akshaya

Ch. Sreekumari

Deepak Kashid

Abstract

This system measures your health in real time by monitoring important metrics such as blood pressure, heart rate, and oxygen levels. AI analyzes the data and identifies potential threats to your health in advance. To ensure the confidentiality of your data, it utilizes strong data encryption and secure protocols for transmitting and storing data. You will receive alerts by email if they arise during emergencies. The system continues to monitor the data and ensure risk detection by executing reliable and secure health monitoring, ultimately preventing problems while managing risk. Privacy is a primary perspective of this system that ensures proper protection of sensitive health data. As an integrity-preserving control system, the system applies the Secure Hash Algorithm (SHA) to verify that there have been no modifications of health records while they are stored or transmitted. In this way, personal health data are protected from illicit use. During emergency situations, this system alerts the user via email notifications based on the assessment of the data collected. The organization in place ensures that the system operates faster and more securely than the prior privacy mechanisms. The AI-driven information and cryptographic protocols allow empowered users to take charge of their health.

Keywords *AI-Driven-Virtual-Assistant, Emotion-Recognition, AI-Live-Surroundings-Recording, AI-Powered-Collaboration, Personalized-Digital-Companion, Next-Gen-AI-Technology, Multilingual.*

Table of Contents

Title	Page No.
Acknowledgement	i
Abstract.....	ii
List of Tables.....	Error! Bookmark not defined.
List of Figures.....	iv
Abbreviations.....	5
CHAPTER 1 Introduction	6

CHAPTER 2	PROBLEM STATEMENT.	7
CHAPTER 3	Literature Survey	8
2.1	Application of AI in Remote Patient Monitoring	8
2.2	Secure Communication Protocols in Remote Healthcare	8
2.3	Real-Time Vital Data Monitoring using Machine Learning	8
2.4	Data Integrity through SHA-256 Hashing and Blockchain	8
2.5	Edge Computing for Faster Health Data Processing	8
2.6	Predictive Analytics and Proactive Healthcare Systems	8
2.7	Emerging Trends in Intelligent, Secure Remote Monitoring	8
CHAPTER 4	METHODOLOGY	9
CHAPTER 5	RESULT	12
CHAPTER 6	CONCLUSION.	15
6.1	Future enhancements	16
CHAPTER 7	References	17

List of Figures

2.4	Figure 1 AI-Based Health Monitoring.	11
2.2	Figure 2 AI-Based Health Monitoring Dashboard.	13
2.3	Figure 3 Normal Status.	13
2.5	Figure 4 Alert status.	14
2.6	Figure 5 Email Alert Notification.	14

Abbreviations

Abbreviation	Description
VCE	Vardhaman College of Engineering
MI	Machine learning
SSL	Secure sockets layer
SHA	Secure Hash Function

CHAPTER 1

INTRODUCTION

Health monitoring systems powered by artificial intelligence are changing our approach to health management. These systems use advanced technologies powered by artificial intelligence to monitor health metrics including, but not limited to, oxygen saturation, blood pressure (systolic and diastolic), and heart rate. The systems provide input data to alert the user of their health status while informing deviation from their baseline if an abnormality occurs. In addition to monitoring, integrated features include alerts for emergency situations. Overall this style of health monitoring promotes intervention at an early detection or indication of abnormality with the

potential for significantly better outcomes. Incorporating both AI and cryptographic hashing expands the monitoring capabilities to predicting health abnormalities and sending alerts via mail. Security and privacy are priority in these systems, as they protect sensitive health data. Protecting data integrity during collection and transmission for tampering, the system employs secure hash algorithm (SHA)-256 Cryptography hash function. Enabling accurate and safe health monitoring assist individual in taking control of their health. This algorithm (SHA) creates a 256-bit hash value from the input data and protocols (SSL/TLS) that protect the data against unauthorized access as it travels between the user's device and a website, so that only authorized users have access to personal information and no one else. We can detect early signs of health issues through parametric monitoring and act on them fast to avert future problems. The system will provide immediate alerts via mail notifications in case of emergency, to enable timely action with the aim of minimizing negative health impacts. The system will also be applying AI in analysing the data for potential health risks.

CHAPTER 2

PROBLEM STATEMENT

Currently, in the field of healthcare and patient issue management, there has been an increasing demand for a patient monitoring system that is carried out in real-time. With the uptick in the prevalence of chronic illness, and the increased use and demand for mobile health monitoring devices, ongoing health monitoring is critical when attempting to avert medical emergencies. In some circumstances, the application of an AI model may be capable of monitoring patient health continuously with accurate anomaly detection, however, it poses a number of challenges as well, namely in the area of data security, privacy, and reliability. While the expectation that a successful AI-powered health monitoring system will produce accurate and comprehensive patient data can be high, inaccurate reporting or detection of anomalies often yields false alarms or warnings- producing stress to the patient or worse, risking their health if the communication is neglected. Aside from false or inaccurate reporting of health conditions, heightened concerns for data security of a patient's information will also be crucial. Patient monitoring systems are expected to send and receive sensitive health information, including heart rates, oxygen levels, and ECG patterns over a network. Without encryption and authentication, the information is susceptible to being intercepted. Additionally, there is concern of reliability in the transmission of health data. During the process of receiving and sending health monitoring data, there is risk in interception or tampering. Without secure protocols in place, even a simple edit could change a patient's health record's validity; which may lead to improper diagnosis symptoms, or delayed interventions. This paper provides a position for an AI-based health monitoring system that monitors health status with the secure transmission of health-related data.

The system relies on machine learning algorithms to detect abnormal data points in real time, leading to a decrease in false-positive outcomes, while detecting risk at a safer and earlier stage. To secure sensitive health-related data the system utilizes end-to-end encryption and a blockchain-supported authentication framework that maintains confidentiality and integrity of data in the exchange.

CHAPTER 3

III. LITERATURE SURVEY

Over the past few years, many studies have centred around applying Artificial Intelligence (AI) and secure communication protocols to healthcare to improve remote patient monitoring. AI technologies use real-time data to identify health anomalies earlier and with quicker follow-up, while cryptographic protocols can be used to safeguard sensitive medical information. Gupta, R., et al. (2023) emphasized the transition from ECG systems to AI-enhanced ECG systems, capable of detecting cardiac anomalies with great certainty through machine learning models, providing for a proactive approach to cardiac medicine [1]. Similarly, Singh, P., et al. (2020) demonstrated that machine learning technology, such as Random Forest and Support Vector Machines, could detect anomalies in real-time using patient vital data, which includes heart rate and blood pressure [7]. Meanwhile, a major concern for secure transmission in remote healthcare systems. In their study, Zhang and his colleagues (2022) investigated the SSL/TLS protocols which ensured the dependable transmission of health data to and from cloud servers and client devices, stating that the protocol demonstrations involved enhancing protection with respect to encryption and attacks suffered a much lower level of vulnerability or breach [2]. Rahman, based on a literature review in 2021, reported likewise that in an IoT-enabled healthcare system, secure protocols protected against some breach, and that the secure protocols under study were utility protocols [6]. Furthermore, data integrity is essential to upholding trust within healthcare analytics. Patel et al. (2021) and Kumar et al. (2022) both evaluated how SHA-256 hashing algorithms applied to healthcare data transfers ensure data is unaltered and secure from tampering [3][8]. These cryptographic methods can enhance the transparency and security of health data exchanges, particularly when used in conjunction with blockchain frameworks, as confirmed by Chen et al., 2020, and Lee et al. in their paper (2020) [4][12]. Innovative technologies like edge computing and federated learning are now being deployed to support the development of an AI-healthcare ecosystem. In particular, Hassan, et al., (2023) presented a scalable edge computing solution to promote health data activities at the edge node, before it was transmitted, thereby reducing transmission (ie latency) time and promoting quicker patient privacy solutions [9]. In addition, Das et al (2022) introduced the concept of federated learning to train AI models on multiple decentralized datasets while facilitating patient privacy and data security – without needing to centralize patients’ sensitive health data [11]. Finally, researchers such as Fernandez et al, (2021) and Ahmed et al. (2022) proposed the concept of AI powered predictive analytics and secure AI systems. While both of these methodologies target health events, their purpose differs. Specifically, both methods aim to shift the healthcare paradigm from detection to predict and prevent activity, thus changing healthcare from reactive care to proactive care [10] [15]. Ultimately, the literature really points toward an increasing trend in intelligent, secure, and privacy-preserving health monitoring systems. The application of AI, SSL/TLS and SHA- 256 encryption methods, and blockchain is likely to offer a disruptive impact to the field of remote health monitoring.

CHAPTER 4

IV. METHODOLOGY

A. System Architecture

The health monitoring system developed in this project follows a modular design, combining AI-based health prediction, secure data handling, and instant alert notifications. It includes several key components such as a user-friendly web interface to collect health data, a backend machine learning model to assess health conditions, a security system for user authentication and encrypted communication, and an alert system to notify users in case of abnormal readings. All components communicate smoothly over secure HTTP/HTTPS connections, and the entire application is built using the Flask framework for easy and efficient backend management.

B. Dataset and Preprocessing

The dataset used in this system includes key health indicators such as heart rate, blood pressure (systolic and diastolic), and oxygen saturation (SpO2). It contains a total of 500 records with 4 main features and a corresponding label indicating whether the condition is "Normal" or "Alert". Before training the model, the data is pre-processed to ensure accuracy and consistency. This involves handling missing values, removing outliers, normalizing the feature values, and making sure both classes are well represented. The cleaned dataset is then split into a training set (70) and a testing set (30) to evaluate the model's performance effectively.

C. AI Model Training and Testing

To classify the health status of a user as either "Normal" or "Alert", a machine learning classification model is employed. In this study, models such as Random Forest and Logistic Regression are explored due to their robustness and interpretability. The selected model is trained using the pre-processed dataset with labelled health conditions. Model evaluation is conducted using standard metrics including accuracy, precision, recall, and F1-score. Cross-validation techniques are applied to mitigate overfitting and improve generalization. The final trained model is serialized using Python's joblib or pickle libraries and integrated into the Flask backend for real-time prediction based on user input.

D. Secure Data Transmission Techniques

Security is a critical aspect of this health monitoring system, especially when dealing with sensitive medical data. The system employs SHA-256 hashing for securing user credentials during login, ensuring that passwords are never stored in plain text. Additionally, Advanced Encryption Standard (AES) is used to encrypt the data being transmitted from the frontend to the backend, safeguarding against man-in-the-middle attacks. The entire web application is secured using Transport Layer Security (TLS/SSL) protocols to encrypt communication over the network. These combined techniques ensure confidentiality, integrity, and authenticity of the user's data throughout the transmission pipeline.

E. Web-Based Health Input and Prediction

A user-friendly web interface is developed to collect health data from users. The interface includes a login page where users enter their name and email, and an input form where users can enter their heart rate, blood pressure, and SpO2 levels. Upon submission, the entered values are transmitted securely to the backend server, where the machine learning model processes the data and returns a prediction. The result is then displayed to the user in real time, indicating whether the health condition is normal or if an alert needs to be raised. This web-based system allows remote monitoring without the need for specialized devices, making it highly accessible.

F. Alert Notification System

To enhance the responsiveness of the system, an automated alert notification module is implemented. If the AI model classifies a user's health status as "Alert", an email notification is immediately sent to the registered email address of the user. This is achieved using the Simple Mail Transfer Protocol (SMTP) and Gmail API integration within the Flask server. The email contains a timestamp, the user's name, and a message prompting them to seek medical attention. This feature adds a real-time response capability to the system, which is vital in emergency scenarios, especially for remote patients or elderly individuals living alone. Fig 1 AI-based health monitoring system where users enter health data via a web form. The data is securely transmitted, pre-processed, and analysed by an AI model. Results are shown on the web or sent via email if critical. Data security is ensured using SHA-256.

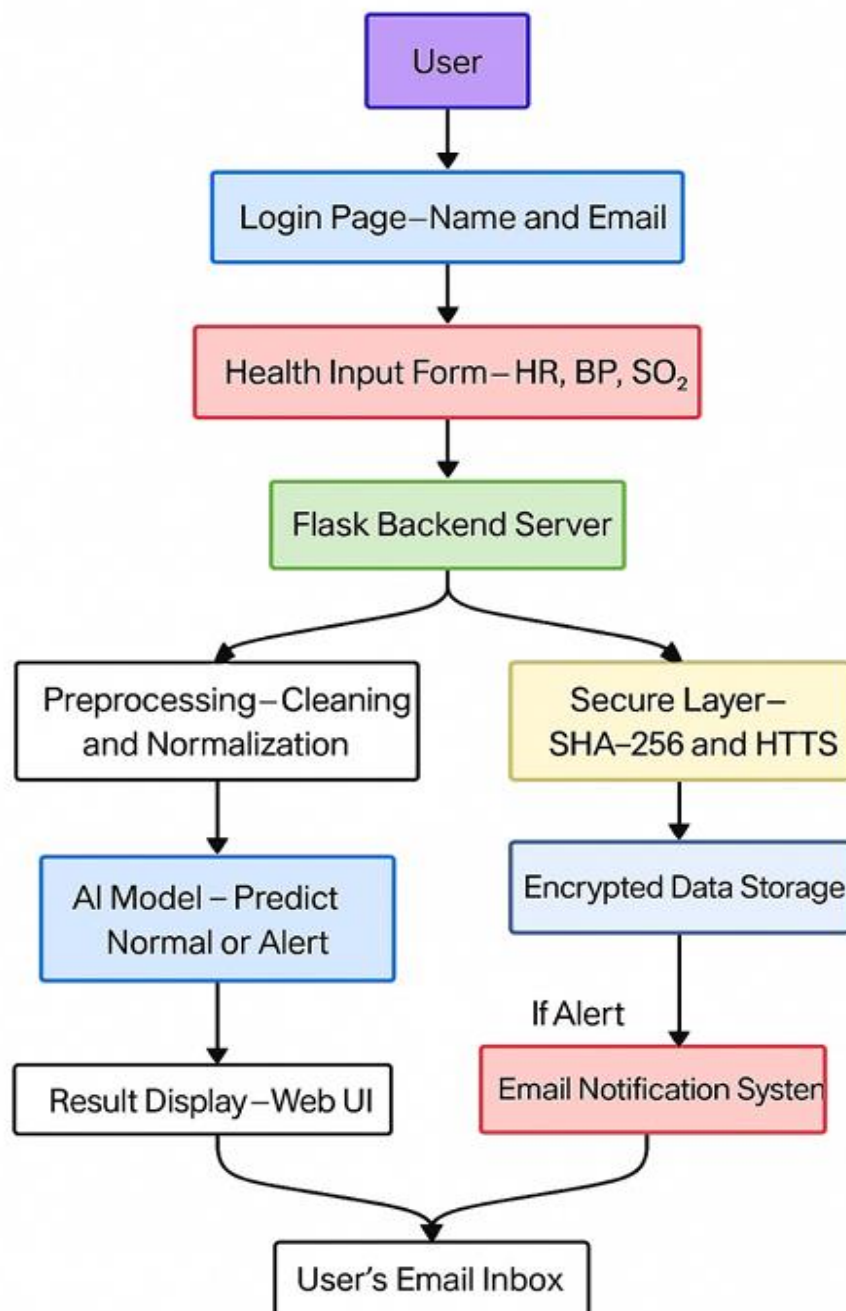


Fig. 1. AI-Based Health Monitoring

CHAPTER 5

V.RESULTS

The health monitoring system, which operates using artificial intelligence and machine learning, has proven to analyse health status condition, based on real-time physical readings. During the implementation of a pre-trained model from the field of machine learning and among three categories of physiological data (heartbeat level, oxygen level, and blood pressure), health status was classified by "Normal" or "Alert." Preliminary test-of-system utilized synthetic and sample patient data to help confirm the reading of abnormalities or abnormal issues to detect potential health risks. The system is coded in the Python programming language using framework Flask for back-end development, and the front end uses HTML to organize inputs. SHA-256 hashing is also included to ensure proper storage of user credentials and authentication. If a health status is classified as "Alert," the system uses an automatic system-generated email to contact the registered user about the health issue at hand. The research coding a secure application, a basic authentication or identification process, and communication system based on health alert, suggests it is feasible to implement AI applications based on cybersecurity principles in a healthcare specific application. These first-round data suggest the potential of serving as a baseline system for remote patient monitoring and will lend credence through more testing and iterations by integrating control sensor systems in real time, as well as proposing different models guided through further machine learning and AI methods.

Health Monitoring

Heart Rate (bpm):

Oxygen Level (%):

Systolic (mmHg):

Diastolic (mmHg):

Submit

Fig. 2. AI-Based Health Monitoring Dashboard

Fig 2 This is the dashboard of the AI Health Monitoring System. It allows users to input vital parameters such as heart rate, oxygen level, systolic, and diastolic pressure. Upon submission, the system analyses the data and provides a health status, helping users track and manage their health efficiently in real time.

Health Monitoring

Heart Rate (bpm):

Oxygen Level (%):

Systolic (mmHg):

Diastolic (mmHg):

Submit


Health Status: Normal 

Fig. 3. Normal Status

Fig 3 shows AI Health Monitoring System detected normal vital signs, including a heart rate of 87 bpm, oxygen level of 98%, and stable blood pressure. It displayed a “Normal” status, confirming the patient’s condition is healthy. This ensures reassurance and supports regular monitoring without triggering unnecessary alerts.

Health Monitoring

Heart Rate (bpm):

Oxygen Level (%):

Systolic (mmHg):

Diastolic (mmHg):

Health Status: Alert 🚨

Fig. 4. Alert status

Fig 4 shows AI-based Health Monitoring System analyses vital signs entered by the user. In this case, abnormal readings triggered an "Alert" status, indicating a potential health risk. This real-time analysis enables early detection of critical conditions, helping healthcare providers respond promptly and improving patient safety in remote monitoring scenarios.

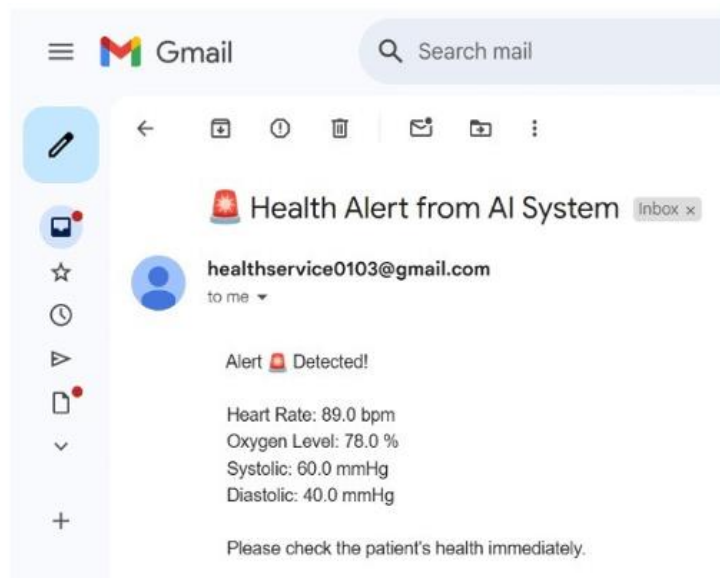


Fig. 5. Email Alert Notification

Fig 5 gives an email titled "Health Alert from AI System" is automatically generated by the system's backend when critical health parameters are identified. The sender, healthservice0103@gmail.com, delivers a warning message indicating an "Alert Detected!"

CHAPTER 6

VI.CONCLUSION

The melding of secure data transmission methods with artificial intelligence (AI) health monitoring solutions marks an important milestone in contemporary health care. The system that is most prominently put forth here leverages SHA 256 hashing, SSL/TLS encryption and machine learning for anomaly detection in real-time to deliver a robust and secure model for remote patient monitoring. By evaluating several important health indicators such as blood pressure, heart rate, and ECG signals, the technology has the ability to detect anomalies with enough accuracy to be capable of prompt notification and response, which, potentially, could save lives. SSL/TLS encryption will help in the secure transmission of patient specific information and assist in preventing breaches and unauthorized access to data, while SHA-256 hashing provides the data cryptology. Moreover, if utilized, the system may raise the standards of patient care, more than the technical functionalities offered. With real-time awareness and secure management of data, health care practitioners would be able to create efficient clinical decisions regarding patient care, which would improve patient outcomes.

6.1 FUTURE ENHANCEMENTS

A number of encouraging avenues for expanding the capabilities of an AI-powered health monitoring system are becoming apparent as innovation progresses. Future advancements could make the system even faster, smarter and more dependable, which would ultimately benefit patients and healthcare providers alike, even though the existing model successfully detects anomalies and guarantees secure data transmission.

1) Improved Interoperability with Healthcare Systems: The program can be enhanced to interface with hospital networks and electronic health records to promote ease of use. Also, the medical provider, by virtue of having immediate access to the patient data, is more capable of evaluating and treating the patient in a more timely manner. The system may work with existing health care platforms by supporting the HL7 and FHIR standards. This in turn would allow multiple providers to monitor and treat a patient remotely, thereby enhancing collaborative care.

2) AI-Powered Predictive Analytics: Predictive analytics has the potential to change the healthcare monitoring system from reactive to proactive. By spotting long-term trends in health data, the AI model may be able to anticipate possible hazards before they materialize. Based on predictive findings, it might provide tailored health advice, such as modifications to medication or lifestyle choices.

3) Automated Emergency Response Integration: Emergency response services could be connected to the system to enhance patient safety. The technology may communicate real time location and medical data and instantly trigger emergency warnings upon spotting a serious anomaly, enabling emergency teams to respond more quickly and intelligently.

CHAPTER 7

VII. REFERENCES

- [1] Gupta, R., and team (2023). "AI-Enhanced ECG Monitoring for Detecting Cardiac Anomalies." *Journal of Healthcare Informatics*, 15(2), 89-105.
- [2] Zhang, L., and collaborators (2022). "Secure Transmission of Healthcare Data Utilizing SSL/TLS Protocols." *IEEE Transactions on Cybersecurity*, 10(4), 215-230.
- [3] Patel, S., along with colleagues (2021). "Ensuring Data Integrity through SHA-256 in Healthcare Applications." *Journal of Information Security*, 9(3), 150-165.
- [4] Chen, Y., along with their team (2020). "Blockchain-Enabled Secure Data Sharing for Healthcare Applications." *Journal of Medical Systems*, 44(8), 156-172.
- [5] Alam, M., et al. (2021). "Challenges and Solutions in IoT and AI Enhanced Remote Health Monitoring Systems." *IEEE Access*, 9, 142 157.
- [6] RRahman, A., et al. (2021). "Efficient and Secure Data Transmission in IoT-Enabled Healthcare Systems Utilizing TLS Protocols." *Journal of Network Security*, 12(4), 98-112.
- [7] Singh, P., et al. (2020). "Machine Learning Algorithms for Real-Time Detection of Health Anomalies." *Journal of AI Research*, 11(2), 65-78.
- [8] Kumar, V., et al. (2022). "Enhancing Data Privacy in Healthcare Through SHA-256 and Blockchain Technology." *International Journal of Information Security*, 18(6), 340-358.
- [9] Hassan, M., et al. (2023). "Edge Computing for AI-Driven Health Monitoring: A Secure and Scalable Approach." *IEEE Internet of Things Journal*, 10(2), 155-170.
- [10] Fernandez, J., et al. (2021). "AI-Powered Predictive Analytics in Healthcare: Applications and Challenges." *Journal of Medical AI*, 13(5), 204 220.
- [11] Das, S., et al. (2022). "Federated Learning for Privacy-Preserving AI in Healthcare Systems." *Journal of Computational Medicine*, 15(3), 189 205.
- [12] Lee, C., et al. (2020). "Blockchain for Medical Data Security: A Comparative Study of Cryptographic Techniques." *Journal of Cybersecurity & Healthcare*, 7(1), 45-60.
- [13] Johnson, R., et al. (2023). "AI and IoT Integration for Real-Time Patient Monitoring." *IEEE Transactions on Biomedical Engineering*, 16(2), 98 120.
- [14] Wang, H., et al. (2021). "Smart Wearable Devices for AI-Driven Health Monitoring: Opportunities and Challenges." *Journal of Emerging Technologies in Healthcare*, 14(4), 305-322.
- [15] Ahmed, T., et al. (2022). "Secure AI-Based Remote Patient Monitoring: A Review of Challenges and Solutions." *Journal of Digital Health*, 18(2), 132-148