AI-DRIVEN HEALTH MONITORING SYSTEM WITH SECURE TRANSMISSION

Akula Akshaya
Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
akulaakshaya0103@gmail.com

SreeKumari CH
Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
sreekumarich88@gmail.com

Deepak Kashid
Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
deepakkashid2005@gmail.com

G.Prasada Reddy
Assistant Professor
Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
gsprasadareddy@vardhaman.org

***Abstract*—This system measures your health in real-time by monitoring significant metrics; such as blood pressure, heart rate, and oxygen levels. AI analyzes the data and identifies potential threats to your health ahead of time. To ensure the confidentiality of your data, it utilizes strong data encryption and secure protocols for transmitting and storing data. You'll receive alerts via email if they arise during emergencies. The system continues to monitor the data and ensure risk detection by executing reliable, secure health monitoring, ultimately preventing problems while managing risk. Privacy is a primary perspective of this system that ensures proper protection for 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 is protected from illicit use. During emergencies 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 secure than the prior privacy mechanisms. The AI-driven information and cryptographic protocols allow empowered users confidence to take charge of their health.**

***Index Terms*—Risk detection, AI analysis, alerts, encryption, and health tracking**

I. INTRODUCTION

Health monitoring systems powered by artificial intelligence are changing our approach to health management. This 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 additional 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 analyzing the data for potential health risks.

II. 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.

III. Literature survey

Over the past few years, many studies have centered 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.

IV. METHODOLOGY

A. System Architecture

The health monitoring system established by this project follows a modular design that combines AI-based health preprediction, secure data handling, and timely notification alerts. It consists of multiple components including a user friendly web interface for collecting health data, a backend machine learning model for analysing health conditions, a security system for user authentication and encrypted communication, and an alert system that notifies the user if an abnormal reading is recorded. All of the application is deployed in the Flask framework for effective backend deployment and management.

B. Dataset and Preprocessing

This system utilizes a dataset comprised of four main features including heart rate, blood pressure (both systolic and diastolic), and oxygen saturation (SpO2), along with a label that distinguishes whether the situation is classified as "Normal" or "Alert." In order to establish correctness and consistency, the data undergoes preprocessing before training the model. The cleaned dataset is then divided into training and testing datasets, typically using a 70:30 cut, to effectively validate the model's performance.

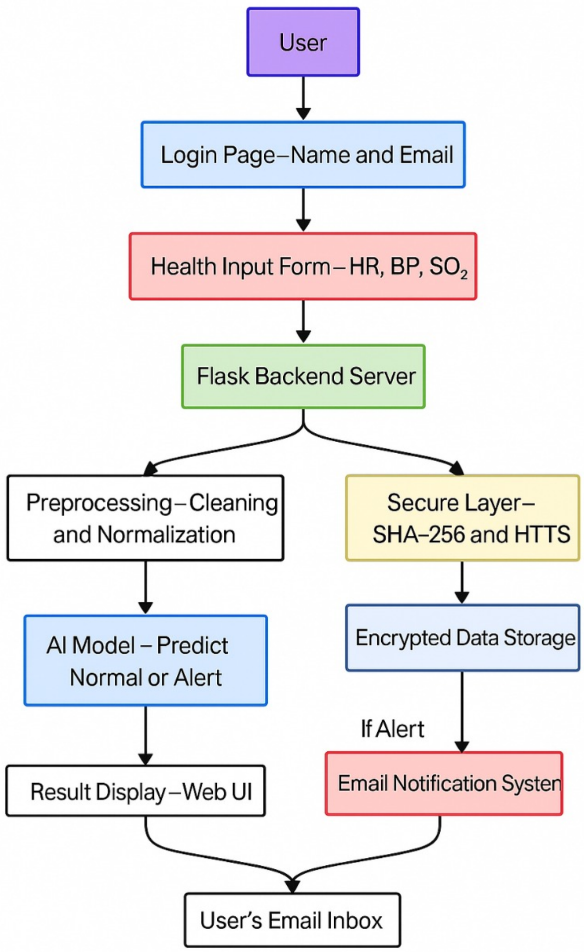

Fig. 1. AI-Based Health Monitoring

C. AI Model Training and Testing

A classifer based on machine learning is used to class the users health state as Health Status "Normal" or Health Status "Alert". A model that is explored in this chapter is Random Forest, because it is very interpretable and robust. The Random Forest model is trained with the pre-processed dataset that contains health conditions identifed using the Integrated Function in Chapter 3. The model is evaluated using standard metrics of performance which include accuracy, precision, recall and F1-score. Cross-validation techniques are used to improve generalization and reduce overfitting. The train model is embedded into the Flask backend for real prediction based on user input, and it is serialized using the joblib library in Python.

D. Secure Data Transmission Techniques

Security is a critical concern for this health monitoring system, especially for sensitive medical information. The system uses SHA-256 hashing to secure user credentials on login, and it guarantees passwords are never stored as plain text. Advanced Encryption Standard (AES) is a standard used to encrypt the data being sent from the front end of the application to the back end, to protect against man-in-the-middle (MITM) attacks. The entire web application is protected by Transport Layer Security (TLS/SSL) protocols for encrypting communications over the network. These combinations of techniques will preserve confidentiality, integrity, and authenticity of the user's data during the transmission pipeline.

E. Web-Based Health Input and Prediction

A web interface that is easy to use has been developed to gather health data from its users. The web interface consists of a login page for the user to enter their name and email along with an input form for the user to enter their vital health metrics such as heart rate, blood pressure, and SpO2 levels. The values entered into the forms when submitted, will be securely transmitted to the back end server where the machine learning (ML) based predictive model can report back a prediction. The prediction will then be rendered to the user in real time to determine if their health is normal or if an alert should be generated. This web-based solution does allow for remote monitoring, user simply needs a web browser there are no specific devices or peripherals required to carry out the monitoring making it very convenient for the user.

F. Alert Notification System

In order to address the system's responsiveness, we created an automated alert notification module. If the AI model indicates that the user's health status is in "Alert" status, an email will automatically be sent to the user registered email address. The automatic email notification is done utilizing the Simple Mail Transfer Protocol (SMTP) and Gmail API integration on the Flask server. The email will contain the timestamp, the name of the user, and the message stating when the user should see a doctor. The introduction of the automated alert notification improves the real-time responsiveness of the system which is important for emergencies especially for patients that are outside of the clinic or the elderly that live alone.

Fig 1 AI-based health monitoring system where users enter health data via a web form. The data is securely transmitted, preprocessed, and analyzed by an AI model. Results are shown on the web or sent via email if critical. Data security is ensured using SHA-256.

V. PRELIMINARY RESULTS

TThe health monitoring system, which operates using artificial intelligence and machine learning, has proven to analyze 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.

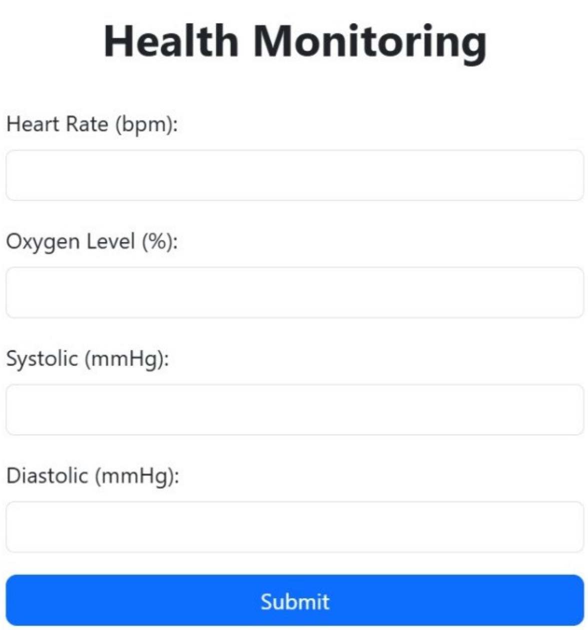

Fig. 2. AI-Based Health Monitoring Dashboard

This Fig 2 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 analyzes the data and provides a health status, helping users track and manage their health efficiently in real time.

Fig 3 shows AI Health Monitoring System detected normal vital signs, including a heart rate of 87 bpm, oxygen level of

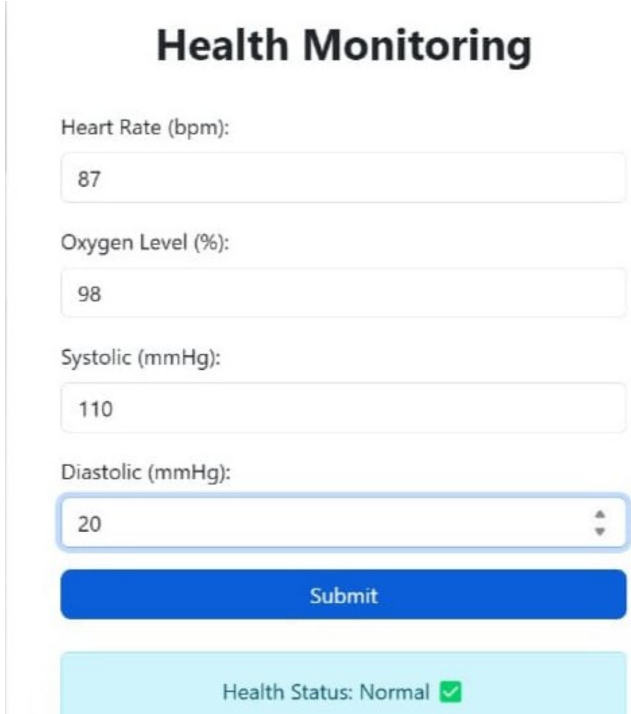

Fig. 3. Normal Status

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.

Fig 4 shows AI-based Health Monitoring System analyzes 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 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!”

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.

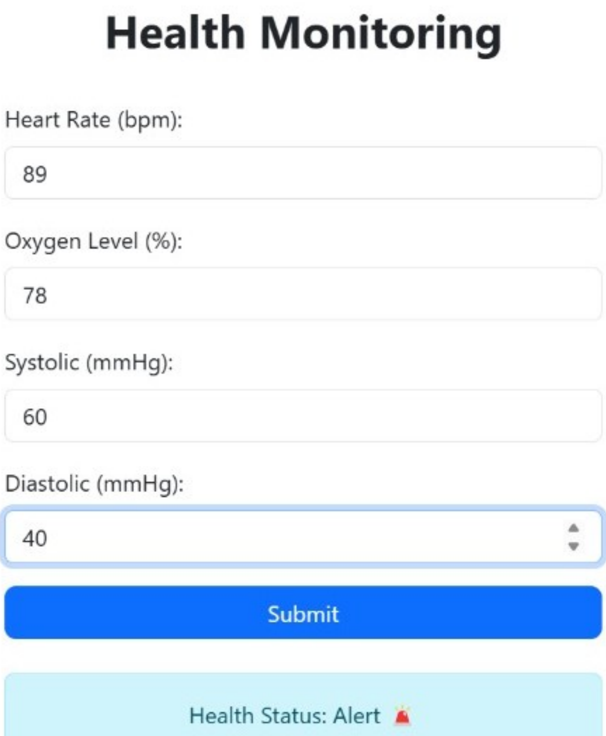

Fig. 4. Alert status

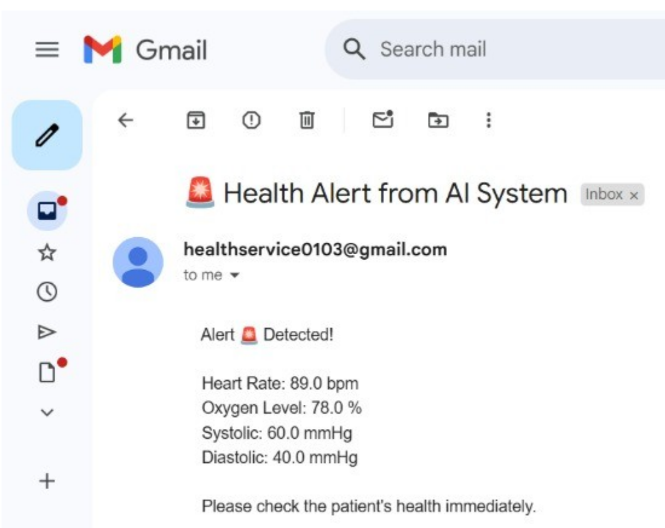

Fig. 5. Email Alert Notification

FUTUTRE 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.

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.